

U.S. DEPARTMENT OF COMMERCE
National Technical Information Service

PB-275 064

Consumer Issues in EFT, Part I: Testimony
Presented to the National Commission on Electronic
Fund Transfers, October 26, 1976

National Commission on Electronic Fund Transfers, Washington, DC

46834

Oct 77

PB 275 064

National Commission on Electronic Fund Transfers
1000 Connecticut Avenue, NW Washington, DC 20036

IWD-56

"Consumer Issues in EFT," Part I

Testimony Presented to the
National Commission on Electronic Fund Transfers
October 26, 1976

NCJRS

MAY 2 1978

October 1977 ACQUISITIONS

REPRODUCED BY
NATIONAL TECHNICAL
INFORMATION SERVICE
U. S. DEPARTMENT OF COMMERCE
SPRINGFIELD, VA. 22161

PORTIONS OF THIS REPORT ARE NOT LEGIBLE.

HOWEVER, IT IS THE BEST REPRODUCTION

AVAILABLE FROM THE COPY SENT TO NTIS

NATIONAL COMMISSION ON ELECTRONIC FUND TRANSFERS

USERS COMMITTEE

Rayburn House Office Building
Room 2128
Washington, D. C.

Tuesday, 26 October 1976

The meeting convened, pursuant to notice, at 9:40 a.m.

Mr. William B. Widnall, chairman, presiding.

PRESENT:

William B. Widnall	William Grosser
Verne S. Atwater	Gordon R. Worley
Thomas W. Taylor	Lester W. Plumly
Robert P. Rogers	Walter L. Anderson
Kenneth Anderson	Lewis H. Goldfarb
George W. Waters	Eugene M. Tangney
Herb Wegner	Richard Beech
Freyda P. Koplow	Marjorie Reed
Roy G. Green	Alan Thorndike
George W. Mitchell	

STAFF:

John B. Benton	Garry Singer
James O. Howard	Romena Johnson
Kathryn Humes	John Youngken
Judy Morton	John McDonnell
James Hatch	Bruce Maye
Janet Miller	Diana Jones
Shelly McConnell	Dick Sprague
Beverly Shay	N. Scott Sacks
Bill Neufeld	Henry Polmer

C O N T E N T S

1		
2	<u>TESTIMONY OF:</u>	<u>PAGE</u>
3	ALAN WESTIN,	
4	Professor of Law and Government, Columbia University	11
5	EARL WARD,	
6	President AFS Associates, representing Independent Bankers Association of America	43
7	BARRY DEUTSCH,	
8	Vice President, Provident National Bank, Pittsburgh, Pennsylvania	56
9	CHARLES MARSON,	
10	Legal Director, Northern California Civil Liberties Union	68
11	CAROL GREENWALD,	
12	Commissioner of Banks, Massachusetts	90
13	ANTHONY DEREZINSKI,	
14	State Senator of Michigan, Chairman, Senate Corporate and Economic Development Committee	109
15	ROBERTA WIELOSZYNSKI,	
16	Director, Office of Consumer Affairs, City of Syracuse, New York	134
17	STEVEN MUELLER,	
18	Transamerica Finance Company, representing the National Consumer Finance Association	154
19	ANNA ALDAMA,	
20	National Consumer Information Center, Washington, D. C.	172
21	ROBERT HAYDOCK,	
22	Bingham, Dana & Gould, Attorneys; Chairman, 3-4-8 Subcommittee of the Editorial Board of the Uniform Commercial Code	188
23	NORMAN PENNEY,	
24	Professor of Law, Cornell University; Member 3-4-8 Subcommittee of the Editorial Board of the Uniform Commercial Code	202
25		

C O N T E N T S (continued)TESTIMONY OF:PAGE

KAREN HAYES,
FRITZ BIERMEIER, and
THOMAS K. ZAUCHA,
Joint EFT Committee, National
Association of Food Chains and
Supermarket Institute

225

JOHN BARBER,
Director of Planning,
Mercantile Bank Shares Corporation

250

P R O C E E D I N G S

3

1 CHAIRMAN WIDNALL: As Chairman of this new
2 Commission I want to welcome all of you who are here today to
3 hear the testimony and to see some of the Commissioners in action.
4 We have very good attendance.

5 I expect that what you would like to hear more than
6 anything else right now is who is on the Commission, and I
7 would like to ask each one of the members of the Commission to
8 identify himself or herself, as the case may be, and then we
9 will proceed after that.

10 First of all, the Vice Chairman of the steering
11 committee, Mr. Wegner, sitting on my left.

12 MR. WEGNER: Thank you, Mr. Chairman.

13 MS. KOPLOW: Freyda Koplow.

14 MR. MITCHELL: George Mitchell, Federal Reserve.

15 MR. GREEN: Roy Green, savings and loan industry.

16 MR. GROSSER: William Grosser, representing George
17 Oram of the Federal Home Loan Bank Board.

18 MR. WORLEY: George Worley, representing retailers.

19 MR. PLUMLY: Les Plumly, U.S. Treasury.

20 MR. THORNDIKE: Allen Thorndike, representing
21 Mr. Daddario from the Office of Technology Assessment.

22 MS. REED: Marjorie Reed, representing Robert E. Lee
23 of the Federal Communications Commission.

24 MR. BEECH: Sandy Beech, representing Mr. Montgomery
25 of the National Credit Union Administration.

1 MR. TANGNEY: Gene Tangney, representing Dick Hill of
2 the Commercial Banks.

3 MR. GOLDFARB: Lewis Goldfarb, representing Robert
4 Lewis of the Federal Trade Commission.

5 MR. WALTER ANDERSON: Walter Anderson, representing
6 Donald Scantlebury, General Accounting Office.

7 MR. ROGERS: Robert Rogers, representing the Federal
8 Deposit Insurance Corporation.

9 MR. KENNETH ANDERSON: Ken Anderson, representing
10 Department of Justice.

11 MR. WATERS: George Waters, non-financial credit
12 cards.

13 MR. HOWARD: Jim Howard, general counsel.

14 MR. BENTON: Jack Benton, Executive Director.

15 CHAIRMAN ATWATER: Verne Atwater, representing Mutual
16 Savings Banks.

17 CHAIRMAN WIDNALL: Now, for this meeting today, Verne
18 Atwater, sitting on my right, will chair the meeting and the
19 discussion that takes place.

20 Prior to that I would like to make a few
21 remarks.

22 I find that in going around the country -- and I
23 don't have to go very far -- just my own community, for
24 instance -- people say, "What in God's name is EFT? What does
25 electronic funds transfer mean, and what are you involved in?"

1 This is a checkless society that some people talk about. That
2 is not my definition, but it is their own. And I
3 just want you to know that the 26 who serve on this Commission
4 are really dedicated to providing sound judgments on facts and
5 figures and hopes and fears as far as the future is concerned.

6 If we go into a true electronic fund transfer
7 society, the pressure that I have had as Chairman of this
8 Commission is rather difficult for me to describe to you. I
9 just know that I have never seen people -- and I have been in
10 government for a long time -- I have never seen people as
11 dedicated as the members of this Commission, who really
12 recognize and are willing to burden themselves with the neces-
13 sary work to provide a sound judgment on this for the entire
14 society of the United States.

15 I believe that the decisions and recommendations
16 this Commission can make during the short term that we are
17 committed will have a great deal to do with shaping the
18 future of our society during the next 25 years. It is a heavy
19 responsibility because there are areas in this investigation
20 that could well affect all phases of an
21 electronic fund society--the areas of privacy, security, legal
22 rights and duties, and above all, I think, consumer choice and
23 consumer convenience.

24 This is our first full-scale hearing in
25 the lifespan of the Commission as we know it. It is appropriate

1 and fitting that the subject that we chose to go into during the
2 course of the hearings today, this morning and afternoon, has
3 to do with the impact on the consumer in an electronic fund
4 transfer society.

5 The public will judge those of us who are serving on
6 the Commission by the way we handle this hot consumer item.
7 We are all consumers. I often wonder, myself, what is the
8 definition of a consumer representative? Anybody in our society
9 can actually be a consumer representative because he is a con-
10 sumer and he can always speak for himself. But there are some
11 who have specialized in doing things that would bring to the
12 attention of government and the people in our society the
13 very serious problems faced by consumers. Action is taken
14 by the government or by individuals and/or organizations within
15 our society.

16 Congress recognized the importance of this issue
17 when they mandated that the Commission investigate the impact
18 of EFT on the consumer. Specifically, the law requires that we
19 take into account, first, the need to afford maximum user and
20 consumer convenience; second, the need to afford maximum user
21 and consumer rights to privacy and confidentiality; third,
22 implications of such a system on the availability of credit.

23 Today we begin our dialogue on consumer issues.
24 And I first want to call your attention to the fact that there
25 are five major areas that are included in consumer issues: the

1 right of privacy, security, legal rights and duties, consumer
2 choice, and consumer convenience. The Commission earnestly
3 wants a dialogue to be conducted by the public and by those who
4 are organized, for one purpose or another, within our society
5 to tell us by way of a two-way communication what they feel is
6 important and must not be forgotten

7 Consumer groups,
8 state and federal consumer protection groups, financial and
9 non-financial institutions with consumer experience, the trade
10 and industry associations, we earnestly request all of them to
11 submit their feelings, ideas, and recommendations.

12 We have honored every request to testify. Many
13 organizations and individuals who could not be here today are
14 submitting statements for the record. We invite more comment.
15 Any of those in the audience today, we invite your written
16 comment for the record, and the record will be open for three
17 weeks. You may still contribute your ideas during that period.

18 I would like to turn over the meeting at this
19 time to Verne Atwater, who is Chairman of the subcommittee that
20 is handling this particular subject matter.

21 And as to procedure, Verne, I expect to call
22 witnesses and swear them in, and you can take over from
23 there.

24 CHAIRMAN ATWATER: All right. Thank you.

25 CHAIRMAN WIDNALL: Would you like to make some

1 preliminary remarks?

2 CHAIRMAN ATWATER: Thank you, Mr. Chairman. I will
3 take just a moment to restate the general ground rules
4 for the operation of the hearing which have been incorporated
5 in the Notice of Hearings submitted as a part
6 of the Federal Register, on October 5th.

7
8
9 First, each witness will be asked to limit his
10 presentation to a 10-minute summary of the written statement
11 which he has submitted to the Commission before this hearing.
12 There will be a period of questioning which will typically not
13 exceed 10 minutes, but it is the option of the Chair to
14 determine the length of questions that the Commissioners that
15 may want to ask each of the witnesses who will appear before
16 us. There may be questions addressed to the witnesses by the
17 Commissioners in writing after the hearings. I am certain to
18 many of our Commissioners there will be questions that appear
19 during the testimony that may or may not be appropriate to ask
20 in oral form but which will certainly be submitted to the
21 witnesses and requested answers after these hearings.

22 Third, each witness will be sworn in, as the
23 Chairman has indicated.

24 All of the questions and the answers of today's
25 hearings are being transcribed. A transcript of these hearings

1 will be sent to each witness following the hearings today for
2 him to review and essentially to edit, because all of the
3 testimony will become a part of the report the Commission makes
4 to the President and to the Congress at the completion of our
5 work.

6 We do appreciate the excellent attendance in the
7 audience today of people concerned about what the Commission is
8 doing. Although there is no basis for participation directly
9 from the audience in these hearings today, as the Chairman has
10 indicated, we are very much open to written testimony or
11 written questions you may wish to submit to the Commission
12 today or after today's meeting.

13 I would like simply to indicate that the general
14 questions we have asked the witnesses to address the
15 Chairman has summarized in his introductory remarks.
16 As a part of the note sent to each witness, we did ask three
17 general questions which we would like to have a response from,
18 either during this testimony or later.

19 The first one is, to what extent do existing
20 regulations or laws provide protection -- in short, convenience
21 to the consumer--and to what extent does EFT affect the adequacy
22 of those laws or regulations?

23 A second question is: In the event new legislation
24 or new regulations are required, should they be at the federal
25 or state level?

1 And then to the extent you can, we would appreciate
2 the specific recommendations you may make about what you
3 think this Commission ought to consider being done or
4 incorporated in its final report.

5 With that, I would suggest that we can, reasonably
6 on schedule, proceed to our first witness.

7 CHAIRMAN WIDNALL: Professor Alan Westin.

8 Would you stand up and hold up your right hand. And
9 I will ask Jim Howard, our general counsel, to swear you in.

10 (Witness sworn.)
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

1 CHAIRMAN ATWATER: We are very fortunate, indeed, to
2 have a distinguished scholar in the field of information
3 technology, privacy and freedom with us to be our first witness
4 in these hearings.

5 Dr. Alan Westin is Professor of Public Law and
6 Government at Columbia University. He was a principal
7 consultant to Senator Sam Ervin in the drafting of the Federal
8 Privacy Act of 1974, and has served on the National Wiretapping
9 Commission, as well as having a long history in this
10 important field of privacy.

11 Dr. Westin, we would appreciate your comments.

12 TESTIMONY OF ALAN F. WESTIN, PROFESSOR OF LAW
13 AND GOVERNMENT, COLUMBIA UNIVERSITY

14 DR. WESTIN: Thank you.

15 Mr. Chairman, ladies and gentlemen of the
16 Commission, I am honored by your invitation to appear here
17 today and share some thoughts with you about electronic fund
18 transfer developments and proposals.

19 This is an area that I have
20 been involved in for almost 15 years now, from the time when,
21 early in the 1960s, proposals for so-called
22 checkless, cashless societies began to surface, and I was
23 involved as the director of a study for the Association of the
24 Bar of the City of New York on the impact on privacy. I took
25 a second look at the issue when I was directing the National

1 Academy of Sciences' Project on Computer Data Banks between 1969
2 and '72. And now your invitation gives me a good opportunity
3 to look again at where EFT proposals stand in 1976.

4 As the rules indicate, what I would like to do is
5 to summarize some of the highlights of the written statement
6 that I have supplied to the Commission and invite your questions
7 about anything that I suggest that may intrigue you and upon
8 which you would like further development.

9 Obviously, this Commission does not start with a
10 clean slate. It has been over a decade that we have been
11 debating whether there is in fact a plan for an EFT system for
12 the United States and what the implications of any kind of
13 comprehensive EFT system would mean for individual privacy.
14 Much of this debate, I think, has been highly stylized. On the
15 one hand, the presentations of EFT enthusiasts describe a system
16 of total pre-authorized deposits of income virtually from all
17 sources, and on the other pre-authorized disbursements and
18 recurring obligations. The assumption is that there would be a
19 single data base on the individual account-holder in the hands
20 of some kind of a financial utility, a system of a national
21 communication network that would be terminally oriented so
22 individuals could make various kinds of transactions anywhere
23 in the country or within a region and have it immediately
24 entered into such a data base. Also, there would exist some
25 system for a

1 unique personal identifier, so one could be sure
2 that the individual was properly identified, and security
3 against fraud and misuse and so forth could be policed.

4 These three elements, the central data base and
5 national terminal-oriented communication system and unique
6 personal identifier system, are usually the key elements that
7 have been portrayed in the last decade of writing as the
8 essentials of what I would characterize, not meaning it in the
9 pejorative sense, as a total-system approach to EFT.

10 On the other hand, in the last decade we have seen
11 the responses of civil libertarians and others presenting an
12 equally total approach. They have looked at such a
13 system and seen it essentially as an Orwellian delight -- clearly,
14 such a system as I just described would aggregate far more
15 personal information than is presently collected by any single
16 financial institution or retailing group or credit reporting
17 system, et cetera; -- and this would allow those who
18 managed such a system or anyone else that had access to it by
19 law or by stealth to accomplish literally unprecedented feats
20 of surveillance over the individuals, associations and
21 organizations whose accounts would be in such a system. It
22 could make it possible to locate individuals at a given moment,
23 track their movements over time, develop profiles of their
24 spending and savings habits, monitor whether the use of
25 government or private funds met various regulatory or program

1 requirements. It could identify their money base, political,
2 religious, civic or sexual affairs, and it could lead to imposing
3 various controls over access to funds with enormous conse-
4 quences for various economic and social groups in the popu-
5 lation.

6 I think civil libertarians have particularly pro-
7 jected the possible use of an EFT total system against the dis-
8 closures of the last five years or so about the FBI's covert
9 access to the bank deposit records of civil rights and anti-war
10 groups in the late '60's, as illustrated in the Media,
11 Pennsylvania FBI papers about FBI access to bank records in the
12 Philadelphia area. They point out disclosures about the
13 access to government files by President Nixon and his aides
14 during their war on alleged political enemies and domestic
15 subversives, and the kind of revelations about leaks of confi-
16 dential information that have made up recent inquiries into
17 the CIA, the FBI, et cetera.

18 Thus, it is against that backdrop of government
19 abuse, or disputed government actions, that civil libertarians
20 have responded to the proposals for a total system of EFT.

21 I think that this was a useful first stage in the
22 debate. It was almost inevitable. I think the civil libertarians
23 performed a completely appropriate function in trying to
24 underscore the
25

1 long-term possible negative consequences of any total system
2 of EFT that might be considered. In fact, I reminded myself
3 in preparing for this, that since I had lust in my heart for
4 privacy as much as the next civil libertarian, I wrote just
5 such an analysis for Playboy Magazine in 1968--

6 (Laughter.)

7 DR. WESTIN: --to discuss where the then current
8 proposals for EFT might lead us and where a national data
9 center might lead us lest we first strengthened our basic
10 privacy laws.

11 My feeling is that it is going to be at least
12 several decades before any such total system of EFT could
13 be conceived or instituted. Furthermore, no plan for EFT
14 that has been presented to your Commission by Congress or
15 the President or an executive agency, nor is one available
16 from the business community as a sort of endorsed, compre-
17 hensive projection. Therefore, it seems to me that the job
18 of this Commission is to look at where we stand today in
19 the protection of the individual's right to privacy in
20
21
22
23
24
25

1 financial records, to look at the experiments with less-check
2 and less-cash arrangements that are currently developing, and
3 to see what new conceptions of rights and procedures,
4 monitoring agencies and new institutional arrangements
5 might be important for your Commission to recommend to Congress
6 to deal with the transition from where we
7 are now to where we will be going in the next decade or two.

8 With that kind of controlled
9 experience, we can then make some judgments about how
10 more total system EFT approaches
11 should be evaluated for their social value, for their
12 business value, and for their respect for individual rights.
13 What I would like to do now is suggest
14 the key transitional issues that are
15 presented at this stage in 1976.

16 Let me start by suggesting some terms that I
17 have found helpful and that I think might clarify some
18 of the conflicting use of language that appears in much of the
19 literature on this and privacy-related issues.
20
21
22
23
24
25

1 I think, first of all, the word "privacy" should
2 refer to the question of what information should be collected
3 at all for a given business, governmental or social purpose.
4 It involves issues of legitimacy and of relevance, and it is
5 the way in which a society says that, for certain purposes,
6 they do not want a given body of information collected at
7 all and stored by an organization.

8 Secondly, the term "confidentiality," refers to
9 who should have access to information once it is legitimately
10 collected, either within an organization, such as which units
11 should have access to it inside a multibureau organization,
12 and who--if anyone--outside the organization should be given
13 access to that information. The rules of confidentiality
14 arise from the original bargain between the individual and
15 the collecting organization as to the purpose for which the
16 information has been provided and the uses that should be made
17 of it.

18 The term "individual access" refers to the right
19 of individuals to know what information has been collected
20 about them, to examine it for accuracy and completeness,
21 and to know what uses have been made of it. It has a due
22 process dimension to it, in terms of the guarantees of fair
23 procedure required under American constitutional law.

24 Finally, as to the often ill-used word, "security,"
25 I suggest this should be understood as a test of whether
an organization can keep its promises of

1 confidentiality, either the promises made as a matter of its
2 policy or as a matter of law. Security ought not to be
3 confused with privacy or confidentiality, both of which are
4 policy issues, whereas security, essentially, is a technical
5 condition, the organization's capacity to safeguard data
6 according to the rules of confidentiality that have been set
7 against misuse from inside or against capture from outsiders.

8 With those definitions in mind, the first point
9 I would like to make is that I think our present law as to
10 confidentiality, privacy and access in the field of financial
11 records is in disarray. The first recommendation that I
12 would hope this commission would make is for Congress to
13 strengthen the rights of privacy of depositors and other
14 users of financial institutions. Since I know that there will
15 be testimony presented later today by Mr. Charles Marson of
16 the American Civil Liberties Union of Northern California,
17 and since I think that the criticisms he will make to the
18 Supreme Court decisions in the Schultz and Miller cases and
19 his endorsements of the new California state banking approach
20 represent the kinds of things that I also would recommend,
21 let me do no more here in the summary than to say that I
22 think that we cannot move toward more automated payment
23 systems until we first get the baseline of law into adequate
24 condition. We do not have it such today.

25

26

27

1 We have at the moment no depositor right of privacy
2 that is recognized nationally by the Supreme Court. We do not
3 have adequate procedures by which process is served to obtain,
4 with notice to the depositor, financial records

5 for investigative purposes. And, until we
6 build that foundation, it seems to me we dare not move to more
7 elaborate data bases and more terminal-oriented communication
8 of such information, simply because we would be increasing
9 the efficiency and the speed of transactions and creating
10 inviting data bases for surveillance purposes without setting
11 first into place proper definition of rights that exist today.

12 But I hope in this summary to stress more
13 what I think this commission could begin to help the American
14 society formulate, and that is a new conception of the
15 individual's right to privacy, not in existing financial
16 records but in the new types of financial records that would
17 be developed by EFT-type pilot programs and, ultimately,
18 an EFT-type national system.

19 I begin by believing it is a mistake to say that an EFT
20 account holder should have the same rights as he or she does
21 today in a bank account or in records of a financial
22 or retailing establishment or any credit reporting service. I
23 believe that when personal information is merged from a wide
24 variety of sources into
25 income, deposits and recurring transactions being recorded

1 in a central data base, capable of being manipulated by
2 computer technology, that a new trustee relationship will
3 have arisen, or should be held to have arisen by law,
4 under which that property in an EFT data base belongs only
5 to the individual and not to the system. The system
6 managers should be, obviously, allowed to use it for the
7 purpose of the information between the account holder and
8 the EFT system for funds transfer purposes, and also would
9 have to have access to it for various kinds of security
10 purposes, audit and so forth. But any further commercial
11 or gainful use of an individual's transactional history
12 would, in my judgment, represent the taking of valuable
13 property owned by the individual for which both consent and
14 compensation should be required.

14 Here, I am and will be talking only about commercial
15 and private use. I will save for a minute government use.

16 On the commercial and private side, I think the
17 day should be over in which the profile of an individual
18 generated by such a data base is thought of as a free
19 good, like clean air and clean water used to be regarded in
20 the economic theory of the country. Rather, I would
21 suggest that when a detailed profile of our consumer
22 transactions is generated by such a system, that this is a
23
24
25

1 valuable property of the individual and that no further
2 use should be made of it unless the individual has expressly
3 consented and has been compensated for it.

4 The way I would envisage this happening is that,
5 when we open our accounts in any kind of more automated
6 payments system, we would have options presented to us.
7 And one option would be to check off "no further use made of
8 my information." The second might be, "use in the following
9 listed categories: charitable solicitation, religious
10 solicitation, commercial solicitation," or whatever categories
11 might be developed. And a person would be automatically
12 credited -- that is one of the nice parts about computer
13 technology and an automated payment system -- 3 cents or 5
14 cents or 10 cents for each such use that is made of our
15 personal information. Then, when the postman arrives
16 at our house and we get all of those direct mail order
17 things sent to us, we can smile with happiness that 3 cents is
18 automatically going into our account for each such use. And
19 then there is some incentive for us to open ourselves, perhaps,
20 to commercial, charitable, political and other solicitations.

21 One other option for which, in my thinking at
22 least, we might give the highest compensation is the
23 individual who says, "Send me everything. I'm perfectly
24 willing to have anything that you want made available to
25 me by direct mail."

1 The reason I am somewhat enamored of this
2 suggestion is that I think it is the most privacy-respecting
3 approach to the issue of what additional commercial uses
4 could be made of such account information. That is, it does
5 not let anybody, whether it is the ACLU or the bankers or
6 anyone, decide what we should do with the profile that is
7 built up with us in such a system. It lets us as individuals
8 decide if we want to have direct mail, and that is marvelous.
9 If we feel that our solitude is important and that we hate
10 junk mail, we also would have a right under such a system to
11 control that.

12 I think you will find that virtually every
13 definition of "privacy" starts by saying that this is the
14 right or the claim of an individual to decide for himself or
15 herself what information about them will be shared with others
16 and what uses would be made of it. So I think this respects
17 the individual's privacy in the exact degree to which we ought
18 in any such enhanced profile system.

19 Secondly, what about government access by law
20 enforcement and other authorities to such a central account?
21 It seems to me there are three basic approaches one could
22 take.

23 First, no access whatever for any government
24 purpose, which I cannot accept, seeming to me much too total
25 and unwise an approach. We reserve this for very rare

1 instances, like psychiatric registers or for the priest-
2 penitent privileges. I can't
3 believe financial transactions should enjoy that total
4 immunity.

5 The opposite alternative would be to say access
6 as it is today. But I have already suggested that our rules
7 today are inadequate and dangerous to civil liberties, and
8 so I reject the notion that we should simply try to transfer
9 existing rules and regulations into a more enhanced payment
10 system.

11 Between these two lies what I would suggest is the
12 right approach, which is to define a new set of rules and
13 regulations for access by government for various purposes to
14 such an account. I would suggest these kinds of basic
15 approaches. First, any inquiry by government which involved
16 inspection of records of an EFT system that directly related
17 to First Amendment protected activity -- religion, press,
18 speech and assembly -- and especially where the records of
19 private associations, civic groups, et cetera, are
20 involved, would be presumptively improper. There ought
21 to be a special procedure of judicial warrant that would
22 inspect proof of probable cause and, especially, would look
23 to see whether there were not available other means of
24 investigation less intrusive into the privacy of individuals
25 than a search of an EFT account.

1 The Omnibus Crime Control Act of 1968 requires
2 such a judicial inspection when wiretap warrants are
3 made. And, while we don't have a stunning record of judges
4 turning down federal officials when they have sought
5 electronic warrants for wiretapping or room-bugging, I think
6 it is the right approach. Perhaps the judges would be
7 better disposed to balance the equities in this situation
8 than they would in a wiretapping situation.

9 There would be, in my mind, no general search of
10 an EFT data base permissible by law. That is, no putting of
11 lists of alleged suspects through an EFT data
12 base to see what hits you might get, comparable to the wanted
13 persons search that can be done in the NCIC system of the
14 FBI. To my mind, that would be as close to the
15 general warrant that our Fourth Amendment intended to outlaw
16 as anything that would correspond to the earlier British
17 practice.

18 Secondly, before any automated payment from a
19 government social benefit program was included in an EFT
20 system, I would suggest that there ought to be a public
21 notice proceeding or a privacy impact statement before the
22 legislature, so it could examine whether it was appropriate
23 to have that system included in the EFT plan and what means
24 of enforcement would be followed. My statement goes on
25 to describe that more fully, and I won't go into it here.

1 Finally, I think we ought to seek some new
2 institutional arrangements for an EFT plan. That is, I would
3 hope that some kind of regulatory commission could be
4 conceived, whether existing or special, with private as
5 well as public members, whose function it would be to audit
6 such a system in general, but, in particular, to look at its
7 rules and practices as far as protection of privacy,
8 confidentiality and individual access were concerned. I think
9 we need just that kind of an audit and monitoring by
10 independent agencies to insure that the system is meeting the
11 kinds of standards that I would hope Congress would
12 set.

13 This concludes my oral presentation, and I would
14 be very glad to answer questions from the commission about
15 any aspect that I presented.

16 CHAIRMAN WIDNALL: Thank you, Professor Westin.

17 CHAIRMAN ATWATER: I certainly thank you for
18 an enlightening beginning to our hearings. We now have time
19 for questions from the commissioners.

20 I would like to ask, as a beginning question, to
21 what extent the Bank Secrecy Act, in your judgment, represents
22 that base building block that would need to be revised as,
23 essentially, a first step.

24 DR. WESTIN: I think the Bank Secrecy Act, as
25 it has been interpreted by the courts, was strong on

1 record-keeping and weak on protection of the individual's
2 right of privacy. Also, the kinds of amendments that are
3 now pending in several bills in Congress to specifically
4 recognize the depositor's right to privacy in an account,
5 to provide the kind of notice and defense proceeding when
6 any legal process is presented, and to provide for some kind
7 of rules governing the the permanent record-
8 keeping system would be the essential first steps.

9 I think, whenever you look at systems like the
10 criminal justice information systems that are developing, or
11 the local government data banks of welfare and social benefit
12 programs that are developing, they almost have

13 a concept of the individual's primary control of
14 information, though shared with the keeper of the system.
15 The trouble with the Bank Secrecy Act is that it set no such
16 right of privacy to the depositor and left it up to the bank
17 to be the keeper of the individual's privacy.

18 My experience has been that some banks have been
19 exemplary in that, but many, many of them are not. They have
20 close relations with the same FBI officials who have to
21 investigate bank theft and other kinds of issues, and that
22 doesn't necessarily help them to take an adversary stance
23 vis-a-vis inquiries by IRS or the FBI or other agencies.

24 CHAIRMAN ATWATER: Thank you.

25 MR. MITCHELL: Mr. Chairman?

1 CHAIRMAN ATWATER: Mr. Mitchell?

2 MR. MITCHELL: I am a little unclear as to whether
3 the abuses that are implicit in your statement to privacy
4 originate from commercial banks, who are the only agencies
5 that are handling large-scale money transfers today, or
6 whether they arise from a weakness in government rules and
7 regulations with respect to disclosure.

8 For over a decade now, we have been using electronic
9 means for doing our accounting in banks and for doing our
10 storage of information. So that phase of EFT has been in
11 existence for a considerable time. And my impression is that
12 there have been some abuses arising, but not many relative
13 to the number of accounts. There are 100 million accounts
14 in the country and a very small number of abuses, as far as
15 I can tell.

16 As I listen to what you are saying, I have a
17 feeling that you are bringing into the focus of your attention
18 data banks that are used primarily for credit purposes and
19 are not based in any sense on transactions information. I am
20 not sure that all banks do not use transaction
21 information in their own credit phases, but I don't believe
22 they do. In any event, I'm sure they would not share
23 that information with anybody else.

24 So, my question is, is privacy really a
25 new issue, or is it an old issue? And, if it is a new issue,

1 why is it a new issue?

2 DR. WESTIN: I will try to be very brief for what
3 is, obviously, a very large question.

4 No, I was not thinking about credit reporting
5 systems. I was thinking about, primarily, the access to
6 paper bank records and microfilm bank records

7 in the past decade, in which Congressional com-
8 mittees, grand juries, state investigating committees, IRS
9 and a wide variety of government sources have, in fact, sought
10 the checking account and other physical evidences of monies
11 in banks, and where as with the FBI access to the
12 accounts of black militant groups and antiwar groups in the
13 Pennsylvania area, the issue was, would the bank notify
14 the group that, in fact, its accounts were being searched by
15 the FBI. Would there be any proceeding by which that group
16 would be able to say, "You have no proper authorization; it is
17 a fishing expedition," et cetera?

18 I'm not necessarily prejudging how the court will
19 decide that particular issue. But it seems to me absolutely clear that
20 there ought to be such a general right and such a standard procedure.

21 One example of which many people are aware was
22 when the Fifth Avenue Parade Committee, one of the antiwar
23 groups in New York, had its accounts subpoenaed by a
24 Congressional committee which was wanting to see who had
25 sent checks to the Fifth Avenue Parade Committee to hire

1 buses when that group was bringing citizens to Washington to
2 launch a war protest. And it seems to me -- nothing is
3 absolutely clear on the Supreme Court decisions -- that the
4 right to come to the nation's capital and seek a redress of
5 grievances is one of the privileges and immunities of citizen-
6 ship protected by the 14th Amendment
7 and that anything that would take the records of those bus
8 purchase transactions and make them part of a Congressional
9 committee hearing would be dangerously chilling First
10 Amendment rights and the kind of right to express grievances
11 that we like to protect.

12 So, in short, I think it is an old issue, in the
13 sense that the balance between depositor privacy and govern-
14 ment's right to know has been with us a long time. The points
15 I tried to stress in my testimony are that it will be a far
16 larger data base of transactions in any kind of more compre-
17 hensive system than we --

18 MR. MITCHELL: Why is there a larger date base
19 than we have now?

20 DR. WESTIN: If you are assuming a kind of EFT
21 system in which there will be more transactions that will
22 be programmed in it --

23 MR. MITCHELL: Are you talking now about what you
24 call "the total system"?

25 DR. WESTIN: Or something moving toward it. In

1 other words, I think you could do it this way. If you looked
2 at the typical individual's account today in a bank, it
3 excludes, does it not, American Express and BankAmericard,
4 et cetera, because they are not part of
5 your normal checking account?

6 MR. MITCHELL: Well, it includes the settlement
7 for those.

8 DR. WESTIN: But it doesn't give you location
9 information and movement information in the same sense.

10 Now, as I read the proposals, some of the proposals
11 for EFT, one of the first things some people would like to
12 see brought into such a system would be those kinds of card-
13 based transactions. To the extent you did, the account would
14 suddenly be able to tell you where you had dined, where you
15 had traveled, which hotels you had stayed at--things which I don't
16 think are normally within the checking account transactions.

17 MR. MITCHELL: Well, that could happen, of course.
18 But I think the convenience accumulation that occurs,
19 accumulating transactions throughout some period and then
20 paying them at the end, is pretty well established as an
21 operating practice. I don't see any reason for that to be
22 eroded with immediate payment.

23 DR. WESTIN: I think it depends on
24 where you think the terminal input would be placed. You know,
25 neither one of us has one plan in front of us that we are

1 dealing with. But as I view some of the plans, they call for
2 a terminal, let's say, in the Hilton Hotel or at Garfinkel's
3 department store, where you have a direct
4 input at that point that you have stayed there, that you
5 have made such a purchase.

6 That would not, at least in the plans I have seen,
7 go to a separate American Express account, and only when 20
8 of those had been aggregated would it be transferred to the
9 EFT system. Rather, the idea is that it would go directly from
10 terminal to data base. That means -- and I think it is very
11 important -- that what is now information located partly in
12 your bank, partly in your credit card, oil card, T&E card
13 records, partly, perhaps, in your credit bureau transactions,
14 could, depending on which EFT plan one would see, would
15 then be direct inputs to the EFT system. The data base
16 would have that information. And, depending upon how it is
17 formatted, I would imagine, for security purposes, you
18 would have to know where it took place and the amount of
19 transaction and the day.

20 You would have created one of the most efficient
21 ways of tracking individuals, of monitoring where they have
22 been, what they have spent, et cetera. So I would argue very
23 strongly that it is an old problem, not stunningly new in
24 its conception. But it becomes a far richer, more
25 comprehensive data base available on a nationwide, terminal

1 communications system, raising problems of many people having
2 access, which you hope to control through access and audit
3 controls in the computer system, but raising different problems
4 of security than you do in existing, non-terminal-oriented
5 banking systems or credit card systems. I think those are
6 the elements I would stress as different.

7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

1 CHAIRMAN ATWATER: Mr. Goldfarb.

2 MR. GOLDFARB: Your testimony focused primarily
3 on access to consumer information.

4 Do you believe that consumers' claim to the accuracy
5 of that information in data banks is also part of the concept
6 of privacy? Do you believe the existing laws which are
7 supposed to enable consumers to monitor the accuracy of that
8 information are adequate, namely, the Fair Credit Reporting
9 Act?

10 DR. WESTIN: In my written statement, I did
11 mention that I hope one of the declared standards of any kind
12 of legislation that might be set up would recognize such an
13 individual right of access, and it would be fully implemented.

14 Specifically, I would think that in any such
15 system, we would need a different kind of
16 bank statement or different kind of consumer statement than
17 we probably get now that would enable us to know better and
18 to check better the accuracy of the information. The
19 Fair Credit Reporting Act, because it is limited, as you know,
20 to credit, pre-employment, pre-insurance reporting, and does
21 not purport to cover bank transactions per se, does not seem
22 to me to be on all fours with this problem.

23 I happen to think the Fair Credit Reporting Act
24 is an excellent statute. It could use some improvement, but
25 I think it has worked very well. As good as it is, though,

1 it is not the answer to the problem that we are discussing
2 today, because its reach is not co-extensive with the credit
3 card companies, the financial accounts and financial
4 institutions and so forth.

5 MR. GOLDFARB: Do you believe consumers should have
6 the opportunity to verify the accuracy of this information
7 from time to time?

8 DR. WESTIN: Absolutely.

9 I spent a year in Italy, and one of the most
10 frustrating things I encountered was the European banking
11 tradition that you don't get an automatic statement of your
12 account each month.

13 I was barely able to survive not getting the thing
14 that I was used to as an American consumer.

15 Yes, we need a statement of accounts,
16 but I think you would have to work out on a much better
17 basis what the format of such a statement to the consumer
18 should be, what information it would need to have in it to be
19 truly effective so the consumer could see what was being
20 charged and who had charged it, and all of those elements that
21 would enable the consumer to know.

22 I can imagine nothing worse than having some
23 of the computerized statements that we now get simply
24 transferred over to an EFT, virtually undecipherable, full of
25 abbreviations that may make good sense to a software

1 programmer, but not to human beings trying to understand
2 what their transactions have been.

3 CHAIRMAN ATWATER: Mrs. Koplow?

4 MS. KOPLOW: Professor Westin, you stated that
5 general legislation is needed to prevent abuse of personal
6 privacy by the government and by others, but you
7 go on to charge that all of this should be incorporated into
8 EFTS legislation or regulations.

9 By doing so, don't you put a roadblock in the
10 way of the development of EFTS so that it cannot really
11 develop as a consumer convenience along the line of
12 consumer services?

13 It appears to me that you want to have a uniform
14 EFT code similar to the Uniform Commercial Code all
15 incorporated into EFTS prior to the time that we had the
16 kind of experience with the system that would warrant the
17 development of that kind of a code.

18 And you talk about it being decades away.
19 Probably it is. I'm not sure that I can agree with you
20 entirely there. But if you charge this Commission
21 with reforming the entire privacy segment of transactions
22 legislation, you make it almost impossible for it to go on.

23 You appear to want most of the Bill of Rights
24 incorporated into an EFT code.

25 DR. WESTIN: Well, I'm not sure I agree with you --

1 I'm sure I don't--because of this reason. I'm suggesting,
2 first of all, that long before we take one more step towards
3 EFT I would hope this Commission would recommend to Congress
4 that we put into statutes the kind of protection of the
5 individual's right to privacy in deposit which has been
6 recommended by leading members of Congress and which I
7 think commands very wide bipartisan support: support
8 in the business community, support in the civil liberties
9 community.

10 So the first step is, even before you spell out
11 what an EFT looks like, to deal with the existing legal
12 situation in a good way.

13 Secondly, I don't agree that if you were to set
14 the kinds of safeguards that I have been describing, that
15 this would prevent experimentation with pilot EFT programs;
16 this is unlike the kinds of civil liberties demands in
17 which fast costs are mandated on systems.

18 For example, there were some proposals a few years
19 ago regarding privacy in government records such that before
20 any file was opened on an individual or any additional piece
21 of information was put into a file, there had to be a notice
22 sent to the individual to that effect. That would have been
23 a blizzard of paper, an environmental disaster, and no
24 real protection, I think, to the citizen. It would have been
25 a great breach of privacy as all those notices would have gone
out onto landladies' tables and wives opening husbands' notices

1 and husbands opening wives' and so forth.

2 What I have suggested is a cost
3 variable, almost cost-free approach to the question of
4 safeguarding every experiment toward EFT as it moves
5 forward.

6 If you really were to put to me the choice of
7 your closing remark, that is, to let the systems go ahead
8 without these protections versus not letting them go forward,
9 I would say don't let them go forward.

10 But I do that with the feeling that there is
11 nothing impractical or harmful to the working out of the
12 competitive questions and the financing questions, the
13 ownership and regulation questions in stating certain
14 basic rights of the individual and defining certain rights of
15 government access to that information for commercial use.

16 MS. KOPLow: Professor Westin, do you know of
17 any other type of development in economic transactions that
18 has had a code before it even got started?

19 DR. WESTIN: Yes.

20 Let me just say "yes" in this sense--not economic,
21 but the criminal justice information systems had first the
22 code drawn up by Project Search, an excellent LEAA-sponsored
23 user committee that drew up a code of safeguards for privacy
24 and security before there was any exchange of
25 criminal history information.

1 In many counties and cities I've examined
2 that are going into dated bank developments -- Santa Clara
3 County and Alameda County in California, just to name two --
4 there were codes of privacy and confidentiality that were
5 written before the first computer program started bending.

6 I think that is the way you deal with
7 this kind of large system data base. The reason is that
8 you must think the minute the switch gets pulled, you have
9 fast transfers of information taking place. Most important
10 of all I would suggest that if you have an array of computer
11 manufacturers or systems developers here today,
12 they would say to you that the best thing for the building
13 of a system is to develop such policies clearly, and let them
14 be the guides to the builders of the system.

15 What you recommend, I suggest, would be very,
16 very frightening to good systems developers because it would
17 say to them "build a system before you know what the rules
18 are for privacy, access, confidentiality," and that is
19 disastrous, because then you have to do what Dr. Ruth Davis
20 called "retrofit a system," which is extraordinarily
21 costly and I think very dangerous.

22 MS. KOPLOW: We have a system with the check
23 society which moves some regulation, but not with the kind of
24 code you are suggesting for this one. Is this so vastly
25 different from the check society?

1 DR. WESTIN: For the existing
2 check system we need the kind of bills I'm suggesting.
3 Mr. Marson will go into it in more detail from Congressional
4 legislation. I'm saying let's get the code for the present
5 system in place, then let's develop the new approaches for
6 more elaborate, faster transmission, larger data base
7 type system.

8 My approach is a very
9 graduated one, a Fabian approach to the issue, a
10 sense that you should not drop a regulatory bomb on systems
11 developers that puts them out of business. Quite the opposite.

12 If I can make one additional point, in my
13 testimony I mentioned the trouble that the Uniform Products
14 Code is having now for supermarkets.

15 To me that is a perfect example of the failure of
16 systems developers to have considered in advance the way the
17 consumers would want to have, at the shelf, the cost of
18 each item so they could make a decision when they were reaching
19 up for the can of asparagus or whatever; and also, the need
20 to have at the checkout stand some way of knowing
21 what the costs were that were mounting as the cash register
22 rang so you could exercise consumer choice there.

23 I have talked to many people involved in the
24 Uniform Products Code, and they say one of their greatest
25 mistakes was in not appreciating ahead of time the consumer

1 reaction to that system. they are paying dearly for it
2 in consumer resistance, and should, because they did not in
3 advance anticipate the desires of consumers to have more
4 control and choice in the payment system inside the
5 supermarket.

6 CHAIRMAN ATWATER: Professor Westin, I think you
7 generated a blizzard of written questions that are going to
8 be coming your way as a result of your testimony and the
9 questions that you have answered here.

10 We have time, I believe, for one more question
11 from Mr. Wegner, and then we will have to proceed to our
12 next witness.

13 MR. WEGNER: Mr. Chairman, we are overtime, and
14 I will yield and pick it up on another witness.

15 Thank you.

16 CHAIRMAN ATWATER: Thank you very much.

17 CHAIRMAN WIDNALL: I would just like to make this
18 statement for the record.

19 First of all, in connection with your testimony,
20 Professor Westin, is it your desire to have your complete
21 statement incorporated in the record?

22 DR. WESTIN: Yes, sir.

23 CHAIRMAN WIDNALL: That will be so ordered.

24 Would you
25 be willing to answer questions submitted after this hearing is

1 closed?

2 DR. WESTIN: Yes, sir, I would.

3 CHAIRMAN WIDNALL: All right.

4 That will be so ordered.

5 CHAIRMAN ATWATER: Thank you very much.

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

National Commission on Electronic Fund Transfers
Users Committee Public Hearings
"Consumers Issues in EFT"
October 26 and 27, 1976
Washington, D.C.

The documents which follow are submitted for the record
of this hearing by:

Alan F. Westin, Professor of Public Law
and Government
Columbia University

TESTIMONY OF ALAN F. WESTIN, PROFESSOR OF PUBLIC LAW AND
GOVERNMENT, COLUMBIA UNIVERSITY, before the National Commission
on Electronic Fund Transfers, October 26, 1976, Washington, D. C.

I am honored by your invitation to appear before the National Commission on Electronic Fund Transfers, to discuss the individual-rights aspects of EFT proposals.

I first began exploring this issue in the early 1960's, during a study of science and privacy that I was directing for the Association of the Bar of the City of New York.¹ My second major look at EFT came between 1969-1972, when I directed the National Academy of Sciences' Project on Computer Data Banks.² Your invitation to testify today provided me with the incentive to examine where EFT developments stand in 1976, and I am happy to share my thoughts on this with the Commission. In the interests of time, I will present these reactions briefly, trusting to the Commission and its staff to seek further elaboration of any themes that may particularly interest you.

1. Much has already been written about the potential problems of individual and associational privacy that would supposedly be presented by a comprehensive EFT system.³ Much of the public debate on this matter has seen the fanciful speculations of "total system" EFT enthusiasts met by equally fanciful (though horrified) reactions from civil libertarians.

For example, the enthusiasts project a national or regional EFT system in which almost all of an individual's income sources and recurring obligations would be deposited and automatically paid out of one central account held in a financial utility; a nationwide terminal system would allow immediate debits and credits to the individual's central account from locations across the country; and secure techniques for personal-identity verification would protect against fraud or misuse. This is presented as technologically feasible, increasingly necessary for our transaction-laden financial and consumer-purchase systems, and a socially-desirable innovation.

In reply, civil libertarians have condemned such EFT conceptions as an Orwellian delight. An EFT system of this kind would aggregate far more personal information than is presently collected by any single financial, retailing, or credit-reporting institution, or any existing multi-organizational network. The automated data base of individual accounts would allow managers of the system -- and anyone else allowed to use it or able to penetrate it unlawfully -- to accomplish unprecedented feats

1. See the discussion of "checkless, cashless society" proposals in Alan F. Westin, Privacy and Freedom (New York: Atheneum, 1967), pp. 163-168, 298-326.
2. The report of this project is Alan F. Westin and Michael A. Baker, Databanks in A Free Society (New York: Quadrangle Books, 1972). A further listing of this writer's work in the privacy field appears as an Appendix to this testimony.
3. Among the most extensive recent discussions are James B. Rule, Value Choices in Electronic Funds Transfer Policy (Washington, D.C.: Office of Telecommunications Policy, Executive Office of the President, 1975) and The Consequences of Electronic Funds Transfer: A Technology Assessment of Movement Toward A Less Cash/Less Check Society (Cambridge, Mass.: Arthur D. Little, 1975). The Rule essay is a thoughtful and sophisticated analysis, though one that I believe understates the "libertarian" position and does not recognize its larger commitment to egalitarian goals under a Bill-of-Rights aegis.

of surveillance: to locate individuals at a given moment, track their movements over time, develop profiles of their spending and saving habits, monitor whether their use of government or private funds met various regulatory or program requirements, identify their money-based political, religious, civic, or sexual affairs, and impose various controls over access to funds that could have enormous regulatory consequences for various economic and social groups in the population. Projecting these capabilities of a "Total System" EFT onto recent disclosures of the FBI's covert examination of the bank records of anti-war and black-protest groups in the late 1960s, the use of White House power over government files by Nixon and his lieutenants during their war on alleged subversives and "political enemies," and similar revelations about breaches of confidentiality from the Watergate-CIA-FBI probes of the past five years, civil libertarians have warned that proposals for developing such a "checkless, cashless society" are extraordinarily dangerous.

The way civil libertarians first reacted in the middle and late 1960s was, I submit, understandable and proper. Faced by the new technological power of computer and communications systems; the publication of "total system" EFT descriptions and proposals by experts from the business, computer, and government communities, usually without any serious discussion of privacy implications; and the seemingly irresistible momentum of the technological imperative ("if it can be done, it will be done") in the heady 1960s, civil libertarians were providing the necessary "negative" side of the social-forecasting debate -- asking how a socio-technological development of this magnitude might be misused.

Indeed, since I lust in my heart for privacy as much as the next civil libertarian, I wrote just such an analysis for Playboy Magazine in 1968, discussing where then-current proposals for a "cashless, checkless society" and a National Data Center might lead us unless we first strengthened our basic privacy laws.⁴

The trouble with the debate of the 1960s and early 1970s was that it was over a straw man. No "total system" EFT plan had any possibility of being installed then, nor within the 1970s, nor would I see it emerging in the 1980s or even the 1990s. Furthermore, even if we got a comprehensive EFT by the year 2000, it would probably bear little relationship to the kind of one-financial-utility, all-accounts-automated, totally-preauthorized-payments, "cashless" model that characterized much of the writings in the 1960s. One of the most important findings of the National Academy of Sciences' Project on Computer Data Banks⁵ was that there are enormous organizational, legal, competitive, social, and cost-effectiveness constraints on the adoption of "technologically possible" computer and communications systems. The "pure" technological solution is rarely the one that meets those constraints, and thus computer-system innovations in the organizational world almost always take longer and are adapted more fully to social-policy objectives. At the same time, our society has learned that our social policies as to individual rights and organizational duties in personal data must be made unmistakably clear and brought up-to-date before major new data systems are allowed to be installed.

Overall, then, the past decade of debate over "EFT and privacy" has had one quite useful consequence: it has started society toward a reconceptualization of the right to privacy that individuals should have in various bodies of sensitive financial data that will increasingly be contained in large-scale computerized data bases, and has sensitized systems-developers and organizational leaders working in the EFT field to

4. Alan F. Westin, "The Snooping Machine," Playboy, May, 1968, pp. 130-132, 152-157.

5. See note 2, supra.

the need for careful advance planning to respond to those policy considerations. The serious and costly difficulties now facing the participants in the Universal Products Code for supermarkets demonstrates vividly the results of a failure to anticipate the consumer's insistence that eye-readable prices be retained on every item at the shelf location, and that a satisfactory system for consumer review at the checkout station also be retained.

2. Unfortunately for this Commission's work, there is no official plan for an EFT to assess, whether from the federal Executive, Congress, or the business community. It's clear that we are already moving from our traditional financial transaction system (say of the 1950s) toward various less-check and less-cash arrangements. The growing use of bank cards and travel-and-entertainment cards; the automatic deposit of social security checks; and similar specific events are part of this pattern, as are a variety of local pilot projects experimenting with automated deposit of terminal input systems. There is also considerable agreement in the financial and governmental sectors that these moves will increase in the next few decades, some would say inexorably, as a result of high transactional volumes and costs, presumed business and governmental opportunities through new electronic technology, and satisfaction of assumed consumer desires.

If this Commission itself had formulated and endorsed a long-range plan for EFT, or was about to do so and had indicated the main lines of such a system, witnesses called to discuss the privacy implication of "EFT" would obviously have a specific proposal to examine. However, no such Commission plan has been issued, and my assumption is that this Commission will probably not formulate any such plan as part of its conclusion, essentially because it is still too early for such a "plan" to be adopted. Rather, I assume the Commission will analyze the varieties of EFT conceptions that are currently being discussed; assess the automated-payments experiments that have been and are being conducted; and report to Congress the range of economic, legal social, and civil-liberties problems that would be presented by various alternative EFT-oriented proposals.

On that assumption, my testimony concentrates on the key issues of transition. How should American society approach change from our existing financial payments system to various more-automated systems? Are there a set of ground rules and a monitoring process that will serve us well with specific automated payments projects in the next decade, and will also help us to be better prepared to make social-value decisions about the more-comprehensive EFT systems that may, at the end of another decade, be ready for serious consideration? I believe we can formulate such a set of rules and develop such a process, and that this Commission would make a tremendously valuable contribution if it spelled out such rules and procedures as a key recommendation for congressional action.

3. To develop those transitional rules and procedures, we need first to assess the current definitions and safeguards for individual privacy in the use of financial-transaction data. I submit that these are in serious disarray. The voluntary policies of banks, credit-card companies, and similar organizations are not satisfactory. Common law and statutory protections are not sufficient. Recent Supreme Court and lower court rulings on depositor privacy have not installed the necessary protections. Since I know that these points are being fully developed today in the testimony of Mr. Charles Marson of the ACLU of Northern California, I will not take the time to document these points in my remarks. My conclusion is this: unless Congress enacts new national laws that properly insure the privacy of account-holders in banks, credit cards, and various other retail or credit data pools, we will be moving into the next phase of EFT experiments with legal rules that do not spell out rights,

remedies, and monitoring procedures in a way that is critical for the proper design and operation of more automated information systems.

4. Beyond this critical first step lies the formulation of a new conception of the individual's right to control the profile of his/her financial transactions in new, multi-organizational data systems. Today, many commentators, especially those from the financial community, treat this new situation as only an extension of what various financial and commercial organizations now know about their customers; following this view, they suggest that all we need to do is to extend current policies, including current confidentiality policies by financial institutions; credit-card firms, retail establishments, and commercial reporting agencies.

I submit this is a fundamentally wrong and unwise approach. When personal information is merged from a variety of present sources (different kinds of banks, stores, employers and other income sources, Social Security, card-companies, etc.) not to make one-time decisions for specific purposes (such as credit, insurance, or employment decisions from commercial reports) but to create and maintain a permanent financial-transaction data base and network for an EFT system, then a new trustee relationship has been, or should be held to have been, created between the system managers and the individual account holder.

Under this conception, the data-rich profile of an individual residing in the EFT data base would be a valuable legal property belonging only to the individual account holder and not to "the system." The system managers should be allowed to make use of the information solely for the express purposes of the funds transfer process, and its necessary monitoring for security, audit, and other protective purposes. However, any commercial or other gainful use of an individual's transactional history represents the taking of a valuable property right for which both compensation and consent are required.

There may be some who see advocacy of such a property right in personal information as a retrogression in American law, harkening back to the days of liberty-of-contract and substantive due process in the constitutional jurisprudence of 1890-1937. While I am not foregoing for an instant the defense of privacy rights that rests on personal liberty grounds (e.g., First and Fourth Amendment bases) or on positive legislation such as the Federal Privacy Act of 1974 and its counterpart in seven states, I am convinced that a property-based approach is also vital if we are to develop a coherent protection of the privacy rights of individuals as consumers in an increasingly data-rich commercial civilization.⁶

Today, American law is steadily writing into statutes or regulatory rules that personal information given to organizations (both governmental and private) for an express purpose, reflecting an information bargain between individual and organization, cannot be used for additional purposes not within the original agreement unless the later consent of the individual is obtained or it is mandated by law (and within the limits of the original transaction). This is true with medical records, educational records, credit-insurance-and-employment reporting by commercial agencies, and many other areas. When we therefore contemplate the kind of master file that a broad EFT plan would create, even far short of the Year-2000 type systems, I submit we should treat this as a new and concretely valuable collection of sensitive, personal data. It ought not to be thought in any way to become the property of the EFT system, able to be sold by them to business advertisers, political candidates, religious groups, civic causes, magazines, or Fruit-of-the-Month clubs without the say-so of the financial account holder.

6. See Privacy and Freedom, note 1 supra, pp. 330-364.

What would follow from this approach is that every account holder would have to be offered options by the EFT system as to any additional uses made of his/her data. A check-off system could be created, whenever an individual opened the account, which offered various options. One is that data should never be provided to anyone. Another is that data could be provided for all uses checked off on a list, and at so much compensation directly to the individual for such use. Still another option might be a blanket permission for marketing and solicitation uses, at a particularly high rate of payment for giving such permission. The beauty of computer systems is that such a privacy-respecting check-off system, installed at the outset and revised periodically, would be eminently feasible as a technological matter. The privacy of those who want no additional commercial, charitable, or other uses made of their data could be respected while a specific payment per use could be automatically credited to the individual's account whenever each authorized use was made.

One can anticipate cries of outrage from some members of the direct mail industry, who have been buying and selling our personal profiles for decades without our getting a cent for it. But the age of clean air and water as economic "free goods" is over, and so ought to be the age of free commercial use of our personal profiles. In a market economy, any scarce commodity that buyers want becomes an object of value, sold on contract terms. The sooner American consumers wake up to the fact that amassed personal facts about them are becoming the necessary currency of marketing in our economy, the sooner we will have a new and more humanistic exchange theory of value for the electronic age.

So far, I have been addressing the disposition of account-holder data for private, commercial purposes other than management of the EFT system itself. Equally if not more important will be the issues of what access government authorities would have to the system, in a range of entries starting from minimum regulatory-agency oversight to insure the integrity of the system and its security all the way, at the other extreme, to a general right to access the system for criminal investigations, legislative inquiries, civil process, regulatory program enforcement, or internal security programs.

Logically, one can hypothesize three basic answers to this question: (1) no access whatever for any governmental purpose; (2) access for whatever purposes would today allow entry to individual financial records, and under present safeguards; and (3) an intermediate policy of specifically-limited entries under express conditions and procedures.

Option 1 I think is unrealistic and probably unwise. Unlike the immunity our society bestows by law or by practice on a handful of informational resources (psychiatric-incident registers, priest-penitent confidences, etc.), I cannot believe that financial accounts in an EFT-type data-base ought to have such wholesale immunity.

Option 2 is equally unpersuasive, given my already expressed position that our current law of financial privacy is dangerously outdated and weak.

This leaves option 3, whose evaluation obviously depends on an elaboration of what "specifically limited entries and express conditions and procedures" would mean. For me, this would mean the following kinds of rules:

(a) Any law enforcement inquiry that involved inspection of EFT records directly related to First-Amendment-protected activity -- religion, press, speech, and assembly, and especially records of private associations -- would be presumptively improper. A special judicial warrant system would pass on proof of probable cause, and probe whether there was another investigative technique that might be used instead with less harmful impact on personal rights (as the Omnibus Crime Control Act of 1968 now does with regard to wiretapping and electronic eavesdropping). No general searches of the EFT data base for possible "hits" on lists of "suspected persons" should be allowed, on the theory that these would be equivalent to the general warrants forbidden by the Fourth Amendment in the pre-computer era.

(b) Before any automated payment from a government social-benefit program was included in an EFT system, the legislature ought to require that a privacy-impact statement be drawn up and presented by the executive agency involved (state or federal) indicating any techniques of enforcement using the rest of the EFT system that were proposed (collation of payments with other program payments, seeking location information on delinquent program participants, etc.). This ought to be subject to a public-notice proceeding at which various private groups could appear and testify on the issue of whether those enforcement techniques were too violative of the overall confidentiality pledges of the EFT system. If a national EFT system were authorized by Congress at some point in the future, there should be language of a declaratory character mandating the protection of privacy and confidentiality interests of the individual and rights of individual access to all information contained in his/her file and to an audit record of all uses made of it. This language would become the standard that courts could use in reviewing the fidelity of later additions to the EFT system and uses of its data, with judicial power to entertain class action as well as individual law suits and to hold both legislative and administrative declared policy of the EFT system.

(c) While we do not know what shape a future EFT-type system would take, it is not too soon to start thinking about the kinds of institutional arrangements our society might require to be appended to local or regional pilot programs that are being developed or early national experiments. I think a searching public-notice proceeding before a national or state regulatory commission ought to be required before an EFT-type system is initiated, with the commission specifically charged to consider individual-rights safeguards in its decision about the acceptability of the proposal. In addition, if a national EFT-type system were attempted, a board of overseers with private as well as public members should be created to monitor the rules and operation of the system continuously, including specifically its individual rights practices, and to report to Congress annually on the way such practices were being observed, the need for additional protections, etc.

5. To sum up, I have assumed that the next several decades will see the gradual development of various forms of less-cash, less-check payments mechanisms, but not the "total system" plan of the comprehensive, automatic, one-big-utility variety. At what stage partial payments systems on a local or regional basis, or national payments programs for specific income purposes (like Social Security checks) will be deliberately merged into a single national payments system I cannot predict, but I doubt whether this will come within the next 10-15 years.

Therefore, I see the Commission's key contribution on the individual-rights issues to be:

- A. Recommending to Congress that it deal now with the serious problems of privacy in bank and credit-card records that need redress, before we go any further to more comprehensive financial transaction systems.
- B. Recommending that on-going pilot programs of automated financial transactions formulate clear rules of individual rights and protective procedures of the type discussed in this testimony, as applied to the specific contexts of those experiments.
- C. Recommending that Congress create the oversight commission of private and public members, the public-notice proceedings, the declaratory standards, and the protective procedures mentioned earlier at the point, if we reach it, at which a national EFT-type system is created.

If we pass through the next decade or two under such controlled-experiment conditions, American society will then be in a good position to assess any plans that may be offered for a comprehensive national EFT system, and to judge whether such a plan would be a privacy-respecting boon to American enterprise or a dangerously Orwellian step. As I see it, this Commission's role -- and that of the Privacy Protection Study Commission, which is also looking into EFT -- is to help American society, at this very early stage in consideration of EFT prospects, assess the problems and the opportunities that lie immediately ahead.

PRIVACY ACTIVITIES
OF
ALAN F. WESTIN

Alan F. Westin is Professor of Public Law and Government at Columbia University in New York City. Born in 1929, he earned his Bachelor's Degree at the University of Florida, his law degree from Harvard Law School, and his doctorate in political science at Harvard University.

During the past two decades, he has specialized in writing about the impact of technology on organizations, citizens and society. His book, Privacy and Freedom (1967), was a comprehensive study of the social and political functions that privacy serves in democratic societies and the dangers to privacy posed by advances in physical, psychological, and data surveillance.

Between 1967 and 1973, he conducted studies on the impact of information-technology on government programs, planning, and decision-making, as an Associate of the Harvard University Program on Technology and Society. His book, Information Technology in a Democracy (1971), was developed from those studies. A second volume, based on the use of information technology at the local governmental level in the United States, Britain, and selected Western European nations, is presently being completed. In January of 1975, he delivered a paper on another aspect of these studies, "Technology and Citizen Participation: The Politics of Feedback," at the annual meeting of the American Association for the Advancement of Science; as well as the Keynote Address at the Association of Computing Machinery's 1975 Convention, on "Twenty Years of the Computer Revolution: of Privacy, Participation, and Power." He has also been concerned about the public's right of access to information in government's computerized files, and published a study of compliance with freedom of information laws by federal agencies using EDP, in "The Technology of Secrecy," in None of Your Business: Government Secrecy in America, edited by Norman Dorsen and Stephen Gillers, (Viking Press, 1974).

From 1969 to 1972, he was director of the Project on Computer Databanks of the National Academy of Sciences, a three year study of the effects of computerization on organizational record-keeping and civil liberties. The report of that project, Databanks in a Free Society, was published in 1972.

In 1973, with David Martin and Daniel Lufkin, he prepared a report on The Impact of Computer-Based Information Systems on Civil Liberties in the Advanced Industrial Nations, for the German Marshall Fund of the United States.

During the past decade, he has served as a consultant on privacy to a wide range of organizations, such as the New York State Identification and Intelligence System and the IBM Corporation. He also served as chairman of the Privacy Committee of the American Civil Liberties Union, and gave expert testimony before the major committees of the United States Congress dealing with issues of wiretapping, computers, and other privacy issues. In 1974, he was a principal consultant to the Senate Committee on Government Operations, under Senator Sam Ervin, Jr., in drafting the Senate bill that was ultimately enacted as the Federal Privacy Act of 1974.

In 1973, he was appointed by the President of the United States to the National Wiretapping Commission, a 15 member body set up to review federal and state wiretapping practices. The Commission's report to Congress was issued in 1976 and Professor Westin wrote a dissent from the majority's recommendation in favor of increased legalized wiretapping.

He has been for several years a consultant to the United Nations' Commission on Human Rights, in its on-going studies and reports on technological threats to Human Rights, and he has participated actively as a commentator and contributor of papers to the OECD's Computer Utilization Group's work on data banks and privacy. The most recent of these is his chapter, "Entering the Era of Databank Regulation and How We Got There," in Policy Issues in Data Protection and Privacy: Concepts and Perspectives, OECD Informatics Studies (1976).

In 1976, he completed a study for the United States National Bureau of Standards (NBS) on the policy issues for citizen rights involved in automation of medical and health-care records in the United States; the study's report, Computers, Health Records, and Citizen Rights, will be published soon by NBS. He is presently a consultant to the Privacy Protection Study Commission, and is conducting another study for NBS on citizen rights issues in the personnel data systems of government, business, and civic organizations.



United States
of America

Congressional Record

10

41K

PROCEEDINGS AND DEBATES OF THE 93^d CONGRESS, SECOND SESSION

Vol. 120

WASHINGTON, TUESDAY, DECEMBER 17, 1974

No. 177

Senate

S 21855

TRIBUTE TO PROF. ALAN F. WESTIN'S WORK ON PRIVACY

Mr. ERVIN. Mr. President, it is no secret that Congress would have a difficult time legislating on the many complex questions facing the country without the help of the knowledgeable witnesses and expert consultants who lend their time, energies, talents, and resources to individual members and committee staffs.

One such person who has served Congress well in this way is Prof. Alan F. Westin, professor of public law and government at Columbia University in New York City, a lawyer and a legal scholar. Professor Westin recently served as special consultant to the Senate Government Operations Committee during its consideration of S. 3413. This is the bill recently passed by the Senate to protect privacy and provide standards for governmental use of computer technology in records management.

Professor Westin is one of the wisest people I know on this subject. He has probably written and spoken more on privacy and advised more public and private groups on it than anyone in the country. I have found particularly useful his work "Privacy and Freedom," done for the Association of the Bar of the City of New York and his report, "Databanks in a Free Society," resulting from his study for the National Academy of Sciences.

We were fortunate to receive the benefit of his knowledge of this subject as director of numerous private and governmental studies. His testimony in June of this year provided the Government Operations Subcommittee on Privacy and Information Systems and the Judiciary Subcommittee on Constitutional Rights with wise and expert counsel on the desirable policy approach for this legislation in S. 3413. As a consultant, his legal and detailed technical advice to the subcommittee staff was invaluable in helping the committee report a workable, acceptable bill. As a political scientist and as a scholar in many fields, Professor Westin brings to his work a wise understanding of the workings of government.

His counsel to Congress on privacy and other civil liberties matters is not confined to this instance. When I first became chairman of the Constitutional Rights Subcommittee, he rendered service in research and testimony as a consultant to the subcommittee during its study of wiretapping and eavesdropping legislation. Through the years, he has testified before and advised many Senate and House committees as well as the Constitutional Rights Subcommittee, on privacy, due process, civil liberties, freedom of information and computers and data banks.

I wish to acknowledge Professor Westin's valuable contribution to our investigative and legislative endeavors on privacy and to pay tribute to his long dedicated service to Congress and the public on this issue.

Columbia University in the City of New York | New York, N. Y. 10027

DEPARTMENT OF POLITICAL SCIENCE

420 West 118th Street

January 27, 1977

Dear Chairman Widnall:

In answer to the query put to me about my testimony, if a person received direct mail that he or she thought had been sent through improper disclosure of the person's name, address, and characteristics from an EFT account, I would (as this is what the Privacy Commission will probably recommend also) require any/direct mail firm had supplied the name. Then, I would require the direct mail firm to indicate where they had obtained the name. By putting these duties of audit-trail response on the mailer and direct mail firms, it should then be possible to learn whether an EFT had released the data improperly. Similarly, I would give the EFT management the duty to keep records of the disclosures made from an EFT account for direct mail purposes (a revenue trail would be required anyway for billing purposes, identifying the direct mail user) and this would give any account holder the ability to have the EFT management document and account for any disclosures.

I hope this answers the question, and please call on me if there is anything else from my testimony about which additional comment is needed.

Sincerely,


Alan F. Westin

1 CHAIRMAN WIDNALL: The next witness is Mr. Earl
2 Ward, President of AFS Associates, speaking on behalf of the
3 Independent Bankers Association.

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 (Witness sworn.)

2 TESTIMONY OF EARL WARD, PRESIDENT,
3 AFS ASSOCIATES, CINCINNATI, OHIO.

4 MR. WARD: Chairman Widnall, members of the
5 Commission, my name is Earl Ward. I am President of AFS
6 Associates of Cincinnati, Ohio, a firm specializing in
7 banking systems, automation and equipment.

8 During a period of six years, from 1969 to 1975, I was
9 responsible for the conception, partly responsible for the invention,
10 and responsible for the invention and marketing of the first
11 automated teller.

12 In 1975, I left the Mosler Safe company to form AFS, to
13 invent what I thought was needed and still is needed in
14 banking automation.

15 I'm here because, first, I think there are serious
16 security problems in existing financial automated equipment
17 which would be magnified in an EFT system.

18 Security, incidentally, I define not only as
19 consumer losses, but potential losses to host banks of the
20 system and correspondent banks in a connecting network.

21 Second, I am here to emphasize the awesome power
22 of those having control of the computer with access to huge
23 amounts of financial data.

24 Third, I would like to stress that the recent past has
25 shown an inability or an unwillingness of some of the industry,

1 that is, vendors and purchasers, to plug the security holes
2 in existing equipment. And barring regulation, I have little
3 hope that all will do so prior to entering an EFT environment.

4 Finally, I'm concerned about the proposed
5 network's ability to even detect frauds and about the
6 harassment consumers will undergo prior to ascertaining those
7 frauds.

8 Earlier this month, 60 Minutes featured a
9 purported million dollar embezzler, Jerry Schneider, who,
10 from his own home in California, telephoned Dan Rather's bank
11 in New York, entered the bank's system and raised Rather's credit
12 from \$500 to \$10,000. He then quickly lowered it again.
13 Neither transaction was detected as fraudulent.

14 During the same program, Stanford Research
15 Institute's Don Parker reported that the average bank fraud
16 during 1974 was \$19,000, but that the average detected
17 computer-related bank fraud in the same period was just under a
18 half million dollars.

19 The point is, the more automated the system, the
20 easier it is to steal large sums undetected.

21 In another interview, Parker reported that hardly
22 any cases of computer crimes were discovered through normal
23 security precautions or accounting controls, and nearly all
24 were discovered by happenstance.

25 Some experts have estimated that the ratio of

1 undiscovered to discovered computer crimes may be on the
2 order of 100 to 1.

3 The examples I have talked about are crimes
4 committed against a closed system, that is, one where a single
5 bank has security oversight over an entire system. But the
6 proposed EFT networks would consist not only of many financial
7 institutions sharing the same security oversight, but the
8 system would extend to every terminal on and off the premises.

9 These systems' overall security would be only
10 as strong as the weakest terminal in the weakest bank system
11 of that network.

12 Now, would vendors allow and financial institutions
13 accept such risks? Judging from the past few years, I think
14 they might.

15 In my testimony before the Comptroller of the
16 Currency last year, I described the poor security in existing
17 automatic teller systems.

18 Because no party can define security standards,
19 installed ATMs could and still can be defeated.

20 In tests that I am aware of, one ATM was defeated
21 in a few hours, one in about 30 minutes, and a third in about
22 6 minutes.

23 And incidentally, they were machines all of
24 different manufacture.

25 Existing systems are vulnerable in at least three

1 areas. One, the magnetic striped card can be easily changed
2 or duplicated. Two, they identify the card owner using the
3 memory number of the person, the PIN or Personal Identity
4 Number, which can be easily removed from the legitimate owner.
5 Now, that's a serious problem. Three, they depend upon cryptology
6 for systems security, yet were designed by systems people
7 with no cryptology background, and I include myself as one of
8 those.

9 The proposed EFT networks would retain all three of
10 those weaknesses.

11 The magnetic striped card is required for off-line
12 automatic teller systems because it must be changed during
13 each transaction, and the magnetic media is the only way that
14 they found to change the records on the card to record as cash
15 that is withdrawn from the machines.

16 The data in an off-line automatic teller system --
17 the data bank-- is actually being carried around from terminal
18 to terminal in the customer's pocket. It is not centrally
19 located in the bank.

20 Off-line ATMs are simply incompatible with the EFT
21 networks, and that has been fairly well recognized. Therefore,
22 the magnetic stripe is not really required.

23 Incidentally, it should be remembered that because
24 EFT networks will be on-line, their reliability as opposed to
25 their security is only as good as the phone lines connecting

1 them, and the computers controlling them, so there is a
2 reliability problem here which we haven't really gotten into.

3 As for the PIN again, numerous attempts have been
4 made to find a physical identification which would be as good
5 as the signature and which would require the physical presence
6 of the customer.

7 At Mosler, we attempted to develop the system as
8 early as 1968. To my knowledge, no reliable economic
9 alternative to the PIN has been found. The PIN remains a
10 dangerous cornerstone on which to construct an EFT system.

11 Then there's the problem of cryptology. Whether
12 PINs are generated by a scrambler using information written
13 on the card unscrambling them to generate the number,

14 or whether the PINs are scrambled and sent
15 over phone lines to the host computer to be compared with the
16 clear scrambled PIN in the central data bank,

17 there must be a secret coding
18 device at the point of each transaction.

19 That is a security problem. Defeating
20 the security device of one terminal could conceivably penetrate
21 the entire system.

22 As systems expand from single to multiple
23 institutions, and as they further expand to thousands of
24 terminals, the number of people having access to the system,
25 insiders and outsiders, expands exponentially, and so does the

1 risk.

2 Who would blame an initiator of an EFTS from refusing
entry of a competitor on the basis of security? And yet, who is
4 to say whether such reluctance is actually caused by concern
5 with lessening security or lessening of market advantage?

6 On-line networks demand that charges be made to
7 and monies be withdrawn from established accounts, the
8 accounts located in the central data bank. These accounts
9 can be either legitimate or fraudulent accounts, established
10 specifically to support the particular crime.

11 If the fraud is directed against legitimate
12 accounts, the first indication that the bank may be in trouble
13 is the customer saying, "Hey, I did not do that. I did not
14 make that transaction."

15 There is no signature now, only the Personal
16 Identification Number. How long must a customer protest before
17 the bank realizes that it is a fraudulent transaction, and
18 what can the customer do about it? How many of us have
19 attempted to change a mistake on a credit card computerized
20 bill and not experienced the frustration that results?

21

22

23

24

25

1 And what happens when there are more than two
2 parties involved? Who is responsible for fraud, once detected,
3 committed on the account of a customer of Bank A at a terminal
4 of Bank B, when the break in the security allowing the fraud
5 may have been in any number of Banks C?

6 The other side of the coin has been alluded to
7 by Ron Osterberg in his excellent new study, "Security, Privacy
8 and Accuracy in EFT Networks," and I would like to quote a
9 couple of paragraphs from that study.

10 "Often neglected by security experts, system
11 accuracy can have a significant impact on fraud losses. A
12 classic illustration of this occurred over a decade ago
13 when the Illinois Central Railroad installed an automatic
14 fare collection system. As designed, tickets were purchased
15 for a specific number of rides encoded on the card, and with
16 each use the number of rides remaining was decremented by one.

17 "Unfortunately, the system reliability was so
18 atrocious that, for reasons of public relations, complaining
19 customers were automatically issued replacement tickets when
20 the original ones failed to work.

21 "However, as the operating reliability was slowly
22 improved, the number of tickets which were returned
23 unexpectedly remained constant or increased. Not until the
24 system users were put on notice that return tickets would be
25 tested did the number dropped, and then it dropped to less than

1 five percent of previous levels.

2 "The lessons here" — and I'm still quoting — "The
3 lessons here for financial institutions are clear. Without
4 adequate measures of safeguarding transaction data, journals
5 with no customer signatures may be challenged, and a system
6 which occasionally posts a transaction to the wrong account
7 may find many times as many false claims of no transactions."

8 Now, some will argue that there have been few
9 crimes reported against existing ATM systems, and some may
10 conclude that, therefore, they, in the proposed EFT systems,
11 will be secure enough.

12 The low incidence of reported attacks against
13 installed systems may be due to a number of factors: the
14 newness of the industry, the relatively small number of ATMs
15 installed, the relatively few insiders with the knowledge
16 to easily defeat the system, and possibly the understandable
17 reluctance of the institutions to reveal the attacks.

18 Certainly, with time, there is a danger that
19 the attack against these electronic symbols of the
20 establishment would become a fad such as were the attacks
21 against the telephone company's long distance lines.

22 There are instances in my prepared testimony which
23 support the hypothesis that they may already be becoming
24 popular.

25 Rather's 60 Minutes article was viewed by 25 million

1 people. Therefore, at least 25 million people have been
2 made aware of the potential of this crime and the procedures
3 to go about committing it.

4 CHAIRMAN ATWATER: Mr. Ward, would you object, in
5 view of the fact that we have had the benefit of reviewing your
6 written testimony before this
7 meeting, to responding to questions
8 from the Commissioners at this time?

9 MR. WARD: Yes, sir.

10 I just have one more paragraph, if I might
11 conclude.

12 CHAIRMAN ATWATER: Fine.

13 MR. WARD: I strongly believe that the financial
14 institutions should proceed cautiously towards EFTS with
15 thorough security analyses as part of the architecture.

16 I also feel that the consumer, in the entire payment
17 system, must be protected now from the results that could
18 occur should they not do so.

19 CHAIRMAN ATWATER: Mr. Tangney.

20 MR. TANGNEY: There is a basic
21 rule in banking that the bank is responsible for its
22 depositors and can only dispose of funds as the customer so
23 directs.

24 That law is long-standing in banking,
25 and banks have always assumed the risks.

1 Why do you think that EFTS, with that basic
2 rule that we can only do what our customers tell us to do,
3 will change that rule? You talk about fraud, but you
4 know, all fraud in banks must be reported to the FBI if you
5 are a member of the FDIC or a national bank.

6 You indicated or hinted that these frauds were being held
7 under secret cover, and they are public knowledge.

8 MR. WARD: I intended to express my concern that
9 banks are understandably unwilling to make
10 public embezzlements and crimes, or even attempts, attacks,
11 unsuccessful crimes, and I do not know
12 if there is a significant number of attempts against these
13 automatic teller machines.

14 CHAIRMAN ATWATER: Mr. Rogers.

15 MR. ROGERS: Yes.

16 I'm sort of curious just what your specific
17 recommendations are to the Commission regarding the problems
18 you've outlined.

19 For example, the Bank Protection Act requires
20 the federal banking regulatory agencies to publish the
21 regulations regarding reasonable cost procedures for
22 banks to follow for the prevention of fraud or embezzlement.

23 Are you suggesting that that legislation is
24 inadequate or further legislation is needed, or specifically
25 what are your recommendations?

1 MR. WARD: My recommendations are to the
2 industry -- in other words, to the equipment suppliers -- and
3 to the financial institutions as well as to the regulatory
4 agencies.

5 I think that to date there has been demonstrated
6 no willingness -- perhaps because there has not been a
7 substantial attack by the criminal element -- there has
8 been no move toward providing the security that I feel is
9 going to be necessary, that is necessary now.

10 I think that it is incumbent on the industry to
11 go about developing the security required, and I think for
12 the protection of the consumer and the entire financial
13 system, the payment system itself, I think it is incumbent
14 on the government to develop enough sophistication and
15 enough regulations that they make sure that the industry
16 does provide these protections.

17 I have not seen these protections being provided
18 yet, and the bank protection industry or the Bank Protection
19 Act does not do it. The Bank Protection Act concerns itself
20 primarily with physical attacks.

21 CHAIRMAN ATWATER: Are there other questions by the
22 Commissioners?

23 (No response.)

24 CHAIRMAN ATWATER: I think the concluding question
25 might be related to Mr. Rogers' comment. To some extent it

1 seems to me that the interesting detail in which you have
2 outlined exposure of the system and your reference to the
3 60 Minutes program still leave unanswered the general question
4 of what kind of security policies might be proposed. Is
5 legislation appropriate for this problem, or is some other
6 answer necessary?

7 I think one answer might be that the
8 competitor pressures by the institutions involved are going
9 to be great to prevent loss to them should these systems
10 prove to be inadequate against the kind of security breakdown
11 that you are proposing here.

12 So as a Commission we are looking for some general
13 approaches that might strengthen the security of the
14 systems and protect the consumer.

15 You are suggesting that the protection of the
16 consumer by limiting his risks--which, I think, is what has
17 generally been done through credit and other policies--
18 will not be really adequate because the system itself might
19 be so seriously hurt that we would have other risks to the
20 consumers than those we are now talking about.

21 But if you do have any suggestions, we would be
22 very pleased to receive them, perhaps following the hearings.

23 MR. WARD: I would be very happy to do so.

24 CHAIRMAN ATWATER: Are there any other questions
25 by the Commissioners?

(No response.)

CHAIRMAN ATWATER: We thank you very much, Mr. Ward.

National Commission on Electronic Fund Transfers
Users Committee Public Hearings
"Consumers Issues in EFT"
October 26 and 27, 1976
Washington, D.C.

The documents which follow are submitted for the record
of this hearing by:

Earl Ward of AFS Associates, representing
Independent Bankers Association of America

BEFORE THE
NATIONAL COMMISSION ON ELECTRONIC FUND TRANSFERS
Washington, D.C. October 26, 1976

Statement of Earl Ward, President
AFS Associates
Cincinnati, Ohio

My name is Earl Ward. I am President of AFS Associates, specializing in banking automation.

A detailed account of my experience in the field of EFT is contained on pages 1 and 2 of my Statement before the Comptroller of the Currency on April 3, 1975, which is attached hereto and is submitted as a part of my testimony in these hearings. (Your attention is directed to "Security Considerations" on pages 6 through 9). In addition, I have attached my Follow-up to that testimony and it too is submitted as a part of my testimony in these hearings.

In the Commission's Notice for hearings, you have stated that you "will explore issues relevant to the interests of the consumer in the development of electronic fund transfer systems (EFTS)." One of the specific areas set out to be investigated at these Hearings is "security from error and fraudulent use." Yet, in detailing the above, the Notice narrows the definition of security and restricts the questions in this area beyond what, I believe, is reasonable and practical for an adequate consideration of consumer concerns related to this subject.

Security cannot be "broadly defined as the prevention of either the unauthorized disclosure, destruction or modification of financial data that results in a loss to the consumer." Security must also be concerned with currency (non-data) and direct losses to the financial institution, which only in the

- 2 -

long-run impact the consumer. Also, the concern of the consumer rests equally, if not greater, in the financial institution's ability to detect fraudulent activity in the consumer's financial accounts so that the consumer is not hassled by the result.

I will not address the questions of liability or legislation; I am neither a lawyer nor experienced with bank customer relations. I will discuss some developments in the area of security with which all of us involved with EFT must be concerned in order to allay the consumers' legitimate concerns whenever cash and/or checks are replaced by an EFT transaction.

Earlier this month CBS's "60 minutes" did a television article on computer bank fraud. (A copy of the text is attached). In that piece Dan Rather interviewed Mr. Jerry Schnieder, a convicted computer thief, now a consultant, whose "crime was to steal perhaps as much as a million dollars, from the telephone company, through their computer."^{1/} In a sensational demonstration of the vulnerability of a modern bank's computer system Schneider used his home telephone to raise Rather's credit limit from \$500 to \$10,000.

In the same program, Donn Parker of S.R.I. told Rather that the average computer-related bank fraud in 1974 was just under five hundred thousand dollars, whereas the average non-computer related bank fraud was just nineteen thousand dollars. The next day banks

^{1/} CBS News: Transcript, Dial E for Embezzlement, p. 2

across the country received thousands of telephone calls from concerned customers. They should be concerned.

In another interview, Parker "concluded that hardly any [recorded cases of computer crime] were discovered through normal security precautions or accounting controls and that nearly all of them were uncovered by happenstance. Some experts estimate that the ratio of undiscovered to discovered crimes may be in the order of 100 to 1."^{2/}

I too am concerned. The computer room security problem in a single bank is itself significant. Allowing that system to be accessed by the public using unattended Automated Teller Machines ("ATMs") opens the transfer system to many more security hazards than would otherwise exist. Let me explain.

Automated Teller Machines today are activated by an encoded card and a Personal Identification Number. It has been demonstrated that reproducing magnetic cards, "skimming," is no great feat. Off-line ATMs - and most are off-line all or part of the day - protect themselves against skimming by "remembering" the last X number of transactions. If a duplicate card appears within the span of the ATM's memory, ("X") the card is captured. Naturally, the length of the memories of the various ATMs is a guarded secret, for an off-line ATM with a memory of X can be emptied with duplicate sets of X+1 card/P.I.N. combinations. Some installed ATMs have memories several hundred transactions long. Since testifying before the Comptroller of the Currency, I have learned that some others have no memory at all! In that

2/

Schuck, Electronic Funds Transfer: A Technology in Search of Market
35 Maryland L. Rev. 74, at 83, (1975), citing Porter, Computer
Raped by Telephone, N.Y. Times, Sept. 8, 1974 (Magazine), at 34

case, just one card/P.I.N. combination could relieve each ATM of its cash. Such a situation should be proscribed through appropriate standards.

If an attacker has access to cards and correct P.I.N.'s, he can obtain ATM cash at will. Where does he get the sets? "Insiders," employees of certain financial institutions, of merchants, or of ATM manufactures can collect the needed data during their normal work routines. Card writers are available on the open market.

But the attacker need not be an insider. For fifty cents he can purchase a copy of a patent describing the concept of writing the card and of generating the P.I.N. Next he can buy, steal, or have stolen the needed materials and equipment. Then it's a matter of solving puzzles.

Some designers of existing ATMs have made a logical error in designing encrypting devices. They have defended against only obvious attacks. For example, it would take years of calculations and hundreds of thousands of samples to try to deductively solve a card/PIN equation. Yet, when test teams "attacked" an entire system, one was successful in six hours, the second in 30 minutes.

The frontal attack is well-defended while obvious alternate methods are often left open. This problem is not new to banking. For example:

"The employee who hit the repeat button on the [computer] printer and caused multiple copies of his legitimately prepared pay check to be printed." 3/

Or the case where the branch banks were connected to a central station via a high line security alarm system designed to foil anyone attempting to record the signals then play them back while the line was cut. The burglars simply bombed the control station, knocking out the entire system then burgled the branch.

The PIN system is just as unsatisfactory for on-line-only systems especially if they are to be connected in a nation wide EFT network. Either all banks must have access to a PIN generator or encryptor or the PIN must be decoded as it leaves one bank system and enters another. And the fundamental weakness of the PIN remains: it can be separated from the legitimate owner.

Bankers with experience in ATM systems are aware of many of the problems.

"Some bank auditors, security specialists, data research analysts and regulators are questioning whether the plastic card - called the most inexpensive means available today for identifying and activating electronic funds transfer transactions - will prove too vulnerable an instrument to adequately protect all the users and applications involved in the operational aspects of an electronic environment.

3/

Nycum, Computer Abuses Raise New Legal Problems, (April, 1975). 61 A.B.A.J. 444, at 446.

- 6 -

"John F. King, research systems analyst at Continental Illinois, the states' largest bank, said, '...Continental Illinois devised a scramble system for PIN numbers and an in-house binary keyed access method for account numbers which the systems analyst said was hard to get into but not impossible. 'No matter what can be done to a piece of plastic, decoding is conceivable, Mr. King noted.

* * *

"Although the customer's PIN is not on the card and is accessed in-house only through a master file, the auditor still does not like it because the PIN can be penetrated, Mr. King noted....

* * *

"Penetration of PINs and fraud can occur accidentally because of software problems, the analyst continued. He told the bankers of a Continental Illinois customer who brought in her statement showing a deposit she said she had made but also an immediate withdrawal of the same amount, 'after checking, we found the software had an opening which could be triggered by software on another machine.'" 4/

Telecommunication and the related I/O devices have expanded the area of the "computer room" to anywhere and everywhere a terminal (including a telephone) with access to the computer is located. Locks and limited-access devices protect the computer. Only software protects the data it contains.

As the networks connect to form multi-institutional EFTS, the number of P.I.N. generators, host computers, and personnel with

4/

Hansen, Security Specialists Hunt Ways to Plug Openings for Fraud Against EFT Card Users, American Banker, October 19, 1976, p. 1.

access to the system hardware and software expand exponentially-- and so does the risk.

The PIN/CARD SYSTEM can be defeated and therefore is a weak and dangerous cornerstone on which to build an EFT system.

If ATMs are to part of an EFT system they must have a better method of personal identification. To my knowledge, no economical alternative yet exists, but perhaps the price tag is necessarily high.

Attempts have been made during the past ten years to find a reliable, economic, physical identification of customers. Holograms of fingerprints, mechanical recognition of signatures, voiceprints, finger lengths, and other devices have been tried but have been found to be either too expensive, or not reliable enough for the application. (Unlike most other tests which require either a low incidence of accepting a wrong sample or of rejecting a correct one, this system requires very low incidences of both!). Absent a completely new approach, improved technology in one or more of these areas is necessarily the answer.

DETECTING a fraud is another problem with memory numbers. The customer claims he made no transaction. Does the bank give him the benefit of a doubt? If so, it may be placing itself into a situation like one described by Ron Osterberg in his excellent study, Security, Privacy, and Accuracy in EFT Networks.^{5/}

^{5/} U.S.S. & L. League, April, 1976, p. 13.

"Often neglected by security experts, system accuracy can have a significant impact on fraud losses. A classic illustration of this occurred over a decade ago when the Illinois Central Railroad installed an automatic fare collection system. As designed, tickets were purchased with a specific number of rides encoded on the card and with each use the rides remaining field was decremented by one. Unfortunately, the system reliability was so atrocious that, for reasons of public relations, complaining customers were automatically issued replacement tickets when the original ones failed to work. However, as the operating reliability was slowly improved, the number of tickets which were returned unexpectedly remained constant or increased. Not until the system users were put on notice that returned tickets would be tested did the number drop and then it dropped to less than 5% of previous levels.

The lessons here for financial institutions are clear. Without adequate measures of safeguarding transaction data, journals with no customer signatures may be challenged and a system which occasionally posts a transaction to the wrong account may find many times as many false claims of no transactions."

Present systems controlled by single banks are vulnerable to massive compromises either by many attacks of small dollar volume on terminals or few attacks of huge dollar volumes on central computers --- or both.

There have been few reported attacks against ATM's. This may be because of the newness of the industry, the relatively small number of ATMs installed, or the relatively few insiders with the new knowledge and opportunity to defeat the system. However, as outsiders become aware of the potential, there exists the possibility of attacks against these electronic symbols of the establishment developing into a "fad" crime-- just as were the attacks on the telephone company's long distance lines. More recently, a case here in the Washington area was

typical of Susan Nycum's Robin Hood syndrome.^{6/} A computer expert was convicted for tapping classified government files maintained on the computer of his former employer, claiming he did it to show how lax security was. (Subsequently, he circulated letters to potential clients offering his services as a "security consultant" to protect their computer from people like him!) The recent TRW/credit scandal, where the alleged ring of perpetrators, including at least one TRW employee, would allegedly alter your credit limit and rating for a fee, is possibly another example of fraud by computer. The computer field is crowded with honest people, but I have been told that some of the best programmers are coming out of our prisons, where data processing is an extremely popular curriculum. I truly hope that they have been rehabilitated, and not provided a mechanism for more criminal activity.

Rather's "60 Minutes" article was viewed by 25 million people. The popularization of these attacks may already be underway.

Who is liable for a fraudulent transaction committed on an account of a customer of bank A at bank B when the solution allowing the fraud to be successful may have been gleaned from data of Bank C? Might not a bank that has established tight security procedures over its network be understandably reluctant to allow a newcomer into its system for that reason? And who is to say whether such reluctance comes from concerns regarding lessening of security or lessening of competitive advantage?

I believe that financial institutions should proceed cautiously toward automation with thorough security analyses as part of their architecture. I also feel that the consumer should be protected from the results of their not doing so.

⁷ Nycum, supra, at 447.

54K

BEFORE THE
COMPTROLLER OF THE CURRENCY
Washington, D.C., April 3, 1975

RE: December 24, 1974 Ruling on CBCTs

Statement of Earl Ward, President
AFS Associates
Cincinnati, Ohio

My name is Earl Ward. I am President of AFS Associates, specializing in bank automation. I will limit my prepared comments to the automated teller form of CBCT since automated tellers have been the bulk of my experience.

I began working with automated tellers in 1969 while employed by the Mosler Safe Company of Hamilton, Ohio. I specified the functions Mosler's unit should perform and was instrumental in the system design of the Teller-Matic, the first system to dispense currency, accept deposits, and transfer funds between accounts. For my efforts on the operating system, I was awarded patent credits.

In early 1972, I oversaw the installation of the Teller-Matic in the first completely automatic branch, the Huntington National Bank's "Handy Bank" in Columbus, Ohio. I have represented Mosler at national meetings on automation and at industry shows. In January of this year, I left my position as Director of Marketing for the Teller-Matic Division to offer consulting services to those interested in financial automation and to assist in the orderly and constructive growth of financial automation systems. I have visited the major manufacturers and reviewed their equipment.

I am also a devoted automated teller customer. I haven't entered my branch (for banking business) since I opened my account.

I would like to discuss two subjects which may have a bearing in these proceedings -- the nature of automated teller equipment (ATE) from an operational (as opposed to legal) viewpoint and some of the problems which I believe may be encountered if automated tellers are installed as proposed by the Comptroller's Interpretive Ruling.

THE NATURE OF ATE

As its name implies, the Automated Teller was designed to duplicate as nearly as possible the functions of a live teller. The concept was to minimize the differences and thereby the adjustments which would be required in the bank operating system and by the banks' customers. The ATE had to interact with the customer, i.e., give instructions, ask questions, react to answers, etc.

ATE follows the basic teller routine for consumer transactions: identify the customer, verify the account, conclude transactions, and issue a receipt. First the automatic teller asks for, receives, and reads an identification card magnetically encoded with information. It verifies the cards authenticity, checks it against lists of hot or stolen cards or if on-line, checks the account balance or cash allowed from a central computer working file. It then asks the customer to "sign in" by entering a personal identification number which only he is supposed to know. This deviation from the traditional signature was a concession to the state of technology. Machines can't read signatures well.

Once identified, the customer may deposit funds, transfer funds, and withdraw currency from a checking, savings or credit card account or from a line of credit. He may also pay bills and in some machines change his Personal Identification Number or purchase a money order. He is issued a memo or receipt either after each transaction or after all transactions have been completed. The deposit envelopes are stamped with a serial number. This number is also printed on the receipt along with the number keyed into the machine as the amount of the deposit. The envelopes are retrieved from the automated teller at the start of the following banking day, opened and checked against the copy of the printed receipt. If there is a discrepancy, a correcting credit or debit is made to the account.

Just as live tellers usually produce a machine-readable document (usually MICR-encoded transaction slips), the automated teller operating off-line produces machine-readable records. These take the form of MICR transaction slips, optical character recognition printing, punched paper tape, and magnetic tape cassettes. When operating on-line, the machines are continuously interrogated or "polled" by the central computer. When there is activity at the teller, the machine may request authorization and report transactions completed. In this mode, they perform actions not unlike those of a human teller equipped with an on-line terminal.

New additions to automated tellers include pre-recorded greetings, multi-lingual instructions, and audio-visual contact with live tellers when assistance is required. I am certain that as

54
n
additional needs are identified, new features will be developed to meet them. In my opinion, the consumer banking functions provided by an automated teller are essentially those provided by a traditional manned branch.

PROBLEMS IN THE UNRESTRICTED PLACEMENT OF
AUTOMATED TELLER EQUIPMENT IN TODAY'S ENVIRONMENT

Unfortunately, there is no standard for encoding the magnetic stripe, for the information required on the stripe, or for generating the personal identification numbers. The American Bankers Association has approved the use of track 2 for use in on-line devices including on-line automated tellers. However, most machines are off-line. Even on-line automated tellers are usually capable of falling back to off-line operation when the computer is taken off the telecommunication network either for use in batch-processing operations or because of malfunctions of the computer or communication lines.

In the off-line mode, the magnetic information must be changed after each use. Since the ABA has specified that track 2 is not to be rewritten, other tracks must be used for the off-line mode. Until recently, the ABA maintained that interchange (between banks) of off-line machines involving common identification number generators was too risky to be practical and that therefore they would not sanction an off-line standard.

Pressed to revise the position, they are now working with the International Standards Organization and the American National Standards Institute to arrive at acceptable off-line standards for the card and to develop a secure memory number generator that could be shared by all. If they would be successful in both attempts, there

would still be significant obstacles in activating large scale shared-facilities networks.

340

First, let me say that in concept shared facilities make sense. They expand customer services without raising the specter of a line of machines in a shopping center, each bearing the logo of a different bank. The concept also permits sharing of equipment costs.

However, in practice there are some problems to consider. We have heard testimony on the Washington Shared Facilities Act. Mr. Heckman yesterday confirmed the existence of a capture theory where, due to the proprietary nature of the memory number generator and the magnetic encoding locations, banks who purchase, say, Docutel equipment are "captured" for Docutel in that they cannot integrate into their systems competitive equipment.

In a shared facility network all potential automatic teller customers who wish to have the ability to join in a shared facility must purchase the system that got there first. Specifically, if they wish their customers to be able to use Docutel CBCTs, they must issue Docutel-encoded cards. If they wish to install equipment and allow competitive banks' customers to use their new CBCTs, the machines must be Docutel equipment. My old friend, Mr. Cairnes said that he has never heard a single negative statement concerning the Washington law. I am sorry I must spoil the record. The law effectively stops Docutel's competitors from selling equipment to participating banks. Moreover, under today's state of the industry, Docutel's capture of 62 of the top 100 banks --- and 138 of the

Top, 300 ----"1/ extends the problem to nearly every region in the United States where shared facilities would be permitted. 54p

Now admittedly this situation exists because of a lack of standards for encoding and identification number generating and because of the basic incompatibility between existing systems. Would the emergence of standards alleviate the situation? Not immediately. Cards would have to be re-issued. Not only is that enormously expensive, but if the cards are credit cards, as most are, and normally expire in stages over a one to three-year period, the risk involved in having two sets of current credit cards outstanding is understandably unacceptable, especially if only to obtain an alternate source of supply to a vendor who is performing to expectations. The establishing of unrestricted shared facilities will make the eventual solution much more difficult and expensive to those banks who have pioneered the industry.

1 SECURITY CONSIDERATIONS

Two threats exist to automated teller equipment: physical attack and compromise of the system. Some of the physical threats are obvious. Trucks with grappling devices could back through the wall of an exterior unit, hook on to the entire machine, and drive off with it. Unlike most night depositories, automated tellers are not usually surrounded by concrete. Normally the depository, cash dispenser, and sometimes the entire assembly are housed in a safe with inch-thick carbon walls or the equivalent.

1/ Memorandum in Support of Interpretive Ruling...etc. Homer J. Kirby, Senior Vice President & General Counsel, Docutel Corp., March 25, 1975.

System security problems are not as obvious. Off-line ^{54g} machines --including on-line equipment which features fall back to off-line in case of communications failure (highly desired operationally)--are subject to two basic systems attacks: duplicating and altering the card. The intelligent criminal uses a combination of both.

The magnetic stripe card contains the systems operating memory. Magnetic encoding is used because it can be easily re-written in the field. Account balances (more accurately, cash remaining in a time cycle) can be decremented as the card is used to obtain money. Magnetic encoding is the only system I know of which can be easily changed and hence the only one available for off-line operation.

Those who prefer alternate methods of encoding cards (for use on-line only) have publicized the fact that the card and magnetic information can be easily and inexpensively reproduced. Some have extended this uncontested fact to the error that duplicating the card affords automatic access to ATE funds. This is incorrect for at least two reasons. (1) The memory number must also be obtained and (2) The machines contain "short-term memories" which "remember" the last x number of cards that have been presented for cash. Each time cash is withdrawn, the card is updated in a logical manner. If it shows up again--at the same machine--unchanged or changed illogically it is recognized as a fraudulent card and captured.

However, there are ways to bypass this system security.

The short-term memories vary in length from under ten to over 300. If the criminal is able to obtain more cards and associated memory numbers than the machine is capable of remembering, he may produce sets, feeding them to machines sequentially until all money is exhausted.

Even if he only skins one card, he may use one per off-line machine.

I believe these threats have not materialized because the nature of the systems has not been generally understood by those willing to commit the crimes and there haven't been the number of machines in any system large enough to justify the effort and risk. In my opinion, a nationwide system of fall-back machines would be large enough.

One manufacturer purports to lick the skimming attack by encoding the card with two separate systems of machine-readable information. Both the magnetic stripe encoder and the ATE equipment have the ability to read, interpret, and produce a code from the permanent data and encode it on the changeable magnetic stripe. This should deter the simple skimming fraud.

However, it does not solve the problem of obtaining an encoder (or using an automated teller itself) and changing the information on the card. This crime requires the participation of an insider: a bank or vendor employee. It does not necessarily require the access to the particular encoder used by the bank. In some systems the identification number generator or scrambler is part of the encoder;

in others it is separate. Of course, with access to the system ^{54s}
used by the network, an unlimited number of cards could be pro-
duced.

[Mr. Comptroller, I am pro automated tellers on or off premises.
However, for the reasons I have mentioned here, I believe the
state of the industry is not yet ready for the CBCT concept as
authorized by your Ruling. There are too many questions yet
unanswered.

FOLLOW-UP TO TESTIMONY OF EARL WARD
BEFORE THE COMPTROLLER OF THE CURRENCY

My speculation that there existed a physical threat to ATM's in that they could be easily pulled out of a wall and carted away caused some good-humored rebuttals. The following week, an article appeared in The Cincinnati Enquirer describing an incident where a bulldozer was driven through the wall of a new branch of Covington Trust, and pushed a TL-15 night depository safe across the floor. Covington Trust's Mr. Herriman, who testified at this hearing, was saved the embarrassment of a missing safe only because his floor collapsed before the safe could be lifted into a truck.

The Mosler Teller-Matic weighs 3000 lbs. The Docutel planning manual lists the weight of the Docutel module containing the money to be dispensed as 650 pounds; the depository weighs 1500 pounds. Each could be easily removed with a fork lift truck. Incidentally, the walls of the modern, low-cost branches, such as those of Mr. Herriman, are designed to separate cold air from warm and to provide a vision screen. They offer virtually no protection against burglary and would not impede to any significant extent

the physical removal of a safe. One of the recent fads among bank burglars was to pull off the face-plates of night depositories, reach in and remove the contents. Only after this particular wave of crime became known did the majority of banks opt for a more secure UL-listed type of depository.

The idea of "roping" and carting off chests of cash and deposits may strike some as humorous, that is until it happens--as it nearly did in Covington. Had the burglars read my testimony and attacked the more vulnerable automatic system, I believe they would have been successful. Nor is the return as small as Mr. Heckman testified. While his equipment may have a capacity of \$10,000, at least two manufacturers offer capacities of \$40,000. In addition, it has been testified in these hearings that the deposits usually exceed the cash dispensed, making the depository an added attraction.

The defrauding of systems seems to hold some non-technical bankers in awe. Yet to anyone with fundamental knowledge of the technology, the fraud is not very complicated. Possibly because of the newness of the industry, the apparent unconcern of the bankers, and the relatively few "targets", security precautions have often taken a back seat to operational features and engineering expediency. Messages to and from the computer center are not usually scrambled. They could then be duplicated with little effort especially

by an "insider" (of the bank or vendor). This crime could become significant if it became a fad--say among college students--or if the "solutions" were sold by organized crime to a network of smaller criminals, much as a counterfeiter discounts his product to his distributors.

As to Mr. Heckman's response to the conditions necessary to permit card fraud, I maintain they may all be present (as they have been in at least two cases referred to in Mr. Homer Kirby's testimony.)

1. Magnetic-striped cards may be purchased in quantity by anyone. They are handed out at trade shows and are kept in quantities by card companies and equipment manufacturers. Nor does the quantity need to be "unlimited". If each card limit is encoded at the maximum the bank allows, and if that maximum is say \$500, each machine could be defrauded of up to \$15,000 with only 50 cards.
2. With the new standards, encoders also must be standard, therefore obtainable by simple purchase or by burglary. Encoders sell for as little as \$6,000 each, but the technology is published so that a knowledgeable person could build one for much less.

3. No wheelbarrows would be necessary to handle the 50 cards necessary to feed the machine. A paper bag would do fine. Most manufacturers claim that their machines are so fast that a complete cash withdrawal may be made in 25-35 seconds. That would mean about 25 minutes--at any time of night--to feed 50 cards. Of course the 25 minutes need not be consecutive. If interrupted, the fraud could return later to complete his transactions.

Incidentally, the Docutel and Mosler "scrambling" schemes are a matter of public record. The patents may be obtained for 50 cents each. These go a long way toward helping to discover the flaws inherent in the systems.

The appeal of this crime to the criminal is that it involves no violence, there is virtually no time constraint, little chance of being apprehended in the act, and real cash is involved on an impersonal basis (unlike normal computer fraud where a dummy account is fraudulently filled then a live teller must be confronted to obtain the cash.)

There is also an appeal to the first offender, a sort of "it's fair to try to beat the system" syndrome. Susan Hubbell Nycum could just as well have been describing the automatic teller system programmer or analyst as the computer embezzler in her article in the April American

CONTINUED

1 OF 6

Bar Association Journal ("Computer Abuses Raise New Legal Problems") when she reported:

"The elements of challenge and game playing seem to be significantly stronger among computer-abuse perpetrators than among other white collar criminals.

"In some cases claims of victims that their computer systems were safe and could not be penetrated encouraged programmers (sic), who look upon their work as an intellectual challenge pitting their minds against the

intransigent machine. One perpetrator, who claims to have gained over one million dollars from his deeds, said that aside from making money rapidly his motive was to see how far he could go with his crime before he informed his victim of the acts. He was confident that no evidence of his act could be found even if he revealed how he did it.

"The Robin Hood syndrome is common. One interviewed perpetrator indicated that doing harm to people is highly immoral, but since government-regulated industry in general and telephone companies in particular do great harm to society, harming these organizations is fair. This differentiation between doing harm to people and to organizations has some current popularity. The computer within the organization is an additionally attractive and satisfying target capable of sustaining loss but not possessing emotional reactions that might produce feelings of guilt in the unprofessional criminal." ^{1/}

1. Susan Hubbell Nycum: "Computer Abuses Raise New Legal Problems" American Bar Association Journal April 1975, pp.444-448.

I must confess that the relative ease and obscurity surrounding the defrauding of these automatic teller systems has caused a few Walter Mitty mental excursions of my own. Without revealing particulars, here are a few of the formulas for beating the system.

ATM FRAUDS

A. Simply duplicate the cards.

This is a relatively unsophisticated attack but effective against ATMs having short term memories of only a few transactions. One system reportedly remembers only the last three transactions.

1. Obtain three cards and associated memory codes.
These may be three legitimate cards issued to a single account, to more than one accomplice, or may be stolen from the mails or purchased from prostitutes who find the obtaining of the cards a rewarding extension of their profession.
2. Duplicate the cards using a simple skimming technique or an encoder.
3. The cards may now be used in sequence to empty all off-line machines in the system.

B. Create new card/code combinations.

This attack appeals to the "Robin Hood" perpetrator mentioned above. It is somewhat more difficult but effective against more systems.

1. Obtain access to an encoder (machine capable of encoding new information on the magnetic stripe.)

If surreptitious access is impossible, encoders may be purchased, built, or stolen with little difficulty. In the new "standard" systems, an easily portable desk-top encoder is used.

2. Obtain access to a decoder (the machine that carries out the formula for producing the memory number from data on the card.) Unlike the encoder, the decoder varies from manufacturer to manufacturer and is sold only to legitimate end users. They are usually easily accessed by insiders of the manufacturer but in a state before the financial institution enters its own secret parameters. If access to the physical decoder is not possible, mail \$.50 to the patent office to obtain a copy of the patent covering the system. Then figure out the loopholes.

3. Produce new codes and cards. Use them at will.

C. Tap the on-line machines.

1. Obtain the message format used in the machine communications. These are published and easily

obtainable from the manufacturer. System programmers of both the manufacturer and the financial institution have access to this data.

2. Program a mini computer to emulate the normal host computer driving the network.
 3. Cut the phone lines and establish contact with the mini.
 4. Withdraw money based on the new unlimited credit in your fictitious account.
-

Regarding standards, Mr. Brown stated that "it's probably unlikely that we would allow ourselves to be the captive of one vendor," yet that is precisely what the majority of banks owning ATM's have done. He also has faith in the "various standard (sic) committees to develop some kind of off-line standard for which all institutions will be able to use."

My point is that until those standards exist--for memory generating as well as encoding cards--the unregulated promulgation of these machines makes the task of real standardization all the more difficult.

Indeed, it may be that a secure, universal memory number generator system is simply unrealistic. These

are questions that have yet to be addressed, let alone answered.

54cc

"DIAL 'E' FOR EMBROIDERED"

OPEN

RATHER:

The way a banker makes money is to move money around as fast as he can. The faster it moves, the more money the banker makes.

So it's no surprise that the bankers are hell-bent to speed up their systems...with instant communications and electronic wizardry.

Trouble is, the bank thieves are as up-to-date as the bankers...sometimes a step ahead. And the bankers, and the police, and the government all find gaping holes in the electronic banking system...just right for the modern day Bonnies and Clydes.

54dd

-1-

60 MINUTES

VOL. 1X, No. 4

FINAL CUT

10/10/76

"DIAL 'E' FOR EMBEZZLEMENT"

RATHER:

IN BIG BANKS AND SMALL ACROSS THE COUNTRY, THE GOAL IS TO GET OUT FROM UNDER THE CRUSH OF PAPER WE'VE HAD TO DEAL WITH FOR SO MANY YEARS. CASH: NICE TO FEEL AND TO SPEND, BUT MANY BANKERS SAY IT'S CLUMSY, RISKY AND INCREASINGLY OUT OF DATE.

CHECKS: CHECKS BY THE HUNDREDS OF MILLIONS EVERY DAY CHOKING BANKERS WITH PAPER TO BE SORTED AND CROSS CHECKED AND FILED AND STORED. THE WAY OUT, SAY BANKERS, IS TO DO AWAY WITH THOSE PAPER RECORDS, AND USE ELECTRONIC COMMUNICATIONS AND COMPUTERS TO KEEP TRACK OF IT ALL. AND THERE LIES THE CATCH. SOME OF THE THIEVES KNOW MORE ABOUT THESE NEW ELECTRONIC SYSTEMS THAN THE BANKERS.

~~FASTER BANKING CAN LEAD TO FASTER STEALING~~

AS SOME SADDER AND WISER BANKERS ARE BEGINNING TO LEARN. TO UNDERSTAND HOW IT CAN BE DONE, SOMETIMES IT TAKES A THIEF TO CATCH A THIEF. NUMBER, FROM A BANK CARD

-2-

RATHER (CONTINUED)

IN THE HILLS BACK OF HOLLYWOOD, THERE'S A MAN WHO OPERATES JUST THAT WAY. HE'S JERRY SCHNEIDER, A CONVICTED COMPUTER THIEF.

HIS CRIME WAS TO STEAL PERHAPS AS MUCH AS A MILLION DOLLARS, FROM THE TELEPHONE COMPANY, THROUGH THEIR OWN COMPUTER. IN EXCHANGE FOR CONFESSING HOW HE DID THAT, SCHNEIDER GOT A FORTY DAY JAIL TERM, INSTEAD OF TEN YEARS. NOW HE SAYS HE'S A HIGH PRICED SECURITY CONSULTANT.

SCHNEIDER:

IF SOMEBODY'S AFTER MONEY, OKAY, WHICH IS THE -- WHICH IS THE GOAL HERE, FROM BANKS, THEY'RE GOING TO DO IT ANYWAY THEY KNOW HOW TO DO IT.

RATHER:

SCHNEIDER PROCEEDED TO SHOW US HOW YOU CAN JIMMY YOUR WAY INTO A BANK ALMOST ANYWHERE, LONG DISTANCE. ~~WITH A COMPUTER TERMINAL~~ AND TODAY'S COMMUNICATIONS NETWORK. ~~COLLECTOR~~

~~MY OWN BANK ACCOUNT~~ GOT JERRY THE PHONE NUMBER OF THE CREDIT DEPARTMENT. HE ALREADY HAD MY OWN BANK ACCOUNT NUMBER, FROM A BANK CARD THAT LETS ME OVERDRAW MY CHECKING ACCOUNT BY FIVE HUNDRED DOLLARS,

RATHER (CONTINUED)

DOLLARS, NO QUESTIONS ASKED. JERRY IS
TALKING TO A CLERK IN NEW YORK, TRYING TO
GET HIM TO JACK UP MY CREDIT LIMIT FROM
FIVE HUNDRED DOLLARS, TO TEN THOUSAND DOLLARS.

SCHNEIDER:

-- YES, ACCOUNT ONE, THREE, FIVE, 0-0-0...

RATHER:

IF THE CLERK SAYS YES, THE CLERK WILL ENTER
THAT INTO THE BANK'S COMPUTER.

MAN:

CREDIT LIMIT?

SCHNEIDER:

TEN THOUSAND DOLLARS.

MAN:

TRANSACTION CODE, FIVE, ONE, FOUR, EIGHT.

SCHNEIDER:

THANK YOU.

MAN:

WELCOME.

RATHER:

IT ISN'T THAT EASY. YOU CAN'T SIMPLY CALL ON
THE TELEPHONE, AND GET ONE'S CREDIT EXTENDED
FROM FIVE HUNDRED DOLLARS TO TEN THOUSAND
DOLLARS?

BECOMING VERY

-4-

SCHNEIDER:

YEAH, YOU CAN. THE -- THE SECURITY BEHIND
THIS OR THE ALLEGED SECURITY THAT THE
BANK HAS, IS THAT, TOMORROW MORNING WHEN THE
BANK AUDITORS SEE YOUR LEDGER, AND IT SAYS
DAN RATHER ACCOUNT, TEN THOUSAND DOLLARS,
THEY'LL SAY SOMETHING'S WRONG.

RATHER:

ARE THEY LIKELY TO DO THAT?

SCHNEIDER:

-- WELL, NOT IF YOU COULD GET TO THE -- TO THE
-- TO THE BANK AND TAKE -- GET A WITHDRAWAL
BEFORE THE AUDITORS DECIDE THAT -- THAT THEY
WERE GOING TO LOOK INTO THIS SITUATION.
IT -- IT -- IT MAY, IN ALL -- IN ALL
POSSIBILITY, -- YOU WON'T GET CAUGHT TOMORROW.
IT MAY BE AT THE END OF THE MONTH, AT THE
END OF THE QUARTER.

RATHER:

WELL, WE'LL CARRY ON WHATEVER IT IS YOU WERE
GOING TO DO THEN.

SCHNEIDER:

YEAH, I'M -- WHAT I'D LIKE TO DO IS CALL THE
BANK AND UNDO WHAT WE DID. BECAUSE I'M
BECOMING VERY NERVOUS AT THIS POINT.

-5-

RATHER:

ALRIGHT.

SCHNEIDER:

ALRIGHT.

RATHER:

SO JERRY CALLED THE SAME NUMBER AGAIN, TO
UNDO THE FIRST CALL.

SCHNEIDER:

CANCEL TRANSACTION, FIVE, ONE, FOUR, EIGHT --
NEW LIMIT FIVE HUNDRED DOLLARS.

MAN:

OKAY, FIVE, ONE, FOUR, EIGHT, CANCELLED. NEW
LIMIT FIVE HUNDRED.

SCHNEIDER:

THANK YOU.

MAN:

WELCOME.

RATHER:

IF WHAT SCHNEIDER DID SEEMS FAR FETCHED, NOTE
THAT SOMEBODY TRIED THE SAME SCHEME AGAINST
THE CITY BANK OF NEW YORK, THE NATION'S
SECOND LARGEST BANK. EXECUTIVE VICE PRESIDENT,
JOHN REED.

REED:

THEY PICKED UP THE PHONE. THEY CALLED US.
THEY INDICATED THAT THEY WERE A BANKING

-6-

REED (CONTINUED)

CUSTOMER. THEY GAVE THE APPROPRIATE CODED INFORMATION THAT LEAD US TO BELIEVE THAT THEY IN FACT WERE. THEY ASKED TO TRANSFER TWO MILLION DOLLARS FROM THEIR ACCOUNT, TO THE ACCOUNT OF ANOTHER BANK. THE PAPER WORK WHICH CAUSES THAT TO HAPPEN, WAS INITIATED BASED UPON THAT TELEPHONE COMMUNICATION. AND THE TRANSFER IN FACT, WAS MADE. THE RECEIVING BANK WAS CREDITED WITH TWO MILLION DOLLARS.

RATHER:

~~DID THEY GET AWAY WITH THE MONEY?~~

REED:

~~THEY DID NOT~~ THE F.B.I. FOR SOME REASON, BECAME AWARE OF THIS, AND ALERTED US TO IT.

RATHER:

IN JOHN REED'S OWN CITY BANK, MILLION DOLLAR, HUNDRED MILLION DOLLAR TRANSACTIONS FLY ACROSS THE WIRES. PART OF HUNDREDS OF BILLIONS OF DOLLARS MOVING AROUND THE WORLD EVERY DAY. FOR REAL ESTATE DEALS, ARAB OIL, AMERICAN WHEAT AND STEEL AND COTTON. IT'S ALL BEING FED DIRECTLY INTO COMPUTERS, WHICH TALK TO OTHER COMPUTERS. AND SO EVEN THIS

RATHER (CONTINUED)

VISIBLE RECORD WILL DISAPPEAR AS THE WHOLE
SYSTEM MOVES TO NO PAPER TRANSACTIONS. JUST
SILICONE CHIPS AND MAGNETIC TAPES TO
REMEMBER WHERE THE MONEY IS. THE FEAR IS,
~~THAT THE VERY MEN WHO DESIGN AND OPERATE~~
~~THESE SYSTEMS ARE IN A POSITION TO COMMIT~~
~~SOME OF THE BIGGEST BANK HEISTS IN HISTORY.~~

IT HAS ALREADY BEGUN. IN CHICAGO, THE
COSMOPOLITAN BANK LOST SEVEN MILLION DOLLARS
A FEW YEARS BACK. IT WAS BASICALLY A BAD
CHECK SCHEME, BUT ONE OF THE BANK OFFICERS
USED IT'S COMPUTER TO COVER UP THE FRAUD.
IN NEW YORK, THE UNION DIME SAVINGS BANK
HAD A CHIEF TELLER STEAL ONE AND A HALF
MILLION DOLLARS, COVERING UP THROUGH THE
COMPUTER. HE WAS CAUGHT ONLY AFTER THE POLICE
RAIDED HIS BOOKIE JOINT. BANKERS ADMIT
THAT THERE ARE MANY MORE CASES THAT NEVER
REACH COURT BECAUSE BANKS DON'T WANT BAD
PUBLICITY.

AT THE STANFORD RESEARCH INSTITUTE IN
CALIFORNIA, DONN PARKER AND HIS COLLEAGUES
KEEP A CATALOGUE OF COMPUTER CRIME.

PARKER:

THE AVERAGE BANK FRAUD IN EMBEZZLEMENT NOTED BY THE F.B.I., IN NINETEEN SEVENTY FOUR, WAS -- INVOLVED A LOSS OF NINETEEN THOUSAND DOLLARS. THE AVERAGE COMPUTER RELATED BANK FRAUD IN EMBEZZLEMENT BASED ON MY FILE OF CASES, IS JUST A LITTLE UNDER FIVE HUNDRED THOUSAND DOLLARS, PER INCIDENT. AND WHAT WE ARE -- WHAT WE'RE FACED WITH REALLY, IS AUTOMATED CRIME. I MEAN, THAT'S WHAT IT IS. IT'S AUTOMATED CRIME.

RATHER:

BUT, ALONG WITH THE RISK, PARKER SEES AN OVERALL BENEFIT FOR SOCIETY. NEW OPPORTUNITIES CREATED BY NEW BANKING TECHNOLOGY.

PARKER:

TAKE MONEY FOR EXAMPLE. WE USED TO BARTER GOODS AND SERVICES, I'LL GIVE YOU A CHICKEN FOR IT. WE WENT TO PRECIOUS METAL. PRECIOUS METAL GOT HEAVY TO CARRY AROUND. WE WENT TO PAPER THAT SAYS, I HAVE SO MUCH PRECIOUS METAL IN A VAULT. THEN WE DROPPED THE PRECIOUS METAL, AND SAID WHY WORRY ABOUT THAT, WE'LL JUST USE THE PAPER. THEN, WE WENT TO ELECTRONIC FUND TRANSFER, IN WHICH WE'VE THROWN AWAY

PARKER (CONTINUED)

THE PAPER, AND THE MONEY NOW, IS REPRESENTED IN ELECTRONIC PULSES, AND MAGNETIC PATTERNS STORED IN COMPUTER SYSTEMS. SO NOW, INSTEAD OF SAYING, I'LL PAY YOU TEN DOLLARS FOR IT, YOU SAY PLEASE DEBIT MY ACCOUNT TEN DOLLARS, AND CREDIT YOUR ACCOUNT TEN DOLLARS, AND INSTANTANEOUSLY WE HAVE A TRANSACTION.

RATHER:

THAT'S JUST THE WAY IT'S WORKING RIGHT NOW IN CALIFORNIA, AT SUPERMARKETS TIED RIGHT INTO THE COMPUTER, AT GLENDALE FEDERAL SAVINGS AND LOAN. WHEN YOU COME DOWN THE CHECKOUT LINE AT SMITH'S FOOD KING, IN SANTA BARBARA, THE SUPERMARKET CLERK PUTS YOUR BANK CARD INTO ONE SIDE OF THE MACHINE, AND YOU PUNCH YOUR OWN SECRET IDENTIFICATION NUMBER INTO THE OTHER SIDE. AND THEN THE CLERK FEEDS IN YOUR BILL, AND ZIP, JUST LIKE THAT, ELECTRONICALLY THE MONEY FLIES OUT OF YOUR ACCOUNT AT THE BANK, AND INTO THE ACCOUNT OF THE SUPERMARKET. IT'S NOT A CREDIT CARD, BUT AN IMMEDIATE DEBIT CARD. THE WAVE OF THE BANKING FUTURE.

IN PITTSBURGH, THE PUBLIC CAN DEAL DIRECTLY WITH THE BANK COMPUTER. WHEN TONI RICHARDSON

RATHER (CONTINUED)

SITS DOWN TO PAY HER MONTHLY BILLS, SHE
NEEDS NO CHECKS. JUST A TOUCH TONE PHONE,
AND A CALL TO THE COMPUTER AT HER DOLLAR
SAVINGS BANK.

COMPUTER:

DOLLAR SAVINGS BANK PAY BY PHONE. PLEASE
ENTER YOUR ACCOUNT NUMBER.

RATHER:

DOWNTOWN AT DOLLAR, THE COMPUTER ANSWERS IN
PRE-RECORDED BITS OF HUMAN CHATTER. THE
CUSTOMER HAS AN ACCOUNT NUMBER FOR DEPARTMENT
STORES, UTILITIES AND SO ON. AND ALL SHE HAS
TO DO IS TELL THE COMPUTER BY PUSH BUTTON,
THE NUMBER OF THE ACCOUNT SHE WANTS TO PAY.

COMPUTER:

ONE, FOUR, FIVE, FIVE, ENTER PAYMENT AMOUNT.

RATHER:

COMPUTER ASKS WHAT YOU WANT TO DO. CUSTOMER
PUNCHES IN THE AMOUNT.

COMPUTER:

THREE, SEVEN DOLLARS, AND ZERO, ZERO CENTS.

RATHER:

ALL ELECTRONIC, NO PAPER TO REMEMBER WHAT HAS
GONE ON. ON STREET CORNERS ACROSS THE COUNTRY,

RATHER (CONTINUED)

YOU CAN SEE MORE AND MORE COMPUTERIZED BANKING. BANK CARD TO GET INSTANT CASH. BUT SOME OF THESE CARDS CAN BE COUNTERFEITED, AND USED TO STEAL FROM THESE REMOTE CONTROL BANKS. A SKILLED TECHNICIAN CAN RECORD THE ELECTRONIC INFORMATION ON THE MAGNETIC TAPE, ON THE BACK OF MANY CARDS. HE CAN LISTEN TO THE BLIPS, ANALYZE THEM, EVEN DECODE THEM. BANKS HAVE A HARD TIME CHANGING THEIR CARDS TO STAY A STEP AHEAD OF THE COUNTERFEITERS. THE CITY BANK OF NEW YORK THINKS IT HAS A SECURE CARD SYSTEM. AND CUSTOMERS USE IT NOW TO ASK THE COMPUTER FOR THEIR OWN BALANCES, OUTSTANDING LOANS, AND SO ON. AND THE TELLERS USE THE SAME CARDS TO PUNCH TRANSACTIONS AT SOME BRANCHES DIRECTLY INTO THE COMPUTERS.

COMPUTERS IN THE MEANTIME, BECOME SMALLER, FASTER AND CHEAPER. LURING BANKERS STILL FURTHER INTO THE TRANSISTORIZED WORLD. THIS COMPUTER FOR EXAMPLE, CAN BE REPLACED BY ONE THIS SIZE, AT A FRACTION OF THE COST. AND ONCE AGAIN, IT IS THE PEOPLE WHO PROGRAM THESE COMPUTERS, WHO ARE THE GREATEST POTENTIAL THREAT TO THE ELECTRONIC BANKING SYSTEM.

-12-

RATHER (CONTINUED)

THEY KNEW THE SECURITY CHECKS THAT HAVE BEEN BUILT IN. AND IN SOME CASES, HOW TO GET AROUND THEM. IMAGINE, FOR EXAMPLE, HOW FAR A SAVVY CRIMINAL COULD GO, IF HE HAD JERRY SCHNEIDER'S KNOWLEDGE OF COMPUTER PROGRAMMING AND THE BANKING SYSTEM.

JERRY SHOWED US A DESK TOP COMPUTER TERMINAL THAT PLUGS INTO A STANDARD TELEPHONE. IT'S EVERYDAY HARDWARE IN THE COMPUTER BUSINESS. COSTS ABOUT TWO THOUSAND DOLLARS. FROM JERRY'S LIVINGROOM IN HOLLYWOOD, YOU CAN DIAL BANK COMPUTERS IN NEW YORK, OR ANYWHERE IN THE WORLD. THE TRICK IS TO LEARN THE RIGHT NUMBERS, THE RIGHT CODES, SO THE COMPUTERS WILL LET YOU IN.

: SCHNEIDER:

-- THIS IS NO DIFFERENT THAN YOU WALKING INTO -- INTO THE NATIONS LARGEST BANK, AND GOING INTO THEIR MOST SENSITIVE FILE ROOM

SCHNEIDER (CONTINUED)

AND BROWSING THROUGH FILES. THIS ALLOWS
YOU DO TO THAT.

RATHER:

THE NUMBER JERRY HAD DIALED WAS MY OWN BANKS
COMPUTER. BYPASSING THE CLERKS THIS TIME.
AGAIN, WANTING TO JACK UP MY CREDIT TO TEN
THOUSAND DOLLARS....ARE YOU NOW IN TOUCH
WITH MY BANKS COMPUTER?

SCHNEIDER:

RIGHT. AND THE COMPUTER IS NOW ASKING ME
TO IDENTIFY MYSELF. IT'S SAYING, WHO AM I.

RATHER:

JERRY THEN TYPED IN THE CODE HIS INSIDER HAD
SAID WOULD WORK THAT DAY. THE MACHINE SAID
ILLEGAL ENTRY. AND HUNG UP ON US. JERRY
TRIED AGAIN, BUT STILL NO LUCK.

SCHNEIDER:

OKAY. WELL, THE CODE DOESN'T WORK. AND I
CAN KEEP TRYING FOREVER AND IT WON'T WORK.

RATHER:

BUT IF WE WERE GOING TO STEAL BY COMPUTER...

SCHNEIDER:

YEAH...

RATHER:

SOMEONE ON THE INSIDE WOULD GIVE YOU THAT CODE,
AND OR IF YOU WORKED ON THE INSIDE, YOU'D

-14-

RATHER (CONTINUED)

HAVE THAT CODE?

SCHNEIDER:

RIGHT.

RATHER:

BE
YOU'D NOW/IN TOUCH, BEING IN TOUCH WITH MY
BANK'S COMPUTER? YOU'D NOW BE IN A POSITION
TO WALK THROUGH THE BANK'S COMPUTER FILES?

SCHNEIDER:

WELL, I WOULD BE ABLE TO DO MORE THAN THAT.
I'D BE ABLE TO -- TO TRANSFER -- WITHOUT
TALKING TO ANY PERSON AT ALL. IN OTHER WORDS,
BE ABLE TO PUT TEN THOUSAND DOLLARS INTO YOUR
CHECKING ACCOUNT, YOU'D BE ABLE TO LEAVE
WITH IT.

RATHER:

CAN YOU SHOW ME HOW THAT IS DONE?

SCHNEIDER:

I CAN SHOW YOU WHAT IT WOULD BE LIKE ON A
-- ON A MODEL THAT I HAVE CREATED OF THIS --
THIS IDENTICAL SYSTEM.

RATHER:

SHOW ME.

SCHNEIDER:

OKAY.

RATHER:

SO JERRY DIALED INTO A COMPUTER HE USES
IN CALIFORNIA, WHERE HE HAD SET UP A MODEL
BANK PROGRAM. HERE, WITH MY OWN ACCOUNT IN
THIS SIMULATED BANK, HE SHOWED HOW ONCE
AGAIN HE COULD RAISE MY BANK CREDIT FROM
FIVE HUNDRED DOLLARS TO TEN THOUSAND DOLLARS.

YOU HAVE TO BE CAREFUL WITH THE ZEROS,
THAT YOU DON'T MAKE IT A HUNDRED THOUSAND
DOLLARS, HUH?

SCHNEIDER:

WELL, IT WOULDN'T MAKE ANY DIFFERENCE.

RATHER:

YOU MEAN ONCE YOU HAVE THIS KIND OF ENTRY,
YOU COULD GIVE ME A HUNDRED THOUSAND DOLLARS
AS EASILY AS YOU COULD GIVE ME TEN THOUSAND?

SCHNEIDER:

THAT'S RIGHT. OKAY, IT'S DONE NOW. OKAY.

RATHER:

NOW TO TURN THE CREDIT INTO CASH I COULD PUT
IT INTO MY OWN POCKET, IF THIS WERE A REAL
ACCOUNT. JERRY, WITH JUST THE MODEL COMPUTER,

-16-

RATHER (CONTINUED)

TRANSFERRED THE TEN THOUSAND FROM MY CREDIT
ACCOUNT, INTO MY CHECKING ACCOUNT.

SCHNEIDER:

OKAY, IT'S DONE.

RATHER:

THAT EASILY?

SCHNEIDER:

YEAH. WHAT -- WHAT WE JUST --WE JUST
TRANSFERRED -- THE CREDIT ACCOUNT INTO YOUR
CHECKING ACCOUNT.

RATHER:

SO NOW I HAD THE MONEY IN MY ACCOUNT. JERRY
INSISTING HE COULD HAVE DONE THE SAME TO
MY REAL BANK ACCOUNT, IF ONLY HE HAD KNOWN
THE RIGHT CODE FOR THAT DAY.

IF A MAN IN LOS ANGELES, CALIFORNIA, HAS TODAY'S
CODE, FOR THE CITY BANK COMPUTER, HE ^{CAN}/GAIN
ENTRY TO YOUR COMPUTER IN NEW YORK?

REED:

AS YOU SUGGESTED IT, CERTAINLY.

RATHER:

HE COULD AFFECT TRANSFER OF FUNDS?

REED:

COULD GAIN
THAT'S CORRECT.

-17-

RATHER:

HAVE YOU, HAS THIS BANK EVER BEEN DEFRAUDED
BY COMPUTER?

REED:

WE'RE NOT AWARE OF IT. THE REAL DANGER IN
ANY FRAUD IS THE FRAUD YOU NEVER DISCOVER,
OF COURSE. BUT TO THE BEST OF OUR KNOWLEDGE,
WE HAVE HAD NO COMPUTER FRAUD PROBLEMS TO DATE.

RATHER:

ANYONE TRIED?

REED:

TO THE BEST OF OUR KNOWLEDGE NOT.

RATHER:

ROUGHLY, HOW MANY COMPUTER PROGRAMMERS ARE
THERE IN THIS COUNTRY?

PARKER:

WELL, VERY ROUGHLY, I'D SAY, PROBABLY
ABOUT -- FOUR HUNDRED THOUSAND.

RATHER:

FOUR HUNDRED THOUSAND?

PARKER:

WHO HAVE THE -- SOME KIND OF PROGRAMMING
CAPABILITY. OUT OF FOUR HUNDRED THOUSAND --
OF THOSE PEOPLE, YOU - YOU KNOW, I -- I
COULD GUESS THAT THERE MIGHT BE -- A -- A

-18-

PARKER (CONTINUED)

HUNDRED THOUSAND, WHO WOULD BE -- WHO WOULD
HAVE THE SKILLS, KNOWLEDGE, AND ACCESS,
IN ORDER TO BE IN THIS POSITION OF TRUST,
WHERE THEY COULD DO SOMETHING IN SOME
UNDETECTED FASHION SUCCESSFULLY.

RATHER:

WHAT LAW ENFORCEMENT PEOPLE ARE
BEGINNING TO LEARN IS THAT IF YOU HAVE
A COMPUTER FRAUD, THE OLD WAYS OF
CRACKING A CASE CAN BE USELESS. TODAY'S
COMPUTER RECORDS ARE ON MAGNETIC
TAPES...EASILY ERASED OR CHANGED.
GONE ARE THE BLACK-AND-WHITE WRITTEN
RECORDS THAT HELP TRACE A FRAUD.
IT WORRIES THE U.S. ATTORNEY IN SAN
DIEGO, TERRY KNOEPP.

RATHER (CONTINUED)

WHAT IS THE POTENTIAL FOR ORGANIZED MAFIA
TYPE CRIME, TO BE INVOLVED IN THEFT BY
COMPUTER?

KNOEPP:

WELL, I DON'T KNOW, FOR A FACT. MY
GUESS IS THAT ANYTIME YOU HAVE LARGE AMOUNTS
OF MONEY INVOLVED, LARGE AMOUNTS OF CASH,
THAT CAN BE TRANSFERRED WITHOUT ANY
SORT OF AUDIT OR TRACING, YOU'RE GOING
TO GET ORGANIZED CRIME INTERESTED IN
THAT AREA. THIS IS TRUE HERE, AS IT IS
IN GAMBLING OR ANYTHING ELSE. WE HAVE
THE SAME ELEMENTS. AND I THINK THAT
THAT'S CERTAINLY A POTENTIAL, YES.

RATHER:

I DON'T WANT TO BE PRESUMPTUOUS, BUT MY EXPERIENCE AS A REPORTER TELLS ME THE TRANSLATION OF THAT IS, THAT IT'S SOMETHING YOU'RE WORRIED ABOUT?

KNOEPP:

YES.

RATHER:

AGAIN. DONN PARKER. WE ASKED WHETHER SOMEONE WITH THE SKILLS OF A JERRY SCHNEIDER COULD CRACK A BANK TODAY?

PARKER:

YES, BUT I COULD ALSO SAY THAT OF -- OF A LARGE NUMBER OF PEOPLE.

RATHER:

HOW LONG DO YOU THINK IT WOULD TAKE HIM?

PARKER:

-- YOU CAN'T ANSWER THAT BECAUSE, TODAY HE COULD FIND A BANK, THAT WOULD BE -- AS -- AS VULNERABLE AS A CHILD'S PIGGY BANK. OR HE COULD GO UP AGAINST A BANK THAT WOULD BE A FORT KNOX.

RATHER:

JERRY SCHNEIDER, HOW DO I KNOW THAT YOU'VE GONE STRAIGHT?

SCHNEIDER:

YOU DON'T.

RATHER:

HOW COULD I DETERMINE THAT?

SCHNEIDER:

YOU CAN'T.

1

2

3

4

MR. WEGNER: Our next witness will be Mr. Barry

5

Deutsch, the Vice President of Provident National Bank.

6

Mr. Deutsch, please.

7

Counsel, will you swear in Mr. Deutsch?

8

(Witness sworn.)

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 TESTIMONY OF BARRY I. DEUTSCH, VICE PRESIDENT,
2 DIRECTOR OF MARKETING, PROVIDENT NATIONAL BANK,
3 PHILADELPHIA, PENNSYLVANIA.

4 CHAIRMAN ATWATER: Mr. Deutsch, we are very happy
5 to have you here, and we would be happy if you would give
6 your ten-minute presentation prior to the questions.

7 MR. DEUTSCH: Thank you, Mr. Chairman.

8 Mr. Chairman, ladies and gentlemen, my name is
9 Barry Deutsch. I am Vice President and Director of Marketing
10 of the Provident National Bank in Philadelphia, Pennsylvania.

11 I might also say, before I begin, that I am
12 a director and member of the Executive Committee of the
13 Bank Marketing Association. I make that point only because
14 in my prepared testimony, in my written testimony, I've made
15 reference to a certain study which was performed under the
16 sponsorship of the Bank Marketing Association, and I have been
17 asked to inform the Committee that this reference was not
18 meant to align them with my position.

19 I'm not here as a spokesman for the Bank Marketing
20 Association, merely for the Provident National Bank and for
21 myself as an individual.

22 I might start by just saying that my first
23 experience with the question of bank privacy arose 15 years
24 ago when I was working as a teller in a branch of the First
25 Pennsylvania Bank in Northeast Philadelphia.

1 I had one customer who was a regular customer
2 at my particular teller window who was a guard at Holmesburg
3 Prison. This man was paid by paycheck every other week, and
4 every other week he came to the bank with a deposit slip made
5 in the amount of \$125. The amount of the paycheck was always
6 different and somewhat higher than that.

7 The standard policy of our bank and the standard
8 procedure, I think, in many banks, was for the teller to
9 write the amount of the check on the deposit slip, subtract
10 the amount of the deposit, and therefore have a record of
11 the amount of cash which was given the customer.

12 This particular gentleman invariably said to me
13 when he handed me his check and his deposit slip, "Don't do
14 your arithmetic on the deposit slip. Give me my receipt
15 first."

16 I was very naive
17 in those days. His purpose, I later found out, was to conceal
18 from his wife the gross amount of the paycheck.

19 It appeared that there was overtime involved and
20 some other bonus payments being made to the prison guards, and
21 all of the extra pay above the \$125 that he deposited in the
22 bank and that amount of cash which he turned over to his wife
23 was, in his view, his money.

24 I raise that as my introductory remark because it is
25 my belief that consumer concern over privacy is very often

1 misinterpreted by those who discuss it. By the way, I
2 plan to discuss privacy almost entirely in my testimony
3 because I believe in studies — and studies that I have looked
4 at lead me to confirm my own belief that the proper
5 understanding of what people mean when they say they are
6 concerned about privacy is different than the generally
7 accepted definitions that are before us, even in the call to
8 this hearing.

9 We believe that there is some cause for concern
10 over access to consumer records that exist in the bank, and
11 we do understand that the concern is enhanced because of the
12 fact that information held in electronic equipment is more
13 easily accessible.

14 It is the policy of our bank that when we receive
15 a subpoena from a government agency to turn over to them
16 records of the bank, we delay compliance with that subpoena
17 until the customer has been notified of our receipt and our
18 intention to comply.

19 We believe this gives the customer the right to
20 seek whatever legal redress he may have to stop the government
21 from accessing those records.

22 Generally speaking, no customer has ever done that.
23 Generally speaking, we have always felt better about complying
24 with that particular policy.

25 That policy has been discussed, by the way, with the

1 United States Attorney in our district, and appears to be a
2 reasonably acceptable one.

3 It's our belief, and I'm prepared to say to
4 this Committee, that such policy, if it were to become
5 regulation or law as a general practice of all banks, would
6 probably ease some people's concern over that aspect of the
7 privacy question. That is, the government will know a great
8 deal more about me.

9 There are great problems, I believe, in our
10 ability to sell electronic funds transfer services. There are
11 great concerns that people have over its marketability.

12 People don't really believe, that we can control
13 our error rates and correct them once we make them. People are
14 concerned in great measure over whether we will protect
15 their control over the timing of their payments. That is to
16 say, their ability to pay a bill, all of it, some of it, or
17 none of it, on a particular day.

18 And finally, people are concerned whether
19 they be able, in their own private way, to
20 keep their own personal records of what is put in and what is
21 taken out of their bank accounts.

22 It is my firm belief that until the banking industry
23 and those of us who practice marketing within the banking
24 industry — a disadvantaged minority, I might add — until we
25 are able to convince our operations people to solve those

1 problems so that we will have a more marketable set of
2 products to offer to the public,

3 the question of privacy will remain moot.

4 PACE I was a study conducted by the Bank Marketing
5 Association published in 1973, and when it arrived on our
6 desks it did not carry good news for the marketing profession.

7 PACE I revealed very low concept favorability
8 and very low expressed willingness to use automatic pay
9 deposits and automatic bill-paying services.

10 These stated reasons included a great deal of
11 concern over the loss of control, as I previously referenced,
12 and the possibility of error over a statement. And I would
13 just like to digress for a minute to define the "right to
14 deposit my own/want to see it" as a reason for not liking
15 this particular service.

16 The question of invasion of privacy was not
17 even raised in the PACE I study by the respondents to the
18 panel.

19 We did at Provident National Bank qualitative
20 research, and I stress that word because we did not nose-count
21 in the study done by the Darden Research Corporation of
22 Atlanta, Georgia, for us, of the Philadelphia banks market
23 perceptions of banks in general, banks in Philadelphia in
24 particular, and our bank as an even further particular.

25 In that study, we included an exploration of

1 consumer reaction to a telephone bank bill-paying service. The
2 reaction was strong, the reaction was emotional and the
3 reaction was negative.

4 But concern over invasion of privacy was not one
5 of the reasons for the negative reaction. Consumers were
6 concerned that they would relinquish control of their funds
7 to the bank. Consumers were concerned that they would lose
8 the ability to identify with their money. Consumers were
9 concerned that they would be inserting a third party — in
10 this case, the bank — into what they perceived to be a private
11 relationship they had with companies to whom they address
12 their checks.

13 One of them went so far as to say to us that
14 they enjoyed receiving the bill from the department store
15 and reading the perfume ads and that was as pleasurable an
16 experience as shopping. And they were afraid that the bank
17 would disrupt that relationship because they would not
18 receive the traditional stuffed enveloped.

19 Again, I stress it was a qualitative study, and
20 certainly I have no statistics to support that.

21 In the general portion of the study, when we're
22 not talking about the telephone bank bill-paying program, we
23 discovered some hints — and that is really what you do
24 discover, hints only, when you do this kind of research —
25 that leads us to believe that there may be an opposite set of

1 feelings to the concern over privacy questions.

2 We were criticized -- not "we" the Provident, but
3 "we" the banking industry -- for impersonality, and we were
4 urged to get to know more about our customers.

5 We were told that since we know so much about
6 them anyway, why do we keep asking them more questions when
7 we want to start a new service. They keep saying to us
8 "why don't you find out all you need to know the first time
9 I come to the bank so I can borrow money more easily."

10 We now believe, and we have in our marketing
11 programs employed this belief, that consumers want a banker
12 who would know a great deal about them so as to be able to
13 assist them in their banking needs.

14 We believe that customers are concerned over a
15 sense of sterility or impersonality of current banking
16 services, that they recognize the lack of recognition and
17 they feel a lack of appreciation; all of which, in our
18 view, goes against the feeling that they are concerned that
19 the bank will get to know too much about them.

20 We certainly believe -- and we certainly that
21 it ought to be part of regulations -- that the consumer should
22 have access to information stored about him, knowledge of
23 where it is being disseminated, and the ability to contest
24 the accuracy of that information if he has valid grounds for
25 that contest. We certainly would in our bank, and I certainly

1 think in most reasonable banks, would try to make a part of
2 a service revolving around that ability like part of the
3 marketing approach that we are making to the general public.

4 We also believe that there will be a continued
5 existence of the paper-based system. We have been selling
6 direct deposit of payroll accounts in our bank for many, many
7 years, and we prepare 600 payrolls in the Philadelphia area.

8 Only about 5 percent of all the paychecks that we
9 now provide are actually deposited directly into the bank.
10 There's only one piece of information that we need more than
11 what we now get in order to handle a person's payroll, in order
12 to provide direct deposit of payroll, and that is the name.
13 of the employee's bank.

14 We have a problem, I might add parenthetically,
15 in trying to fit that piece of information into an already
16 cramped computer program, but that certainly is not a problem
17 for that Commission.

18 We believe that as long as the paper-based system
19 continues to exist for the reasons I mentioned before, that
20 if there are people who are concerned with privacy who have
21 a feeling down deep in their hearts that they don't want
22 anybody to know where they bank, that those people continue
23 to use the non-EFT alternative.

24 And we believe that as a practical matter the
25 industry will be offering the non-EFT alternative for the

1 foreseeable future.

2 Mr. Chairman, I'm not sure that I've used ten
3 minutes. I really don't feel like reading that which I've
4 prepared for the Commission to read for themselves. And I
5 will answer questions if there are any.

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

64a

National Commission on Electronic Fund Transfers
Users Committee Public Hearings
"Consumers Issues in EFT"
October 26 and 27, 1976
Washington, D.C.

The documents which follow are submitted for the record
of this hearing by:

Barry I. Deutsch of
Provident National Bank, Philadelphia, Pa.

TESTIMONY ON
PRIVACY

before the
National Commission on
Electronic Fund Transfers
by

Barry I. Deutsch
Vice President and
Director of Marketing
Provident National Bank
Philadelphia, Pennsylvania
October 26, 1976

My first experience with the issue of privacy arose some 15 years ago when I was working as a teller for the First Pennsylvania Bank. One of my regular customers was a guard at Holmesburg Prison. Every payday he came to the bank with his check and deposit slip made out for \$125.

Standard procedure calls for tellers to write the amount of the check on the deposit slip and subtract the amount of the deposit, thus showing a record of cash disbursed. My routine with this customer was different and unvarying. Every payday he said, "Give me my receipt before you do your arithmetic." His purpose was to conceal the gross amount of his pay from his wife.

Twelve years later I forgot that lesson.

At that point I was serving in my present capacity, as Director of Marketing at Provident National Bank. Our bank has several branches which serve the waterfront and, as a result, does a fair amount of business with some waterfront unions and longshoremen.

As you are probably aware, the 'shape up' made famous in old Marlon Brando movies no longer exists. Now a telephone system is used to assign men to different jobs. At various times during the year bonus payments are made as for example for hazardous cargo, containerized cargo, and the like.

We thought it would be a sound advertising idea to open our branches early on those days and thus make it more convenient for the men to cash their checks and, perhaps, deposit some of the proceeds with us. We decided to make them aware of our desire to be of service by placing a taped message on the line which would recite to all the callers the facts that our branches were open and would remind the men to bring their bonus checks to us.

What we didn't count on is that many of them had their wives phone in for the next day's assignment and that many of the wives did not know of the bonuses.

All of this is background to the introduction of the central theme of this testimony, which is that consumer concern over privacy is often mis-interpreted by researchers and consumer advocates; that when it is properly understood it will be clear that it is a marketing

problem not a regulatory one; and, moreover, it is a problem that, for a certain segment of the public will never be resolved, thus mandating the continuation of the paper-based payment system.

When privacy discussions arise in the EFT context focus is generally placed on the fear of the consumer that some entity will obtain access to financial records through which other information about the consumer will be available. I might, parenthetically, state that the entity usually referred to in this context is the government.

Even the published notice for these hearings used as an example the possibility of electronic payment records being used by the Internal Revenue Service.

Yet the basis for the concern is not that records will be created which don't exist but that the relative ease and inherent capability of the system to disgorge such information makes the consumer even more vulnerable to incursions than he might otherwise be.

This point is granted.

The policy of our bank, operating in a paper-based environment, is to notify the customer of any governmental request for account records prior to complying with such a request. Thus, the customer is able to seek judicial relief from such an examination of his records if he is entitled to one.

We would welcome regulation making our practice standard for the industry in either a paper-based or EFT system.

However, research that I have reviewed indicates to me that the fear that most people have is that their financial secrets will be penetrated by someone nearer and dearer to them than the I.R.S. Most of the research I am referring to points to the spouse as the dangerous party.

In 1973 the Bank Marketing Association published the first definitive study of consumer attitudes towards automatic pay deposits and automatic bill paying. The study was known as PACE I and it did not bring good news to bank marketers.

All services examined in the report received only moderate or limited ratings for concept favorability and for expressed willingness to use the service, if offered. In that light the examination of the negative replies is more instructive than review of the comments of the relatively few who came out in favor of the innovations.

As it related to direct deposit of payroll, that study turned up

negatives in two areas: reasons for non-use of existing payroll deposit plans and relative importance of certain perceived disadvantages.

Appendix "A" to this testimony, with the permission of the B.M.A., details the results of that investigation.

In the first case 32% of the respondents, by far the predominant plurality, gave this reason for non-use: Like to deposit my own/want to see it. No verbatim touched on privacy.

In the second instance, 42% ranked the following disadvantage first when ranking disadvantages: Removes my control.

My theory is that the respondents meant, "It removes my control over the knowledge of the net amount. Under a pay check system, no one except the depositor knows that amount but when the pay is deposited directly into a financial institution's account, then anyone looking at the bank statement can see what the deposit history was.

The stated objection, "I like to deposit my own," does not negate my theory because we can hypothesize that what the respondent is saying is, "I like to deposit my own pay check because then I can pocket that amount which my wife does not know about."

In the bill paying category, the detail of which is appended, the negatives are again instructive. Here, however, we do come across the words: Too many people know my business. However, these concerns over privacy were the second least popular disadvantage expressed.

Only 7% of the respondents ranked that disadvantage as being most important and only 15% mentioned it either first or second. Loss of control over payment timing was of primary concern to 38% of the sample and at least second most important to 48% of the sample.

Objections that dealt with concern over errors, on the part of either the store or the bank, and those dealt with the desire to examine bills before payment were all mentioned more often.

That was 1973.

Now of course some banks have been about the business of EFT a great deal more. PACE II is on the drawing board. When it is performed we will add to it an attempt to evaluate consumer reaction towards POS services which may shed new light on this problem.

Last year, our bank did a number of focused group interviews covering a wide range of banking questions. Our purpose was to

gain insights into consumer thoughts about banks in general with specific reference to determining whether it was possible to differentiate any one bank on the basis of the manner in which it delivered service.

As an add-on to the survey we explored consumer reaction to several potential services that we may offer. Of interest to this commission was the reactions we received to a "telephone the bank" bill paying service.

Appendix C contains the description of the service which we offered the groups. Of all the services explored in this study, by the way all of the others were of a less technologically oriented nature, this concept met the strongest emotional response.

Participants did not see how or why they might benefit; although they did perceive that the bank or the creditors might benefit through speed-up of payments. They did feel that they would relinquish control of their funds to the bank; that they would lose the ability to identify with their money; and that they would be inserting the bank into the relationship they had with the companies to whom they addressed checks.

For those on tighter incomes, there was a threatening uneasiness based on their preceived concern over loss of the ability to decide which bills to pay...how much to pay...and which might be skipped.

The last source of considerable concern was that when errors occur, the customer would be largely dependent on the bank to correct them. Customers did not have confidence that the bank would make the effort to solve problems satisfactorily.

At no time in any of the discussions did the question of privacy come up; did anyone express concern over bank personnel or records obtaining easy knowledge over their personal affairs; or did anyone express discomfort over sharing their economic life with the bank.

In the more general portion of the study we not only did not find privacy to be an issue, but we found what some might be tempted to interpret as an opposite set of feelings.

Banks were criticized generally for impersonality...for not getting to know more about the customer and the customer better. One participant said, "Everything they need to know about me they already have -- if they would just refer to it."

It is, of course, not valid to draw conclusions from non-quantitative studies such as this one. However, there were strong signals.

We were persuaded that developing personalized, coordinated means of delivering service was a key element in a successful marketing strategy. We were persuaded that the customers wanted a banker who would know a great deal about them and thus be able to assist them and guide them through what they perceive to be a fairly complex financial system.

The overriding theme about the attitudes of the participants in our study was their sense of sterility and impersonality of current banking services, lack of recognition and guidance, lack of appreciation of the customer as an individual. Feelings were strong in this area, with people saying to us again and again that they were distressed about the piecemeal character of their relationships with the bank's personnel, bank accounts and services.

Certainly, the consumer should have knowledge of what information about him is in the possession of financial institutions and access to that information himself. He should know where it is being disseminated and he should be able to contest the accuracy of the information in his records.

All of the above is good marketing because the marketplace wants those rights. Yet, in my view, it is not the area where great stress has to be laid in order for EFT systems to be more marketable.

We as an industry have not been terribly successful so far in selling our EFT products.

Our ACH's do not have impressive volumes; our ATM's are dispensing more balance information than money; and our POS techniques have been most successful when they make check cashing easier, thus perpetuating in some respects the paper-based system.

There is a long list of what the financial institutions of this nation must do in order to satisfy the needs of the marketplace.

We have to demonstrate that we can cope with errors.

We have to design services which do not force the consumer to surrender control over the timing of his value transfers.

We have to provide bank statements which give clear, cogent and meaningful descriptions of the transactions so that the consumer will have good records of that which is put in and taken out of his accounts.

These are things that we must do ourselves.

All of that is basic marketing, determining the needs or wants of the consumer and planning how to meet those needs at a profit.

You will note that I did not include 'privacy' in my laundry list of marketing's action needs. My theory of what constitutes privacy among that set of consumers who are concerned about it leads me to believe that it is sociological issue. It is one which will not be responsive to either regulation by you or to selling techniques by us.

The question of a mandatory EFT system most often arises in the context of direct deposit of payroll. There is, however, general resistance to such a mandatory direct pay deposit service. The employee resents and most employers won't even consider it.

In every presentation that I have made to a possible user, the question of handling those employees who require a paycheck is raised early in the conversation. In every case we agree to provide that option.

It may turn out, as the hearing notice indicates, that in the long run the benefits of direct deposit of payroll through EFT will militate against allowing any employees to receive a paycheck. I believe that long run to be quite long indeed.

If that time does arrive then the discretionary spending patterns of some men, and women, is bound to change markedly.

Until it does privacy, as I have defined it, will be handled by shunting those who fear their spouses into the paper-based system.

APPENDIX A

REASONS FOR NON-USE OF EXISTING PAYROLL DEPOSIT PLAN

This Percent of the Respondents Whose Employer Offers a Payroll <u>Deposit Plan But Who Does Not Use It:</u>	
Gave these reasons:	<u>%</u>
Like to deposit my own/want to see it	32
Usually cash part of the check	13
Want cash on hand	7
Don't want to change banks	10
Fear of errors/delay	5
Don't have checking account	3
Have no reason to use it	12
Prefer credit union	1
Not convenient	1
Just don't like it	5
All other	2
Don't know/no particular reason	9

Source: PAGE I, A study of consumer attitudes on Automatic pay deposit,
Automatic bill paying, Consolidated statements, Bank Marketing
Association, Chicago, Ill., 1973.

APPENDIX A-2

RELATIVE IMPORTANCE OF CERTAIN DISADVANTAGES OF PAYROLL DEPOSIT PLAN

	<u>This percent of the Respondents:</u>
<u>Ranked these disadvantages</u> <u>as FIRST in importance:</u>	<u>%</u>
Removes my control	42
Employer might make a mistake	18
Bank might make a mistake	9
Other disadvantages	7
 <u>Ranked these disadvantages</u> <u>FIRST or SECOND in</u> <u>importance:</u>	
Removes my control	54
Employer might make a mistake	56
Bank might make a mistake	31
Other disadvantages	10

Source: PAGE I, op. cit.

APPENDIX B

RELATIVE IMPORTANCE OF CERTAIN DISADVANTAGES OF THE BILL PAYING SERVICE

This percent of the respondents:Ranked these disadvantages
FIRST in importance:

	<u>%</u>
Removes my control	38
Bank might make a mistake	5
Bill might be wrong	18
Might not want to pay a bill	9
Might not want to pay part of a bill	8
Too many people know my business	7
Other disadvantages	2

Ranked these disadvantages
FIRST or SECOND in importance:

Removes my control	48
Bank might make a mistake	17
Bill might be wrong	42
Might not want to pay a bill	25
Might not want to pay part of a bill	22
Too many people know my business	15
Other disadvantages	3

Source: PAGE I, op. cit.

APPENDIX C

THE "TELEPHONE THE BANK" BILL PAYING SERVICE:

The purpose of The "Telephone the Bank" Bill Paying Service is to help reduce the time you spend each month in paying your bills. Here's how it works...

1. When you get ready to pay your bills, you call the bank notifying the bill paying service department the specific creditors--stores, utilities, insurance companies, and so forth--that you want paid and the exact dollar amount to paid to each.
2. The bank forwards the payments to each of the creditors you have authorized to be paid, and deducts the total amount, depending upon which account you have selected for this purpose.
3. You receive a monthly statement showing all bills payed in the order in which they were handled. This statement is your proof of payment, the same as a cancelled check.
4. The bank charges you for this service on the basis of 10¢ for each bill paid.

Source: Qualitative Research Study...Retail Banking Market, prepared for: Provident National Bank, Philadelphia, Pennsylvania, August, 1975.

64m

Testimony on Privacy before the National Commission on Electronic Funds Transfers by Barry I. Deutsch, Vice President and Director of Marketing, Provident National Bank, Philadelphia, Pennsylvania October 26, 1976...Executive Summary

1. Consumer concern over privacy is often mis-interpreted by researchers and consumer advocates. When properly understood it is clear that coping with it is a marketing problem, and quite a difficult one.
2. Regulation requiring financial institutions to notify customers upon receipt of bona fide requests for records would have a salutary effect on some concerns and should be welcome.
3. The PACE I study conducted by the Bank Marketing Association revealed low concept favorability and expressed willingness to use automatic pay deposits and automatic bill paying. Stated reasons included concern over loss of control and possibility of error but concern over invasion of privacy was almost non-existent.
4. It is the witness' contention that when the average consumer uses the word "privacy" he is referring to his desire to maintain some secrecy from a spouse.
5. Qualitative research done by the witness' bank included an exploration of consumer reaction to a "telephone the bank" bill paying service. Reaction was strong, emotional and negative but concern over invasion of privacy was not a part of the results. Consumers voiced concern over feeling that they would relinquish control of their funds to the bank; that they would lose the ability to identify with their money; and that they would be inserting the bank into the relationship they had with the companies to whom they addressed checks.
6. In the general portion of the study the bank not only did not find privacy to be an issue, but found some indication of an opposite set of feelings. Banks were criticized for impersonality and urged to get to know more about the customer.
7. The witness' bank believes that consumers want a banker who would know a great deal about them so as to be able to assist them with

their banking needs. Customers are concerned over their sense sterility and impersonality of current banking services, lack of recognition, and lack of appreciation.

8. The witness believes that the consumer should have access to information stored about him, knowledge of where it is being disseminated, and the ability to contest the accuracy of the information.
9. However, notwithstanding point 8, the witness believes that in order for EFT systems to be more successful than they have been stress needs to be placed on:
 - a. error control
 - b. protection of consumer control over timing and recall of payments
 - c. well-accepted descriptive statements
10. The witness believes that the continued existence of the paper-based system is indicated by levels of resistance to EFT currently apparent. As long as the paper-based system continues to exist, those who are concerned with privacy, as defined by the witness, will continue to use the non-EFT alternative.

1 CHAIRMAN ATWATER: Thank you very much. You did
2 indeed leave two minutes free, and we will use that for
3 questioning.

4 Questions from the Commissioners?

5 Mr. Thorndike.

6 MR. THORNDIKE: I'm not sure if you were present when
7 Mr. Westin was describing the degree of flexibility on control
8 which a depositor might have over the use of information that
9 the bank would have concerning his account.

10 He was proposing that this could be very much to the
11 depositor's advantage and that there could be flexibility in a
12 completely computerized system that could be useful to him and
13 could, perhaps in some sense, represent a bank which was more
14 responsive to his needs, a more friendly and concerned bank,
15 which you seem to feel the depositor would like to have.

16 Do you feel that the development of that interest
17 and that direction would be valuable to your marketing efforts
18 and would be popular with your customers?

19 MR. DEUTSCH: Yes, sir, I do.

20 Because it was qualitative research,
21 I did not put verbatims into my testimony, but I would like to
22 read you one. As I said before, this particular study was
23 prepared for us -- and it will take me just a minute to find it.

24 It is three consecutive comments about the concept
25 of personal bankers. Personal bankers are those people who

1 theoretically know about a customer. We all know that in large
2 banks the only way they can possibly do that is to readily
3 access electronic records.

4 "I like the idea as long as he is well versed and a
5 jack of all trades."

6 That was one comment.

7 "I like person-to-person comment, but sometimes it's
8 a lot more convenient to pick up the telephone and call them."

9 They were afraid that if you assigned them a
10 personal banker they would actually have to come to the bank
11 each time, because they would have to discuss each of their
12 particular pieces of information each time.

13 And, finally, someone said, "I would certainly like
14 to have someone, as long as he only phoned me, because I find
15 it a lot easier to say no over the telephone."

16 Now, I believe that the marketplace wants a better
17 informed service industry. The marketplace wants the bank to
18 be able to say yes or no quickly, whatever the request, and the
19 only way we can do it is to store and access information.

20 CHAIRMAN ATWATER: Mr. Goldfarb?

21 MR. GOLDFARB: I would like to ask a non-privacy
22 related question, if I may. It involves an issue that, I
23 think, is very important to our inquiry.

24 If your bank were to offer debit cards which would
25 allow point of sale purchases, would you favor a mechanism

1 which would allow consumers to reverse a debit transaction if
2 he had valid claims against a seller of merchandise, something
3 analogous to the Fair Credit Billing Act protection with
4 credit cards?

5 MR. DEUTSCH: Yes, I would. I did not comment on it.

6 I did not comment on nearly all of the questions that were
suggested for the hearings. But we now have what is called a
stop-payment mechanism which somehow or another has to be perpetuated,
9 even over our operation's peoples dead bodies, even in debit transactions.

10 CHAIRMAN ATWATER: Are there other questions?

11 (No response.)

12 CHAIRMAN ATWATER: We certainly thank you, Mr. Deutsch,
13 for appearing before us today and for your thoughtful testimony.

14 MR. DEUTSCH: Thank you.
15
16
17
18
19
20
21
22
23
24
25

MR. WEGNER: Next we will hear from Mr. Charles Marson,
Legal Director of Northern California Civil Liberties Union.
(Witness sworn.)

CHAIRMAN ATWATER: I would like to welcome you,
Mr. Marson, to the Commission's hearing.

Mr. Marson is a very distinguished activist and
scholar in the field of privacy. Those
of you who know his background recognize the input that he has
made to some of the legislation that has evolved on privacy
issues.

So we would very much welcome your testimony today.

TESTIMONY OF CHARLES C. MARSON, LEGAL DIRECTOR,
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF
NORTHERN CALIFORNIA, INC.

MR. MARSON: Thank you, Mr. Chairman.

Mr. Chairman and members, I am the Legal Director of
the Northern California branch of the American Civil Liberties
Union. As in many things, California is in the frontier of
the dispute over financial privacy, and particularly, privacy
in those records held by financial institutions.

I have been involved directly in the dispute since its
public inception in 1972. I have briefed and argued to the
Supreme Court the cases that resulted in the upholding of the
Bank Secrecy Act. I have testified before Congressional
committees with respect to the amendment or repeal of that Act.
I have participated in the litigation in the California
Supreme Court that has arrived at a set of legal rules directly
contrary to the rules that the federal courts now must enforce.

1 And I have, after some difficulty, successfully participated,
2 along with the California Bankers Association, in enacting the
3 California Right to Financial Privacy Act, an omnibus statute
4 protecting customers' rights to privacy, which will go into
5 effect next year and will implicate not every financial
6 institution and every financial record in California, but the
7 effect of federal process on those records, as well.

8 I am pleased to respond to the Commission's kind
9 invitation to come to Washington and describe that experience
10 and those conflicting rules in the confidence that they will
11 highlight the valued choices that are before the Commission.

12 The Bank Secrecy Act of 1970 was probably born in
13 this room. It was a response to increasing technological change
14 in banks which had resulted in the circumstance that banks were
15 no longer making and keeping copies of the front and back of
16 most peoples' checks for a time suitable to government and the
17 many uses to which government put checks for the proof of fact
18 in proceedings of all kinds.

19 Representative Patman introduced a one-line bill.
20 It said banks shall keep copies of checks. By the time it had
21 emerged from the Congress, it was 27 or 28 pages long. It had
22 been largely amended by the Treasury Department and the Internal
23 Revenue Service who were the two agencies primarily concerned
24 with it, and it imposed a massive scheme of record-keeping and
25 reporting to the Federal Government.

1 The reporting was pervasive enough. Every domestic
2 cash transaction of more than \$10,000 was to be directly
3 reported to the Federal Government. Every monetary transaction
4 over an international border in any form of more than \$5,000
5 was to be directly reported to the Federal Government.

6 But the record-keeping schemes imposed by the Bank
7 Secrecy Act were so pervasive that, for example, the Bank of
8 America testified in court that the cost in the first year alone
9 of complying with it was \$394,000.

10 Basically, the record-keeping scheme of the Bank
11 Secrecy Act is that banks must make and keep copies of the front
12 and back of every check that goes through the system, and nearly
13 every other financial document in its possession, with exceptions
14 for repetitive kinds of documents, payroll checks, pension
15 checks, and the like. This came to our attention not because
16 of the Act primarily -- the Act largely, instead of imposing
17 rules, vests power to impose rules in the Secretary of the
18 Treasury -- but because the regulations adopted by the
19 Secretary of the Treasury took that power, that grant of power,
20 to its limit. The Secretary issued a long list of financial
21 documents -- checks, mortgages, the like -- copies of which had
22 to be kept, under the Bank Secrecy Act. Most of that list
23 relates to physical pieces of paper and, therefore, would not
24 impact the records -- kinds of records created by electronic
25 funds transfer systems, although one would, because part of the

1 demand was that for two years the Bank Secrecy Act required the
2 keeping of records sufficient to reconstruct a demand deposit
3 account, and still does, and in that sense would impact any EFT
4 records.

5 It came to our attention because of a small
6 newspaper in Marin County published the content of the federal
7 regulations, and we got literally hundreds of telephone calls
8 complaining about this new big brother surveillance system
9 that the Federal Government had initiated.

10 In the spring of that year I brought an action in
11 Federal Court representing a bank and several bank customers
12 and a bank president and was shortly joined by the California
13 Bankers Association who assessed, and, I think, quite correctly,
14 the mood of its customers to require that it side with the
15 customer rather than the government in this dispute. And both
16 of us took to the Supreme Court a case claiming this Act was
17 an unconstitutional scheme of invasion of privacy of customers.

18 We had won only part in the District Court; that is,
19 the District Court struck down the requirement of affirmative
20 reporting to the Treasury Department but upheld in its
21 entirety what concerns us here, the system of record-keeping.

22 On April Fool's Day of 1974, the United States
23 Supreme Court in a 6-to-3 decision, authored by Justice
24 Rehnquist, reversed the District Court insofar as it had granted

relied to either the banks or the customers and upheld the Bank Secretary

1 Act in its entirety. In doing so, it took a line typical of
2 the adjudications of that court in recent years. It was not so
3 much that the substantive claim of the litigants before it was
4 incorrect -- they reserved that claim for a later day. It was
5 that the litigants did not have standing to pursue it, it was
6 premature, that bank customers had no right to claim that the
7 scheme invaded their privacy until such time as the checks
8 required to be made and kept by the Bank Secrecy Act were used
9 in some proceeding against them.

10 This provoked three angry dissents from a predictable
11 crowd, Justices Douglas, Brennan and Marshall, who claimed that
12 it was a hollow charade to bifurcate the record-keeping of
13 banks from the accessing function of government and to say,
14 "Wait until government accesses those records until you make
15 this claim."

16 In April of this year, the questions that were left
17 open by the Supreme Court in 1974 were closed in a case called
18 The United States vs. Miller. A big building in Alabama burned.
19 The firemen discovered the remains of an enormous still.
20 Prosecutors, intent on convicting for tax fraud, filled out a
21 subpoena for a Grand Jury which they said was to meet the next
22 day -- actually, it was not to meet for another three weeks --
23 took those subpoenas to bank presidents hundreds of miles away
24 from where the alleged Grand Jury was to meet, served them on
25 the bank president with the demand that either they come across

1 with the records and give copies to the agents or they would have
2 to appear the next morning before the Grand Jury.

3 The bank presidents, not surprisingly, chose the
4 first, and without notifying the customers, gave the records to
5 the prosecutors. The prosecutors used them for proof of fact
6 to convict those that were operating the illegal still. The
7 Fifth Circuit Court Court of Appeals reversed that criminal
8 conviction on the ground that this violated the Fourth Amendment
9 rights of the defendants; that they had a right of privacy in
10 those checks and financial documents; that it had been invaded
11 not only because of the invalid Grand Jury subpoena, but also
12 for lack of notice to the customer and a chance to resist.

13 In April of this year the United States Supreme
14 Court, by a vote of 7 to 2, reversed that determination and
15 held, over the dissents of Justices Brennan and Marshall, who
16 would have opted for the contrary California rule, which I
17 will explain in a minute, Justice Powell, writing for seven
18 members of the Court, held that there is no protectable Fourth
19 Amendment interest that a bank customer has in his checks as
20 long as those checks are in the hands of the bank; that the
21 piece of paper was not a private transaction; that it was a
22 negotiable instrument; and that, therefore, the case was
23 governed by the general rule that a party who is implicated in
24 business records in the hands of a third party has no standing
25 to object to their production, rightly or wrongly, in response

1 to legal process, valid or invalid.

2 The dissenters were quoting cases and lines of
3 reasoning that have been developed by us and others in
4 California in the meantime. In 1974 -- in late 1974 the
5 California Supreme Court was faced with the first of the two
6 large questions that the California Bankers Association had left
7 open, and that was whether it was lawful for law enforcement to
8 access financial records without any kind of lawful process,
9 that is to say, without a valid subpoena and summons or search
10 warrant. The unanimous California Supreme Court said the
11 answer to that question was no, and suppressed evidence in a
12 criminal case which had been gained by the simple expedient of
13 a telephone call from a police department to a local branch of
14 the United California Bank and receiving by return mail copies
15 of checks and statements.

16 That left open the question of whether a depositor
17 had any defensible interest or procedural opportunity to assert
18 it, whether there was valid legal process--summons, subpoena or
19 search warrant.

20 Let me put aside the question of search warrant
21 because the search warrant is different from all other legal
22 process, implicates the prescreening by a neutral and unattached
23 magistrate, and is executed immediately and is not affected by
24 the rules that are proposed.

25 But as to subpoenas and as to summonses, the

1 California Supreme Court said, unless the customer is notified
2 and unless the customer is given an opportunity to assert such
3 rights as he or she may or may not have, then it is an unlawful
4 invasion of privacy for the bank to produce those records even
5 in response to an otherwise valid summons or subpoena.

6 That shape of California law finally, I think,
7 reversed the two vetos of legislative enactments that had
8 preceded that case, and last month Governor Brown signed
9 California's Right to Financial Privacy Act, a bill which
10 codifies the principle of notification to a customer whenever
11 process seeks his records in the hands of a bank. It codifies
12 the principle that the customer has time and opportunity to
13 resist that production.

14 The bill for three years in a row passed both Houses
15 of the California Legislature by overwhelming margins and was
16 vetoed by Governor Reagan on the claim that it would interfere
17 with the corporate law enforcement and was vetoed by
18 Governor Brown in his first year on the same claim, and was
19 finally signed this year, largely on the strength, I think, of
20 the fact that the court decisions had already settled the
21 legal issues involved.

22 Those experiences relate to financial records and,
23 by and large, to pieces of paper. EFT records are, obviously,
24 a little bit different; not so much different, though, that
25 some or all of these principles may not be immediately

1 incorporated into treatment of EFT records. The California
2 Right to Financial Privacy Act, for example, speaks not in terms
3 of the form the record takes, but its content, whether it deals
4 with financial information and whether it is in the possession of
5 financial institutions. There is no question in my mind that
6 the existing new California statute will affect EFT records, for
7 example, in the automated clearing houses that now exist in San
8 Francisco and Los Angeles.

9 But by and large, the California rule, influencing
10 perhaps 10 percent of the market, is this: The government may,
11 not access financial records without, first, lawful process;
12 second, notification to the customer of the existence of that
13 process; and, third, a period of waiting in which the customer
14 may consult a lawyer and assert such rights as he or she may
15 have in court.

16 The federal rule is just to the contrary. Everywhere
17 else except for Maryland, which has passed a similar statute,
18 everywhere else and in the federal system a bank customer has
19 no protectible Fourth Amendment interest -- that is to say, no
20 protectible privacy interest in bank records in the hands of
21 his bank. They may be accessed not only with valid process
22 without notice of the customer, but with invalid process and,
23 in fact, with no process at all.

24 The comparison of those two rules speaks volumes, I
25 think, to what this Commission ought to recommend to the

1 Congress and to the President with respect to rules governing
2 access to records generated by EFT systems.

3 But EFT systems escalate the privacy values that are
4 implicit in the controversy over bank checks. In the first
5 place, EFT systems will reflect more information than bank
6 checks do about the lifestyle, financial habits and social
7 characteristics of the people who engage in EFT transactions.

8 In the second, EFT records will be largely instantan-
9 eous. The government may be able to find out whether I
10 subscribe to the New Republic several days after I write the
11 check and it clears the clearing houses; in an EFT transaction
12 it could find out right away. A bigger difference is that it
13 could be used as a device for locating people. If I purchased
14 my plane ticket in San Francisco, I can be met at the plane in
15 Washington.

16 Third, because the technology of EFT makes this
17 larger data base much more quickly and easily retrievable than
18 sorting through millions of pieces of paper or millions of
19 microfiche, it may pass through the hands of the Federal
20 Government at some point in the financial transaction, and that
21 is of critical importance. The Federal Reserve, for example,
22 turns over millions of checks, but it would be technologically
23 somewhat difficult to skim information from them. Not true,
24 for example, with an EFT system.

25 But subject to that escalation of privacy values of

1 EFT over bank paper, I think that the rules that I have proposed
2 to the Privacy Protection Study Commission and the California
3 law, both by statute and decision, both now reflect
4 appropriate directions to recommend to the President and the
5 Congress. At a minimum, the government should be prevented
6 from accessing the records generated in the private sector by
7 EFT without compliance with these rules:

8 First, a data subject's privacy interest in the data
9 concerning him or her must be recognized by statute.

10 As I have said, the federal rule is that it is not
11 recognized by the Constitution of the United States.

12 Second, the data subject's standing to assert his
13 or her right should be conferred by statute.

14 United States vs. Miller says that the data
15 subject has no standing to assert those rights in the absence
16 of statutes.

17 Third, access by government to EFT data without
18 lawful process should be prohibited outright.

19 Up until a few years ago, it was the common, almost
20 universal, practice of banks to let government investigators
21 see bank paper without notice to the customer and without
22 lawful process, pursuant to a longstanding cooperative
23 relationship between the industry and between government which
24 was, after all, carrying out legitimate, respected,
25 law-enforcement purposes. But the data generated by bank

1 checks is sensitive and personal and ought not to be subject
2 to administrative discretion. The data generated by EFT is even
3 more sensitive and personal and ought to be affected by the same
4 rule.

5 Fourth, procedures for access to EFT data by
6 government should be regulated by statute.

7 In the years in which we had court decisions but no
8 statutes in California, there was chaos in our office in advis-
9 ing customers what their legal rights were; in the banks in
10 advising their tellers and their executives what rules to
11 promulgate, what policies, what procedures to follow. I think
12 the endorsement of the California Bankers Association of the
13 legislation that just passed is all the proof we need that we
should have clearly written, understood rules, promulgated in advance,
15 which are essential to so complex an area. Hundreds of
16 thousands of people are involved in protecting the confidential-
17 ity of bank records. Rules written in advance and reflected by
18 statute are essential to that effort.

19 Fifth, statutory regulations should provide for
20 pre-access notice to the data subject.

21 It does very little good for the subject of the data
22 to have a legal argument to assert against access to the data
23 when that access has already occurred.

24 Sixth, the data subject should be given by statute
25 a reasonable time to assert his or her right before access

1 occurs.

2 Now, if you seriously consider these last two rules,
3 in particular, you will hear from law enforcement that they
4 will cripple investigative efforts in a number of areas,
5 particularly in the investigation of white-collar crime. That
6 has been the battleground on which this battle has been fought
7 all along. The Bank Secrecy Act when it went through the
8 Congress in 1970 was ballyhooed by the Nixon Administration and
9 the Mitchell Justice Department as one of that year's two big
10 strokes against organized crime. The opposition to the
11 California law came largely from the California Department of
12 Corporations who said, wrongly, I am convinced, that they
13 could not enforce the corporate stock, security, and stock fraud
14 laws without access to many bank accounts without notice to the
15 customer and without an opportunity to resist that access. The
16 legislature thought it was the other way. The Governor finally
17 thought it was the other way. But that is what you will hear
18 from law enforcement, and I urge you to scrutinize those claims
19 carefully, the claim being that if you give the customer
20 notice and time to resist, that law enforcement will be greatly
21 hampered. That largely amounts to an argument that a search
22 warrant cannot be had because -- remember the difference with
23 a search warrant -- if there is probable cause, a search
24 warrant can be had ex parte from a judge without notice to the
25 customer. It can be executed immediately without any time to

1 resist.

2 By definition, that argument means there is less than
3 probable cause to search a record.

4 Frequently, the amount of suspicion that leads an
5 administrator or an investigator to search a record under these
6 circumstances is an example of the classic fishing expedition.
7 Notice is required to somebody who is the recipient of a federal
8 search warrant, notwithstanding the same argument in the
9 criminal context.

10 I hope that my suggestions for these rules will be
11 food for the committee's thought. I would ask, Mr. Chairman,
12 that my full statement, which goes into these rules in
13 much more detail, be incorporated in the committee's records.

14 And I would be pleased to answer such oral and
15 written questions as the Commission may have.

16
17
18
19
20
21
22
23
24
25

National Commission on Electronic Fund Transfers
Users Committee Public Hearings
"Consumers Issues in EFT"
October 26 and 27, 1976
Washington, D.C.

The documents which follow are submitted for the record
of this hearing by:

Charles C. Marson of
American Civil Liberties Union Foundation
of Northern California

NATIONAL COMMISSION ON ELECTRONIC FUNDS TRANSFER

STATEMENT OF
CHARLES C. MARSON, LEGAL DIRECTOR
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
OF NORTHERN CALIFORNIA

October 26, 1976

Washington, D.C.

MR. CHAIRMAN AND MEMBERS: My name is Charles C. Marson. I am the Legal Director of the American Civil Liberties Union Foundation of Northern California. I appreciate the opportunity to appear before you and to attempt to relate my experience with the law of privacy and financial records to the context of electronic funds transfer (EFT).

I briefed and argued the cases which resulted in the Supreme Court's historic decision in 1974 upholding the Bank Secrecy Act, and was subsequently involved in litigation in the California Supreme Court, and legislation in the California legislature, both of which achieved an opposite result. I have no doubt that the principles and procedures that California statutory and decisional law now apply to records of financial information in the possession of financial institutions would and could be applied to records generated by EFT systems. Moreover, I think they should be. I therefore narrate that experience in some detail here, in the hope that the contrast between the federal and California law concerning the privacy of financial information will highlight the important issues before this Commission.

In 1970 Congress passed the Bank Secrecy Act. Most of the Act's provisions were not self-executing but depended upon regulations to be issued by the Secretary of the Treasury. In due course those Regulations were issued and came to our attention in the spring of 1972, shortly before their effective date of July 1, 1972.

In June of 1972 I filed an action in the District Court for the Northern District of California which sought to enjoin the Bank Secrecy Act as unconstitutional. I did so on behalf of Fortney Stark (then a bank president, now a Congressman), the Security National Bank, the American Civil Liberties Union, and a number of bank customers directly affected by the Act. We charged in that suit that the Act constituted a massive violation of the First, Fourth, and Fifth Amendment rights of banks and bank customers. We were shortly joined in court by the California Bankers Association, an organization representing all the state and national banks in California, which advanced the same arguments. I should add parenthetically here that in 1972, only the California Bankers Association formally opposed the Bank Secrecy Act. Now, however, it has been joined by the American Bankers Association, which has taken the position before the Privacy Protection Study Commission that the Act should be repealed.

The provisions of the Bank Secrecy Act are probably familiar to you, and I summarize them only briefly here. The Act imposes on banks and other financial institutions the twin duties of recordkeeping and reporting on an unprecedented scale. Under the Act the Secretary of the Treasury is empowered to determine which financial records require preservation because they "have a high degree of usefulness in criminal, tax, and regulatory investigations and proceedings." 12 U.S.C., § 1829b. At the time we filed suit the Secretary had taken that mandate to its limit by requiring that banks make and keep copies of

every check, front and back, and nearly every other important financial record in banks' possession.^{1/} The Secretary also dictated retention periods for such records far beyond the current practice of many banks. The stated purpose of this massive recordkeeping was to preserve the records for inspection in connection with "criminal, tax, and regulatory proceedings" of all kinds.

In addition to the recordkeeping requirements, the Act also empowered the Secretary to require from banks and financial institutions the affirmative reporting to the government of two categories of transactions: domestic transactions in such amount as the Secretary required, 31 U.S.C., § 1082, and transactions involving the transmission of amounts in excess of \$5,000 into or out of the United States, 31 U.S.C., §§ 1101-05; 31 C.F.R., § 103.24. The latter requirement is statutory; the former was implemented by the Secretary by requiring reports from the institutions of most transactions involving more than \$10,000 in cash. 31 C.F.R., § 103.22.

In addition, the Act and Regulations bristled with other recordkeeping requirements (such as the identities and social security numbers of holders of domestic and foreign accounts), strict civil and criminal penalties for violation of the Act or Regulations, and broadly worded permission for the Secretary to make such exemptions from or additions to the Regulations as he

^{1/} In between the District Court and the Supreme Court the regulations were amended to restrict the requirement of copying checks to those drawn for more than \$100. 31 C.F.R., § 103.34 (b) (3) (1973). The California Bankers Association argued persuasively in the Supreme Court that this change was a meaningless cosmetic gesture because it cost them far more to sort out the checks than to copy them all.

saw fit.^{2/}

The three-judge District Court agreed with us only in part; it enjoined the requirement of reporting domestic transactions as a massive invasion of privacy prohibited by the Fourth Amendment, but declined to enjoin either the foreign reporting requirements or any of the recordkeeping requirements of the Act. Stark v. Connally, 347 F.Supp. 1242 (N.D.Cal. 1972). All sides appealed.

On April 1, 1974, the United States Supreme Court reversed the judgment of the District Court insofar as it had enjoined the Act, affirmed the judgment insofar as it upheld the Act, and declared generally that the Bank Secrecy Act was constitutional, at least as to these plaintiffs. California Bankers Association v. Shultz, 416 U.S. 21 (1974). The Court divided six to three; Justice Rehnquist, writing for the majority, rejected the argument that any interests of the banks were invaded and treated the privacy claims of the bank customers as premature, holding that:

Claims of depositors against the compulsion by lawful process of bank records involving the depositors' own transactions must wait until such process issues.

416 U.S. 51-52.

The majority of the Court therefore declined to decide whether the recordkeeping requirements of the Bank Secrecy Act violate the Fourth Amendment rights of bank customers, holding that customers have no standing to assert those rights until the

^{2/} The provisions of the Act, Pub. L. 91-508, 84 Stat. 1114, appear in 12 U.S.C., §§ 1829b, 1730d, 1951-59; and 31 U.S.C., §§ 1051-62, 1081-83, 1101-05, and 1121-22. The regulations appear in 31 C.F.R., § 103. The provisions of the Act and Regulations are summarized in more detail in California Bankers Association v. Shultz, 416 U.S. 21 (1974).

records are obtained by government and used against them.^{3/}

The majority also rejected every attack on the foreign and domestic reporting requirements of the Act, holding that claims of self-incrimination were premature until the evidence so obtained was actually used against customers, and that the requirement of reporting did not amount to an unreasonable search or seizure within the meaning of the Fourth Amendment insofar as banks were concerned. 416 U.S. at 63. The Court declined to decide whether bank customers were the subjects of unlawful searches and seizures by virtue of the domestic reporting requirements. 416 U.S. at 68.

Finally, the claims of the ACLU that compulsory record-keeping in effect made its membership available to government was held premature until such time as the Government could be proved to be seeking the records of its contributions. 416 U.S. at 56.

Justice Powell, joined by Justice Blackmun, filed a concurring opinion but cautioned that if the domestic reporting requirement involved transactions any smaller than \$10,000 in cash he would have grave constitutional reservations:

A significant extension of the regulations' reporting requirements, however, would pose substantial and difficult constitutional questions for me. In their full reach, the reports apparently authorized by the open-ended language of the Act touch upon intimate areas of an individual's personal affairs. Financial transactions can reveal much about a person's activities, associations, and beliefs. At some point, governmental intrusion upon these areas would implicate legitimate expectations of privacy. Moreover, the potential for abuse is particularly acute

^{3/} The Court also held that bank customers had no Fifth Amendment right against self-incrimination in records "produced" by a third party. 416 U.S. at 55.

- 6 -

where, as here, the legislative scheme permits access to this information without invocation of judicial process. In such instances, the important responsibility for balancing societal and individual interests is left to unreviewed executive discretion, rather than the scrutiny of a neutral magistrate.

416 U.S. at 78-79.

Justices Douglas, Brennan, and Marshall all filed dissenting opinions. Justice Douglas thought the Act violated the Fourth Amendment because of its scope, saying:

It is, I submit, sheer nonsense to agree with the Secretary that all bank records of every citizen 'have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings.' That is unadulterated nonsense, unless we are to assume that every citizen is a crook, an assumption I cannot make.

416 U.S. at 85
(emphasis in original).

Justice Brennan agreed, but in addition would have held that the Act unconstitutionally vested impermissibly broad authority in the Secretary of the Treasury.

Justice Marshall thought the Act and Regulations violated all three of the First, Fourth, and Fifth Amendments. Perhaps for the Commission's purposes the most telling point made in any dissent was by Justice Marshall in attacking the majority's view that the bank customers had no standing to assert their Fourth Amendment rights until the records were used against them. After pointing out that the recordkeeping and reporting requirements were not separate but part of the same system of governmental access because many records were examined informally and most others without notice to the customer, he said:

By accepting the Government's bifurcated approach to the recordkeeping requirement and the acquisition of the records, the majority engages in a hollow charade whereby Fourth Amendment claims are to be labeled premature until such time as they can be deemed too late.

416 U.S. at 97.

These, however, were dissenting views. The majority of the Court managed to uphold the Bank Secrecy Act while avoiding the Fourth Amendment and privacy claims of the bank customers on the ground that they lacked standing to sue until such time as they could demonstrate the use of such records against them. Whether they would have standing in such a case was left an open question.

That question was closed rather dramatically in April of this year by the Supreme Court's decision in United States v. Miller, ___ U.S. ___, 48 L.Ed.2d 71. In Miller the Court of Appeals for the Fifth Circuit, in a criminal prosecution, had ordered the suppression of evidence gained from bank records. Prosecutors had served a defective grand jury subpoena on two banks, falsely claiming the grand jury was meeting the next day, and had received copies of bank records from the banks. The customer was not notified. The records existed under the compulsion of the Bank Secrecy Act.

The Supreme Court overturned that result, holding in a seven-to-two decision that the customer "had no protectable Fourth Amendment interest in the subpoenaed documents ..." 48 L.Ed.2d at 75. Mr. Justice Powell's opinion for the Court stated, "We must examine the nature of the particular documents sought to be protected in order to determine whether there is a legitimate 'expectation of privacy' in their contents." Id. at 78-79. The Court concluded that bank checks are not private papers but are negotiable instruments used in commercial transactions; that the customer who communicates information on a check to his bank takes the risk that the bank will communicate it to others; and that therefore the case was governed by the general rule that the subject of business records in the hands of a third party has no standing to challenge a subpoena directed to those records. Id. at 76-80.

Justices Brennan and Marshall dissented, saying they would have resolved the question as had the California Supreme Court,

and reiterating their views that the Bank Secrecy Act is unconstitutional. Id. at 81-87.

Justices Brennan and Marshall were relying on developments in the California Supreme Court in between California Bankers Association v. Shultz and United States v. Miller. The California Supreme Court had shortly resolved the two most important questions left open by California Bankers Association v. Shultz -- whether access to bank records without lawful process violates the customer's privacy, and whether access pursuant to lawful process without notice to the customer violates the customer's privacy. Both cases were resolved unanimously in favor of the bank customer's right to privacy, and both cases establish rules plainly applicable to records generated by EFT systems.

The first was Burrows v. Superior Court, 13 Cal.3d 238 (1974), a prosecution of a lawyer for misappropriating the funds of a client. The alleged crime was proved in part by bank records obtained by police by means of a telephone call and without any more formal process. Unanimously the California Supreme Court suppressed the evidence, holding that "any bank statements or copies thereof obtained by the sheriff and prosecutor without the benefit of legal process were acquired as the result of an illegal search and seizure" Id. at 245.

In the course of its opinion the Court in Burrows rejected two arguments highly relevant here. The first was that the customer had lost any right of privacy by furnishing the information to the bank. But the Court said:

A bank customer's reasonable expectation is that, absent compulsion by legal process, the matters he reveals to the bank will be utilized by the bank only for internal banking purposes.

Id. at 243.

The other argument was that there was no search and seizure because the bank had voluntarily given the records to the

police. The unanimous Court replied:

It is not the right of privacy of the bank but of the petitioner which is at issue, and thus it would be untenable to conclude that the bank, a neutral entity with no significant interest in the matter, may validly consent to an invasion of its depositors' rights.

Id. at 245.^{4/}

Burrows established for California law^{5/} the principle that access by law enforcement of bank records without lawful

^{4/} The principle of Burrows has been applied by a California appellate court to telephone toll records, People v. McKunes, 51 Cal.App.3d 487 (1975); and distinguished where the bank is itself a victim of the reported crime. People v. Johnson, 53 Cal.App.3d 394 (1975).

^{5/} California has special protection for privacy in its state constitution. In 1972 the voters added to the list of inalienable rights the right of "privacy." California Constitution, Article I, Section 1. Although this new right has received very little judicial interpretation outside of the context of bank records, the state Supreme Court has held that the state constitutional right to privacy is self-executing, can only be overcome by the demonstration of a compelling governmental interest, and is directed at these specific evils:

(1) 'government snooping' and the secret gathering of personal information; (2) the overbroad collection and retention of unnecessary personal information by government and business interests; (3) the improper use of information properly obtained for a specific purpose, for example, the use of it for another purpose or the disclosure of it to some third party; and (4) the lack of a reasonable check on the accuracy of existing records.

White v. Davis, 13 Cal.3d 757, 775 (1975). Such protections are perhaps unique in state law but are very similar to the principles of the Privacy Act of 1974.

process is an unlawful search and seizure, but it did not measure the right to privacy against lawful process. That question was resolved in December of 1975 in Valley Bank of Nevada v. Superior Court, 15 Cal.3d 652.

In Valley Bank the bank had sued customer A on a note. Customer A had claimed collusion between the bank and its customer B, and, pursuant to state civil discovery law, compelled the attendance of the bank president at a deposition and commanded him to bring along the bank records of customer B. In an unusual move (perhaps because customer B was the Teamsters Union), the bank resisted. A hearing was held at which customer A and the bank were represented but customer B was not. The trial court ordered production of the records but the state Supreme Court unanimously overturned that order, holding that the right of privacy required that

the bank must first take reasonable steps to locate the customer, inform him of the discovery proceedings, and provide him a reasonable opportunity to interpose objections and seek appropriate protective orders.

15 Cal.3d at 654.

The most recent California development is that the Legislature has passed, and the Governor has signed, a statute which will go into effect at the first of next year entitled the California Right to Financial Privacy Act. That Act, subject to only a few exceptions, outlaws access by government to financial records without legal process, requires notice to the customer of that process, and requires a waiting period before access is permitted in which the customer may go to court to contest the process.

Both the federal and California rules developed in the context of access to bank records are directly applicable, in theory at least, to records of EFT transactions. The federal rule is premised on the notion that the holder of the records,

- 11 -

rather than the subject of the records, owns them, and that therefore the subject has no constitutional right in those records to assert. The California rule, both by statute and decision, follows the premise that the privacy interest belongs to the customer, not the record custodian, and that the customer must therefore receive notice of attempted access to those records and have a fair opportunity to resist it. Both those lines of reasoning are obviously applicable to EFT records; in fact, the new California statute would cover such records even as currently written.

There are, however, differences between today's bank records and tomorrow's EFT records. Those differences argue for even greater protection of privacy in EFT records.

The first major difference is that EFT records, assuming widespread acceptance of EFT systems, will contain far more information than will, say, a check drawn on a bank. EFT records will show where a particular individual was at a particular time, the financial resources of that individual, and under some circumstances who he or she was with. If most transactions now conducted in cash become transactions conducted by means of EFT, it will be possible to reconstruct the movements and activities of customers in a detail unknown today.

The second major difference is that EFT records will provide information almost instantaneously, while substantial time may pass before bank records will yield desired information. It is not hard to envision, for example, the interfacing of EFT systems with lists of persons wanted by government for law enforcement or other purposes, so that the subject of interest may be located within minutes of engaging in an EFT transaction.

A third difference of some substance may be that data generated by EFT may be much more readable, and therefore more accessible, than records such as bank checks. It is doubtful, for example, that the Federal Reserve System could easily "skim"

- 12 -

much useful information off bank checks that pass through its hands. The same practical limitations may not exist for EFT-generated data.

I have previously argued to the Privacy Protection Study Commission that in order to protect the privacy of the subjects of financial records, any statutory or regulatory scheme must follow at least six basic principles. All six are at least as applicable to records of EFT transactions. They are:

First, a data subject's privacy interest in the data concerning him or her should be recognized by statute. The Privacy Act of 1974 accomplishes this purpose with respect to individually identifiable data possessed by the federal government. Similar statutory recognition would be required for EFT data possessed by the private sector.

Second, the data subject's standing to assert his or her rights should be conferred by statute. Otherwise the Supreme Court's Miller decision would probably govern the matter.

Third, access by government to EFT data without lawful process should be prohibited outright. Until recently, access to bank records by government without process was widespread. There is no justification for such a cavalier approach to customers' privacy. Most segments of the industry now insist on process.

Fourth, procedures for access to EFT data by government should be regulated by statute. The retroactive, piecemeal development of case law, if in the federal courts it would occur at all, is much less desirable than rules well known and spelled out in advance.

Fifth, statutory regulation should provide for pre-access notice to the data subject. A right one has no opportunity to assert is no right at all. A right the holder of EFT data must assert is hardly better; for all but the most favored customers the holder will either notify the subject after the fact or not

- 13 -

at all. The subject should make his or her own decisions and arguments.

Sixth, the data subject should be given by statute a reasonable time to assert his or her rights before access occurs. Nearly all legal process (except a search warrant) is issued by lawyers and clerks, not by judges. The legality of such process is not tested in advance. The only way to breathe substance into the privacy interest of the subject of EFT data is to give, as the California statute does, sufficient time (for example 10 days) in which a lawyer can be consulted and a motion made.

I am pleased to have this opportunity to state my views. I will try to answer any questions you may have.

1 CHAIRMAN ATWATER: Are there now questions from
2 the commissioners?

3 Mr. Tangney?

4 MR. TANGNEY: Just a point of inquiry.

5 Did not the Tax Reform Act of 1976 include pro-
6 visions similar to the ones you just listed to us?

7 MR. MARSON: It did. They are limited to admini-
8 strative summonses issued by the Internal Revenue Service.

9 MR. TANGNEY: But the customer must be notified
10 of such a summons?

11 MR. MARSON: That is what I understood.

12 MR. TANGNEY: So there are federal laws now that
13 put some of the provisions that you indicated into effect?

14 MR. MARSON: They do. They are all specialized.
15 There are even federal laws that go further than that,
16 especially with respect to tax returns and with respect to
17 census data and make them not accessible at all, or accessible
18 in certain circumstances even more limited than I urge.

19 MR. TANGNEY: This act specifically goes to
20 financial institutions and their records?

21 MR. MARSON: It does.

22 MR. TANGNEY: Thank you.

23 MR. MITCHELL: Mr. Chairman?

24 CHAIRMAN ATWATER: Governor Mitchell.

25 MR. MITCHELL: I had a couple of questions, and I

1 would like to get your comment on them.

2 The way EFT seems to be developing, it is going to
3 utilize present practices which involve convenience credit.
4 You haven't said anything about protection against privacy
5 exposure on the part of two- and three-party credit cards,
6 and they contain a great deal more information about the
7 nature of the purchase or the time of the purchase and the
8 character of the purchase than will ever be found in any
9 bank record. I wonder why you aren't concerned.

10 My second question is that your statement seems to
11 imply that the issue is more acute and serious than it
12 was in a paper-based system. There, again, I would address
13 a similar question that I raised earlier: Is there really
14 a difference in the environment today by virtue of EFT,
15 since EFT has provided accessibility to transactions for at
16 least a decade in most financial institutions?

17 And is it true that the document that is unearthed
18 is a document that has to be pulled out by considerable labor?
19 The information is available in the kinds of systems that
20 we have.

21 MR. MARSON: Mr. Mitchell, the reason that I have
22 not mentioned credit cards is that my focus has been on
23 access by government and largely, the rules of the Bank
24 Secrecy Act. The regulations promulgated under the Bank
25 Secrecy Act in their first draft

1 form, included the records of credit card systems. But, by
2 political discussion -- these details are unknown to me --
3 the Secretary amended out that application when the regula-
4 tions went, finally, into effect.

5 Now, it is entirely true that credit card
6 information contains much the same kind of information that
7 I assert here is very sensitive and private in the context of
8 EFT. The Privacy Protection Commission, as you know, is
9 considering extending the principles of that act to credit
10 card systems. And, as a matter of fact, at least American
11 Express and those systems based in California, to my knowledge,
12 and perhaps some others not to my knowledge, have already
13 voluntarily adopted the policies I urge here for credit card
14 systems.

15 Now, there is some difference in dynamics. A
16 consumer wants credit information available so that credit can
17 be extended. The consumer is not particularly desirous of
18 IRS subpoena power. So there is that difference. But I do
19 not see why these rules ought not to apply to credit card
20 records as well.

21 In answer to your second question as to whether a
22 paper-based system and a computer-based system are really
23 different, I think they are different qualitatively for a
24 couple of reasons. It is sometimes asserted -- and I think
25 it is in the hearing notice -- that an EFT system would be

1 more protective of privacy, because anyone can access a piece
2 of paper, but only a specialist can access EFT data.

3 The witness twice before me said thing- that I,
4 of course, have no technical background to understand, about
5 how even that smaller universe of specialists can be either
6 trained or corrupted to access that data. But let me put that
7 aside.

8 The big difference is that there is more informa-
9 tion than in the paper-based systems, and it is more easily
10 retrievable. It is a well-known irony that inefficiency of
11 paper-based systems is probably the biggest protector of our
12 privacy, that the cost of the retrieval of information is
13 probably the biggest limitation on its widespread dissemina-
14 tion. EFT and computers of course, cut directly against
15 that. And it is certainly true that the more efficient the
16 information acquisition and retrieval system is, the more
17 critical the privacy concerns become.

18 This was one of the big issues in the flap a few
19 years ago about the National Data Bank, in which it was widely
20 pointed out that, in theory, it was possible to access
21 every record about an individual, from dozens of
22 manual files spread, perhaps, all over the country. But, as
23 a practical matter, it was not economical or even very obvious
24 to do. If it was all together in a single place, responsive
25 to a single button in Washington, the dynamics of access are

1 totally different.

2 And, even if you put aside the problem of the
3 honesty and reliability and responsibility of the people who
4 are pushing the buttons -- security is not my field. I have
5 no reason to talk about how to keep a system to comply with
6 the rules that it has. My concern is the rules that the
7 system has.

8 So I think, certainly, there is a difference in
9 kind between electronic data and paper data. There is more
10 of it; it is more centralized; it is more easily accessed.
11 And, of course, it has that aura of infallibility that a com-
12 puter printout always has that the handwritten scratch in a
13 manila file never does.

14 CHAIRMAN ATWATER: Ms. Koplow?

15 MS. KOPLow: Mr. Marson, may I follow up a bit on
16 the type of questioning I had with Professor Westin and ask
17 you if, with all of the work that you have done on the Bank
18 Secrecy Act,
19 you conceive that it is possible for this commission to write
20 the kind of laws and regulations that
21 would govern consumer access to EFT services prior to the
22 time that
23 the consumer would have the use of the electronic
24 fund transfers?

25 MR. MARSON: I personally do. I point to the fact

1 that the California legislature has already done so. It has
2 done so at the urging of the banking community that is already
3 deeply into EFT.

4 Second, the rules that I propose are rules that
5 govern access to either kind of record. EFT is not a
6 different record. It is still the same financial information
7 that takes place. EFT is a manner of collecting and dis-
8 seminating that information. Whereas, before, an anonymous
9 cash transaction could take place, now an EFT transaction
10 will take place. Information that existed but was not
11 centralized in a retrievable place will then be centralized
12 in a retrievable place.

13 You are not without analogies in the paper-based
14 system of the maintenance of financial records. It is new
15 in the sense that it is technologically different. But,
16 in the sense that it impacts privacy, you have all the ex-
17 perience you need, I feel, from the paper-based system and
18 from the disputes over how government and banks and customers
19 treat that paper, if it contains that information, to promul-
20 gate rules for EFT data.

21 CHAIRMAN ATWATER: A general question. I noted
22 that the initiatives on this front to date have originated,
23 apparently, at the state level.

24 Is there any observation you would have concerning
25 the direction in which the commission should address its

1 interests or efforts on this subject?

2 MR. MARSON: Yes, Mr. Chairman, there is.

3 Banking and financial transactions are uniquely
4 interlocked across the country and, in fact, across the
5 world. I don't favor the development of separate, state-by-
6 state rules. We faced this problem when the District Court
7 in 1972 originally enjoined a portion of the Bank Secrecy
8 Act.

9 We fought for hours over the geographic and
10 physical scope of that injunction. And the judge finally
11 threw up his hands and enjoined the system nationwide. We
12 could not write an order which would protect privacy in the
13 District Court area in California that would interfere, in
14 large part, with banking operations all the way to Switzerland.

15 These transactions are so interlocked that they
16 ought to be governed by federal rules. There is a definite
17 trend, in the absence of action by the Congress and by the
18 executive branch, to pass those rules at the state level.
19 California was the second; Maryland was the first. California,
20 being influential, will not be the last.

21 In the next few years you will see many more
22 state laws like that, sponsored, among others, by the American
23 Civil Liberties Union. The trend is clearly for those kinds
24 of protections. The drift is clearly for privacy.

25 It was only the California Bankers Association in

1 1972 who was willing publicly to assess the mood of its
2 customers vis-a-vis its relationship with the government and
3 side with the former. In April of this year, the spokesman
4 for the American Bankers Association testified in support of
5 the six principles I have espoused here to the Privacy
6 Protection Study Commission and, in answer to a question from
7 one of the commissioners, said, "We think the Bank Secrecy
8 Act ought to be repealed."

9 It is clearly the trend among industry, as Mr.
10 Deutsch's testimony, for one of many examples, indicates, to
11 impose these rules on themselves, even in the absence of
12 federal statutes. It is not that these rules will not be
13 imposed; it is a question of, from where?

14 My urging to you is that it be at the federal
15 level and that it be uniform and that it adapt itself to a
16 nationwide banking community.

17 CHAIRMAN ATWATER: Thank you.

18 Are there other questions by the commissioners?

19 (No response.)

20 CHAIRMAN ATWATER: If not, we would like to thank
21 you very much, Mr. Marson, for your thoughtful testimony.

22

23

24

25

CHAIRMAN WIDNALL: The next witness is Carol Greenwald, Commissioner of Banks in Massachusetts.

(Witness sworn.)

1 TESTIMONY OF CAROL GREENWALD, COMMISSIONER OF
2 BANKS, MASSACHUSETTS.

3 MS. GREENWALD: I thank the commission for this
4 invitation to speak before you today.

5 The main thrust of my remarks is that, although
6 privacy has been taken to be the main consumer issue in EFTS, ...
7 and although I think it is important, I believe that the main
8 consumer issue in this, as in other banking developments, is
9 the preservation, or even the promotion, of competition in the
10 provision of services. And that should be the main concern
11 of this commission, to insure that developments unfold in
12 a pro-competitive manner.

13 I believe that is most likely to happen if we rely
14 most heavily on the market rather than on bank regulatory
15 agencies to direct EFTS development and that development of
16 the EFTS be monitored by a national commission similar to
17 this commission which would oversee what developments did take
18 place and if there were any troublesome consumer abuses and
19 then make recommendations from actual fact rather than from
20 hypothesizing about what may occur in the future, when, in
21 fact, we do not have EFTS right now and that we do not know
22 if there will be troublesome abuses that the market itself
23 will not take care of.

24 I believe that the main point of public policy
25 should be that it sees that consumer convenience is maximized.

1 Usually, we presume that the marketplace and competition will
2 assure this happening and that consumer satisfaction will best
3 be realized by market determinations. And we have jumped to
4 another assumption in this case, simply because EFTS involves
5 banks, and we are so used to regulating whatever banks do
6 that there is the assumption that this has to be regulated
7 by statute also.

8 I think we should take another look at that
9 assumption. It seems to me that EFTS is much more of a
10 communications device, maybe more similar to the telephone
11 than it is to a new banking service. It is simply a new
12 delivery of an old banking service.

13 Consumer convenience has been discussed in several
14 areas. I would like to focus on a few of these.

15 One is what would normally be called "location,"
16 but, because we have tried to fit EFTS into a banking mode,
17 we call the "branching question." It seems obvious to me that
18 geographic restraint on EFTS will not enhance performance of
19 the EFTS system, and that concerns about consumer convenience
20 is not why people have talked about constraints on where
21 these are located. Instead, there has been too much concern
22 expressed about the impact of EFTS on small banks, its impact
23 on the McFadden Act, and much less focus on what could best
24 serve the public or maximize consumer convenience.

25 It doesn't seem likely that EFTS will be a major

1 factor in geographic market extension beyond commuting areas.
2 But it is obvious that within a commuting area, and if a
3 commuting area goes over branching boundaries, that it will
4 affect market shares within that area. But if this comes
5 about because of technological change and this technological
6 change has some negative impact on some institutions and a
7 beneficial impact on other institutions, I cannot see the
8 role of government as preventing that from happening.

9 The role of government is not to prevent switching
10 because the consumer chooses another product or another
11 location. It is to allow the consumer to have maximum choice.
12 So, as I see it, the argument over whether terminals are
13 branches is, first, an argument among financial institutions
14 which is geared to their own insecurities and desires for
15 protection from competition. And it is, second, an argument
16 among regulators seeking extensions of their regulatory range.
17 It is not an argument about how the public can best be
18 served.

19 Well, what about small banks' fears that
20 they will be driven out by the high cost of EFTS and sophisti-
21 cated technology, and aren't there other consumer benefits
22 that I am overlooking, like the benefit of
23 preserving small banks?

24 I don't think the costs have indicated in any way
25 that they would preclude small bank participation in EFTS.

1 Now, clearly, it would be enormously
2 expensive if every bank has to put up its own terminal and
3 its own computer system in every retail outlet in its market
4 area. But that is an absurd proposition. No retail store is
5 going to allow a different terminal for every bank in its
6 market area. Instead, we are going to have shared hardware
7 and shared software.

8 And we have that right now. The small banks and
9 medium-sized banks are on computers. Virtually everybody is
10 on computers right now, but it doesn't mean every bank has a
11 computer system. They either use nonbank computer processors,
12 or they use their correspondent bank to do their computer
13 processing for them.

14 EFTS will simply fit right into that. There will
15 be a pro rata sharing of costs, which will make it just as
16 economical for a bank, a small bank, to be a part of EFTS
17 as it is for a small bank to have its bookkeeping done by a
18 computer, which most small banks do. So I think the cost
19 element has really been a fear that has been raised in the
20 minds of small banks but, really, without foundation. Cer-
21 tainly, ATMs are less costly than opening branches, less
22 costly to maintain, and, therefore, are not a threat to the
23 branching possibilities of the small banks.

24 There is some misunderstanding, I think, in
25 the difference between

1 mandatory sharing of software and another term which I
2 would call "nondiscriminatory access." Clearly, we want
3 nondiscriminatory access. If a large bank is putting up a
4 system and it is allowing other banks into it, then it should
5 have to allow other banks into it on a nondiscriminatory
6 basis, once it allows a second bank in.

7 That is not the same thing as saying that every
8 terminal must have mandatory sharing of the software in there,
9 that every terminal must be used by everybody who wants to use
10 it. We have the example of Citibank in New York.

11 There seems to be no reason at all why, if some
12 bank wants to try a proprietary system, it should not be
13 allowed to try it and see if it can market it. I believe,
14 in the long run, that is going to be very uneconomic, and
15 most retailers will not stand for it, because they would
16 simply have to have too many terminals. But if somebody can
17 sell it because they have a better service package, then all
18 the more power to them, and let everybody else then try to
19 copy it.

20 The problem with mandatory sharing, in the
21 beginning -- I believe we have to sort of distinguish the
22 short run from the medium run to the long run. In the
23 beginning, if you start off with mandatory sharing, then you
24 are going to end up with a software package that meets the
25 lowest common denominator of what all the banks in the group

1 are willing to pay for.

2 The smaller banks are going to be less willing to
3 foot the bill for research and development costs for
4 services that are uneconomic for their scale of operation.
5 The larger banks aren't going to be willing to pay for it all
6 if they can't have a monopoly profit out of it. So what you
7 will get if everybody has to join--or, if there is one
8 program and everybody can join, then everybody is going to
9 have pro rata sharing at the very beginning--is

10 a software package which is not the most
11 innovative, but one which simply meets the agreement of a
12 large mass of banks.

13 So I would urge, not the encouragement of the
14 mandatory sharing in the legislation, but simply nondis-
15 criminatory access, which is a different thing.

16 Another area of consumer concern which I think
17 will be handled by competition is this area of whether EFTS will
18 take away from the consumer some services, financial
19 services, that now exist; namely, the use of float or delayed
20 debiting?

21 And I don't think that is necessarily at all
22 what will happen with EFTS. Of course, the banks would like
23 that to happen, but there is another party in this whole
24 transaction, and that is the retailer. The retailer is
25 quite well aware that people will not buy as many things if

CONTINUED

2 OF 6

1 they have to pay for them out of their checking account
2 immediately. And, since point-of-sale terminals are going
3 to be operated through retail establishments, I believe we
4 can assume that pressures from the retailers will insist
5 that there either be a delayed debit card or that the credit
6 card will have automatic debiting without any charge.

7 I think, also, retailers will insist that the
8 terminals take a variety of cards. Retailers are quite well
9 aware that, in this case, the sum of the parts are greater
10 than the whole. People will buy many more things if it is not
11 on one bill. Having several charge cards with several bills
12 leads to the kind of purchasing which does not happen when
13 it is always going to come back on one bill. And their
14 pressure and their cooperation is absolutely essential for
15 an EFTS network to be put up in their establishment. And
16 I think we can assume that the retailers coincidence of
17 interest with the consumers will, in this case, prevail and
18 that we can rely upon the marketplace to produce this desirable
19 consumer objective.

20 The issue that has been addressed this morning,
21 consumer protection problems, privacy, and fraud and theft,
22 in general, I think, has been overstated -- not this morning,
23 but in many discussions -- that EFTS will magnify this
24 problem beyond what now exists. I think the problems are not very
much magnified at all by EFTS.

1 First, all financial transactions or virtually all
2 financial transactions are on computer now. We are in an
3 electronic age. Paper exists, but if you want this informa-
4 tion, you get it out of a computer printout. This is reflected
5 in the way banks are examined.

6 We have gone into EDP examinations, because
7 bookkeeping is not done by bookkeepers anymore. It is all
8 in computers.

9 There are various ways of maintaining privacy
10 through an EFTS system. You can use various codes; you can
11 require telephonic confirmation of transfers above a certain
12 amount. And, certainly, as part of regulatory examinations,
13 the necessary safeguards would be checked for in EDP examina-
14 tions.

15 The idea of a lost debit card or counterfeit debit
16 card doesn't seem to me to be a much bigger problem in EFTS
17 than lost credit cards are now.

18 I am not saying there are no problems here. I am
19 just saying I don't think they are terribly magnified by
20 EFTS, and that, if there is a need for changing present
21 statutes, it arises out of present bank practice, and it is
22 not simply created by this new electronic system.

23 I was very interested in the last speaker's
24 remarks. I would have thought that the U.S. banks used the
25 same standard as British banks. A historian in a very recent

1 issue of Banker's Monthly says that, I think it was the Bank
2 of England -- or, no, Lloyd's Bank -- got a request from the
3 British government for some financial data having to do with
4 the Governor of India. And the bank wrote back and said,
5 "The passage of 200 years does not change our stand on
6 confidentiality. These records are not available to the
7 government of England."

8 My talks with banks in Boston indicate that they
9 felt that this was banking practice. If it has been changed by a
10 recent court decision, I think it is, again, a problem created
11 by the present system, that bank records should have the kinds
12 of protections suggested by the last speaker. But that is not
13 a situation created by EFTS. It exists under the present
14 system.

15

16

17

18

19

20

21

22

23

24

25

1 Well, having outlined what I think should be done
2 or needs to be done, the question is: who should regulate?
3 And I would suggest that bank regulatory agencies who are
4 normally thought of as the appropriate agencies are not
5 necessarily so; that EFTS presents broad consumer issues, not
6 simple bank regulatory matters.

7 It appears natural at first to turn to the bank
8 regulators, first, because you always think of EFTS in terms of
9 financial institutions, and secondly, because bank regulatory
10 agencies already exist. They have already started talking
11 about EFTS and, therefore, they come forward to everyone's mind
12 where the same kind of structure does not already exist for re-
13 tailers. Otherwise, we might have thought of some retail agency.

14 The problem with bank regulation and its whole
15 regulatory approach is that it has a whole mental set that
16 would control entry into the EFTS field. It would control the
17 services that could be offered. It would control the location
18 from which those services could be offered, with most of these
19 aspects spelled out in statute, because it would just be fitting
20 EFTS into the whole present structure of bank regulation.

21 The assumptions behind this are that EFTS has some
22 implications for the safety of depositors' funds, and that it
23 also will negatively impact on the competitive structure,
24 namely, that it will hurt smaller banks by ruinous competition.
25

1 I don't
2 think either of those two assumptions are correct; and that,
3 furthermore, if we proceed largely from statute on what EFTS
4 can do in each case, there has got to be a very inflexible system
5 that we create; and that, furthermore, we will be substituting
6 regulatory judgment for the judgments of the marketplace on
7 competitive matters. And I suggest that we look at the history
8 of banking regulations to see that, in general, banking regula-
9 tion has come down on the side of less competition rather than
10 more competition, and that in some sense we have become captives
11 of the industry we regulate, or segments of that industry, and
12 that the consumer's interest gets lost in the advantages of
13 competition, or that the cries of competition will hurt more
14 than it will help the consumer usually wins.

15 There are, of course, other agencies, other federal
16 agencies that might regulate. The Federal Communications
17 Commission seems like another likely possibility. They will
18 have, it appears, regulatory jurisdiction over the system
19 linking automated clearing houses, and their opinions or
20 policies on possible interconnections of local telephone
21 circuits are also important to the development of EFTS. So
22 that even if we don't explicitly go into an area of assigning
23 EFTS to other regulatory agencies, there will be regulation.
24 Bank regulatory agencies will continue to oversee whatever the
25 banks do. The FCC will continue to have some jurisdiction

1 over these other areas having to do with telecommunications
2 lines.

3 It seems me the best thing that I can recommend to
4 the Commission to recommend to the Congress would be to say that
5 this is really a broad consumer issue, not simply a banking
6 issue. It will be turned into a banking issue if it is turned
7 over to the bank regulatory agencies, and that instead it
8 should be turned over to a monitoring consumer protection
9 agency or commission, similar to this one, which would not be a
10 regulatory body but which would be an investigative body; that
11 you have a staff that would continue to look into problems as
12 they arose, and that you would then have the right to hold
13 hearings to look further into any abuses that actually occurred
14 as opposed to those that were dreamed to occur or imagined to
15 occur, including questions of competition.

16 I am proposing that EFTS will not have a major
17 negative impact on small banks. Small banks say it will. I
18 think we have plenty of time to see if there is that kind of
19 negative impact occurring and for you then to report back
20 whether there needs to be any constraints on competition.

21 There is yet no clear regulatory need in this area,
22 and it seems to me, the most appropriate thing is to have an
23 oversight commission with a longer time mandate than this
24 Commission, one of five or ten years. Because EFTS will
25 develop differently in the medium term than it will in the

1 long term, someone would need to report back to the Congress on what
2 problems have arisen and what legislative needs have been
3 created. This, it seems to me, would be better than starting
4 out in the beginning with an extensive set of regulations. We
5 would allow for maximum flexibility in the field and thus, from
6 my point of view, it would allow for free entry into the field,
7 which I believe would maximize competition and thus best promote
8 the public interest.

9
10
11 CHAIRMAN ATWATER: Thank you very much.

12 Mr. Green.

13 MR. GREEN: Ms. Greenwald, I would like to pursue
14 your comments about the maximization of competition,
15 especially as it relates to sharing, and your comments
16 about all banking institutions sharing at some point the EFT
17 system.

18 I am just wondering if you in your own mind are
19 considering that this sharing would be done by all depository
20 institutions or if you feel there should be different systems
21 and different sharing mechanisms for different type depository
22 institutions.

23 MS. GREENWALD: Well, I think one has to distinguish
24 between the hardware and the software.

25 The switching facilities are going to be

1 shared, and the clearing house facilities have to be shared.

2 Access should be open
3 not only to non-bank depository institutions but also to
4 non-depository institutions, such as finance companies, which
5 in some parts of the country -- except the Northeast--
6 are very important lenders. American Express, which has just
7 opened a very interesting terminal in Logan Airport, would
8 also have to be offered non-discriminatory access to
9 clearing and switching facilities. It is not just non-bank
10 depository institutions, but it seems to me a whole range of
11 people have to be offered non-discriminatory access into the
12 major hardware, the clearing houses, the telecommunications
13 lines, the switching facilities.

14 Then you get to the software, which is what kind of
15 services are going to be offered out of this machine. And here
16 in the short run, I think, you have to allow different
17 competing institutions to try to develop the best software
18 package they can. And that means in the short run that there
19 will probably be more than one mechanical device, at a depart-
20 ment store or at a supermarket, because the developing insti-
21 tution may say, "Well, anybody can join my software package
22 system, but I'm not going to at this point put a different
23 software package on my machine."

24 And I think in the beginning that is good, because
25 there will be competition in creating that software package.

1 As a number of players enter this game, it is going to become
2 impossible to have enough machines, and then the retailers will
3 insist -- in my view, in the long term, the retailers will
4 insist that those terminals have the capability of handling
5 several software packages. That is not a technological develop-
6 ment that does not exist today. We could do it today. So it
7 is not something inconceivable to have happen.

8 MR. GREEN: So I assume that you are saying that at the
9 point of sale at the corner grocery store there is
10 probably one machine that banks, S&Ls, credit
11 unions and their depositors would have rights to
12 access. Is that right?

13 MS. GREENWALD: Right.

14 CHAIRMAN ATWATER: Are there other questions by the
15 Commission?

16 Mr. Mitchell?

17 MR. MITCHELL: I think we should be glad that you
18 brought our attention back. The protection of consumers does
19 involve increasingly the range of their competitive alternatives,
20 and I don't find very much in your statement that I disagree
21 with. But I find it a little weak in showing just exactly how
22 EFT leads to a more competitive environment. I think you
23 hope it will, I hope it will, and perhaps all of us do,
24 with a few exceptions. But just exactly how this takes place
25 is not entirely clear to me. Since you are Commissioner of

1 Banking in Massachusetts, would you project the way in which
2 competitive alternatives would be enriched by EFT in Massachusetts?

3 MS. GREENWALD: Well, in one way, we have what I
4 consider a very restrictive branching law in Massachusetts. It
5 reads something like: if you are a commercial bank, you can
6 branch within your home office county; and if you are a thrift
7 institution, you can branch 15 miles from your home office
8 which, if it takes you over a county line, is all right.

9 Now, the City of Boston is a very small geographic
10 area. I guess it's about four or five miles. The commuting
11 patterns are much larger than the county boundary. EFTS
12 terminals, if they are not restricted to where branches are
13 placed, would allow suburban bank customers who work in the
14 City of Boston to have access to their funds both in the
15 suburbs and at work without maintaining two accounts. That
16 would be one way.

17 And I truly believe that the monopoly situations,
18 if they exist at all in Massachusetts, exist in very small,
19 local markets, and that monopoly does not really refer to the
20 large banks; the monopoly refers to the size of the market
21 in which you happen to be the major or maybe only banking
22 alternative. That would be one way.

23 We are hoping that EFTS will offer you a service
24 package of convenience that exceeds that which you now have.
25 Certainly, I find it very convenient

1 to be the Commissioner of Banks and be able to cash my check in
2 any bank in the state. It would be very nice for other people
3 to have the same privileges that I do.

4 (Laughter.)

5 CHAIRMAN ATWATER: I wonder if I might ask a
6 question on your observation about non-discriminatory access.

7 You are referring, I presume, to the access
8 of institutions to an EFT terminal.

9 I would like you to fill that out, if you
10 would.

11 MS. GREENWALD: Well, I tried to make a distinction,
12 between mandatory sharing, which I have been opposing in
13 Massachusetts, to the other concept of non-discriminatory
14 access. I have no opposition to one bank putting up a system
15 for itself, if it thinks it can do so. I guess Sears is doing
16 that. They are putting up a system simply for the Sears card.

17 But if Sears or any bank is to let one other bank in
18 into their system, then, following antitrust tradition, it
19 seems to me, every other applicant has to be accorded equal
20 access on the same grounds.

21 Now, this ran into some conflict in Massachusetts,
22 and I don't know where the Commission would want to come down
23 on it. The banks in Massachusetts were perfectly happy with
24 that concept as long as I was talking about depository
25 institutions. But they weren't so anxious to have

1 non-discriminatory access to finance companies, or to American
2 Express -- or to the Allied stores or some other chain. I
3 believe non-discriminatory access means non-discriminatory
4 access.

5 CHAIRMAN ATWATER: Thank you very much.

6 Are there other questions by the Commission?

7 (No response.)

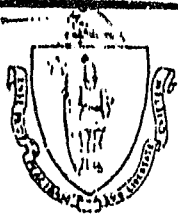
8 CHAIRMAN ATWATER: I thank you very much for your
9 provocative testimony.

10 MS. GREENWALD: Thank you.

National Commission on Electronic Fund Transfers
Users Committee Public Hearings
"Consumers Issues in EFT"
October 26 and 27, 1976
Washington, D.C.

The documents which follow are submitted for the record
of this hearing by:

Carol Greenwald, Commissioner of Banks,
State of Massachusetts



The Commonwealth of Massachusetts

Office of the Commissioner of Banks

State Office Building, Government Center

100 Cambridge Street, Boston 02202

107b

MICHAEL S. DUKAKIS
Governor

October 15, 1976

CAROL S. GREENWALD
Commissioner

Ms. Katharine Humes
National Commission of EFTS
1000 Connecticut Avenue, N. W.
Washington, D. C. 20036

Dear Ms. Humes:

You will find enclosed a copy of a talk I presented on EFTS before the Savings Banks Association of Massachusetts at their Annual Convention in Bermuda in September.

I am also sending a copy to Mr. Richard Sprague as you suggested so that you may decide at which session you may prefer to hear my testimony on competition in EFTS.

I do anticipate that it will be heard on October 29, 1976. If there is any change, kindly advise.

I look forward to seeing you in Washington at that time.

Sincerely,

Carol S. Greenwald
Commissioner of Banks

CSG:esr
Enc.

Public policy's main concern with EFTS should be to ensure that this new method of delivering financial services develops in a manner that best meets the public's needs, that it maximizes consumer convenience and minimizes consumer protection problems. Usually we have a prior assumption that the free market and competition will lead to services most attuned to achieving consumer satisfaction. Only when it is apparent from actual experience that unregulated development will cause serious problems does the government intervene with regulations. This approach to EFTS has not been taken because EFTS has been seen as a banking development, and we are so used to regulating all aspects of banking and defining in statutes what banks may or may not do that there seems to have been an immediate assumption that EFTS development must be directed by statute. Moreover, there has been the assumption that EFTS must be fitted into the structure of present banking regulation, without first determining whether this will result in an EFTS system that will best serve the public.

Public policy's goals are ^{maximum} consumer convenience and minimum consumer protection problems. Concerns about consumer convenience have centered on three areas: branching or location, sharing and types of services available. Consumer protection problems have been raised about possible invasion of privacy and the opportunities for fraud and theft.

Consumer Convenience

Location (Branching)

Geographic restraints on EFTS will not enhance performance of an EFT system. They will simply prevent added competition in some markets which might benefit from new services and/or lower prices. Too much concern has been expressed regarding the impact of EFTS on small banks and on the question of the applicability of the McFadden Act, with much less focus on what will provide the best services to the public. Smaller banks' fears that the costs of keeping pace will be such that only very large institutions will be able to afford to offer EFT services to their customers and have led to demands

that there be mandatory sharing of EFT systems.

EFT does not seem likely to be a major factor in geographic market extension beyond commuting areas. Although where commuting patterns cross branching boundaries, EFT facilities can be a major factor in geographic expansion. Terminals and unmanned facilities can be a major convenience for existing customers and might well cause customers to shift allegiance within a market area from a bank without EFT services to one offering such services. It is questionable whether a bank customer would shift to a bank located in another market area offering only terminals in the customer's area.

But if technological change has negative impacts on some institutions and beneficial effects on others due to consumers preferences for the new service, it is not government's role to prevent the switching. Public policy's concern is to foster consumer convenience and choice. The more scope for management to locate facilities wherever they feel demand justifies, the greater the locational convenience for the public. This would suggest minimizing regulatory restraints. The cost factors associated with facilities such as ATMs should foster greater convenience in the absence of geographic restraints, as machines are cheaper than full branches, and can thus bring services to areas that could not justify a full branch installation.

The argument over whether terminals are branches is first an argument among financial institutions which is geared to their insecurities and desires for protection from competition and second, an argument among regulators seeking extensions of their regulatory range. It is not an argument about how the public can best be served. The recommendation recently of a sub-committee of the NCEFTS that terminals not be treated as branches recognizes this and places priorities in the right order. Government's constituency is the public, not existing banks or regulatory agencies.

Massachusetts law does not classify terminals as branches, but it does restrict them to the bank's home county and does limit the number. Furthermore,

Massachusetts law is silent about manned facilities. The bills submitted last year by the Banking Department and the trade associations would have removed the restrictions and extended the scope of the law. We believe the statute must cover manned as well as unmanned facilities, without regard to number or location, in order to facilitate EFTS development.

But what about small banks' fears that they will be driven out of the market by free market determinations of terminal locations. Is their answer, mandatory sharing, the appropriate or necessary response?

Sharing

Let's be very clear at the beginning about what can be shared. There's first the hardware or terminals, communication lines and clearing facilities, second, the software or programs and services that will be offered. The first obviously must be shared; there is no good economic reason for requiring sharing of the second. In fact, it would seem desirable to promote as many rival software packages at the regional level as possible. Mandatory sharing at this level would obviously work against this desirable result.

Small banks argue that high costs and sophisticated technology will enable only the largest banks to develop an EFT network and that this would give them significant competitive advantages over other banks, especially smaller banks. If banks conclude that it is necessary to their survival to offer EFT services, are the costs likely to be a prohibitive factor for smaller banks? It does not appear that the costs of EFTS are a serious impediment to small bank survival. While there is no doubt that the cost of installing bank-owned terminals in all retail outlets in a bank's market area could be immense, it is absurd to believe that the system will evolve in this fashion with each bank installing its own POS terminals as well as free standing ATMs or CBCTs. The retailer would not put up with such an arrangement. Retailers will insist that one POS system service all the banks. No retailer is going to set up separate registers for individual bank systems. Thus, in the sense

that the terminal in a POS system will accommodate more than one bank card, it will be shared facility. While the smaller bank may well face new competitors through a POS system, the smaller bank need participate only in those retail outlets in the market area it serves. It does not seem likely that pro rata costs of a POS terminal or mini-computer link along with leased telephone lines needs to be prohibitive.

Furthermore, since the retailer wants any such system to continue accommodating his own credit customers as well as those using a variety of non-retailer credit cards and since he will want to see a POS system that also satisfied his internal data needs, it seems likely that the individual retailer will share a portion of the eventual cost with the banks.

Banks need not have individual bank processing capability. There are various alternatives including non-bank processors and processing by correspondents. Most banks have already developed some such capability or arranged for its availability for various internal purposes and there is no reason to believe its extension to new services should be prohibitively expensive.

ATMs will also not present prohibitive costs for small banks. After all, these facilities are in part alternatives to branches and far less expensive than a branch to install and operate.

The final aspect of a system's cost deserving comment is the interbank clearing, switching and processing. While this must be a shared operation, there is no need for the Federal Reserve System to bear the cost and, in fact, for the Fed to do so would be undesirable; costs could be shared through automated clearing house associations, major national credit (debit) card issuers and their members, or communications companies which establish the switch. The costs to the individual bank, if allocated prorata on the basis of volume or some other system will not be unduly burdensome on smaller banks which may still operate through a correspondent.

Access to and sharing a switch would seem essential and antitrust laws should ensure open access. Sharing of programming or software does not seem essential, would be antithetical to the public interest, and, again, antitrust should ensure that local or regional monopoly consortia are not formed.

The problem with a sharing arrangement which provides a local or regional monopoly is that it is very likely to inhibit innovation. Those members with relatively small volume will have little interest in offering services which their scale makes uneconomic, unless the service can be offered at subsidized rates, and they will not wish to pay for research and development costs for such services or for the systems' adaptation to offer such services. Larger institutions will be unwilling to foot the full bill in absence of temporary oligopoly or monopoly profits. The result may be a tendency toward a service package that represents the broadest possible common denominator of what the bank owners wish to offer the public.

Closely related is the administrative difficulty of providing decisive leadership in an organization controlled by numerous independent institutions with diverse goals and interests.

Finally, if monopoly sharing raises concerns regarding pricing with the result that public utility type price regulation is imposed, this may further inhibit incentives to innovate. At this point in EFT development, mandatory sharing of software or programming appears to be not in the public interest.

Another major dimension of the competitive issue in sharing is the question of who should have access to an EFTS and on what basis. While separate and competing switching and processing systems may develop, both non-bank depository institutions and non-depository institutions, like finance companies and large retailers, will be participants in EFTS, helping to assure a competitive environment. They, too, would have to be accorded non-discriminatory access to switching and processing facilities.

Granting retailer credit or consumer loans has been traditionally carried on by non-depository institutions with no thought that they must be subject to bank regulation (as distinct from legislation to protect consumers from interest charge abuses such as usury laws and truth-in-lending.) However, an EFTS would make feasible the use of a debit and cash card against "credit balances" as well as against deposits.

Under these circumstances some would argue (including, certainly, the regulated depository institutions) that non-depository institutions were engaged in banking.

But if banking statutes were determined to cover retailers, the implications for structure could be dramatic. How, after all, can you restrict a commercial bank to a single county or state, if Sears Roebuck, operating nationwide, is a bank?

Types of Financial Services

A third concern in the area of consumer convenience is that EFTS may force the public to forego some of the financial services it already has and desires. The consumer and retailer do not want a system that will reduce sales. Any new system should not reduce the availability of credit either by requiring instantaneous debiting (eliminating float and/or deferred payment) or by accommodating only a plastic card issued by the banks.

The consumer's desire for a system which will not preclude delayed payment, can be accommodated by machine readable credit cards using electronic impulses. The conversion to a debit card to replace the check, however, raises potential problems by eliminating the ability of the customer to employ float. This problem can also be solved, either by the bank offering a delayed debit option, or by use of the credit card with automatic delayed debiting without charge.

On the retailers' desire that the system accommodate cards other than the bank card, there seems to be greater possible friction. Banks seems to desire a universal debit-credit card which will reduce float and give them interest earnings on consumer credit. They perceive the retailers' own credit cards in terms of competition with the bank in granting credit. Most retailers, however, are not interested in the credit as it relates to interest earnings but as it relates to sales and inventory turnover. This is a case of the parts adding up to more than the whole, with retailers aware that consumers will carry a larger volume of credit in multiple accounts than if all are combined in one account.

Pressures brought by retailers in pursuit of their own interests seem sufficient at this time to ensure that the consumer's interest will not be ignored. Competition between competing systems for customers in a regional area would appear to be sufficient to ensure that those options desired by the public will be available.

Consumer Protection

Consumer protection relates to both the potential for large scale fraud and theft and the unauthorized use of an individual's access to funds through an EFTS.

The problems of electronic theft has been pushed to unrealistic limits in many discussions of EFTS. While the transfers can be swift and impersonal, access to enable unauthorized transfers electronically is in the hands of a limited number of people. Furthermore, various codes and requirements for electronic or telephonic confirmation of transfers above specified amounts can significantly limit if not eliminate exposure. Insistence on such controls should be part of any regulatory examination of EFTS facilities. Certainly for banks this could easily enough be fitted into present EDP examinations of banks and their servicers. For non-depository institutions participating in EFTS, examinations by bank regulatory agencies could also be required, just

107j

as now the Massachusetts Banking Department regularly checks finance companies and other credit lenders, including retailers, for compliance with truth-in-lending and usury statutes.

As to unauthorized use of an individual's account through a lost debit card or counterfeit debit cards, this problem does not really seem more severe than the present problem with credit cards.

Questions of invasion of privacy have also been raised by EFTS. In an EFTS, account information of a fairly broad character can be accessed remotely. If this is accessible only via a plastic card or numerical code known only to the individual, not even his bank need know it after the card is issued, privacy would not seem to be compromised. Under such an arrangement a merchant desiring data could request it electronically, but only with the customer's card or only if the customer punched in the appropriate code. If the retailer is concerned about ability to pay and therefore desirous of extensive data (as in large transactions such as purchases of automobiles or real estate), he can request the data with the customer's consent as he does now without electronic aids.

Another aspect of privacy of concern to regulators relates to collection and storage of data and access to it. An EFTS will make it possible to far more easily collect and store data about any individual's or company's behavior, vis-a-vis financial transactions than ever before. It is a matter of legitimate concern to consider what sort of such analysis should be permitted and under what circumstances, to whom does the data belong, and who should have access to it. These would seem to be appropriate matters for federal legislative concern so that national standards are set. Then the appropriate regulatory agencies could examine systems to check that the standards and necessary safeguards are being maintained.

1

Regulatory Alternatives

Having outlined the areas for government concern in EFTS development, the question remains: who shall regulate and how shall it be done. Is it clear that bank regulatory agencies should be responsible for EFTS regulation? EFT presents broad consumer issues, not merely bank regulatory matters.

The notion that EFTS regulation should be in the hands of bank regulators appears natural at first because the individual is conscious of EFTS primarily in terms of its impact on him vis-a-vis his financial institution. The assumption that bank regulators should direct EFTS development also derives from the fact that there is an existing bank regulatory framework and group of regulators concerned with the impact of EFTS on the institutions they embrace, a situation that does not apply, for example, to retailers. Third, much if not most of the traffic handled by an EFTS, even one encompassing a retailer's internal needs, will be financial and involve a financial institution. Fourth, bank regulators already have established certain routes of access to relevant data without the necessity of legal procedures to obtain it, as might for example, be true if data had to be obtained through the state's attorney general. Thus, based on the nature of the service involved and the institutions affected, financial institution regulatory agencies seem logical candidates for jurisdiction over EFTS.

Banking regulation, however, involves a regulatory approach which would control entry into the EFTS field (that is, who could offer services through an EFTS), the services that could be offered, and the location from which services could be offered, with most aspects spelled out in statute. Whoever is involved in the EFT system would be subject to these restraints.

This approach assumes that an EFTS could have significant adverse implications both for the safety of depositors' funds and for the competitive structure of the market for financial services if left unregulated. In particular, it assumes that with the implementation of an EFTS, smaller commercial banks need

an extensive framework to protect them from ruinous competition. As already indicated, neither of these prospects is highly likely. In addition, with such regulation proceeding largely from statute as to the services that might be offered, an EFTS might not be developed with sufficient flexibility to meet ever-changing public needs and demands. A further problem with this approach to regulation is that it substitutes regulatory judgment for the marketplace on competitive matters and may tend to lessen competition. The history of banking regulation is clear evidence of such problems.

I have argued earlier that it seems desirable not to treat EFT facilities as branches. Banking by mail or by telephone or by credit card at locations away from actual bank facilities are popular practices that are flourishing today, and EFT systems would simply extend consumer convenience by permitting electronic analogs to such transactions. From this perspective, it seems appropriate to characterize EFT systems as communications facilities primarily, and banking facilities only incidentally. This view explains the recent interest in EFT on the part of the White House Office of Telecommunications Policy, indicates the potential role of the FCC, and gives further reason for modesty with regard to the role of bank regulatory authorities. The FCC would apparently have regulatory jurisdiction over a system linking automated clearing houses, and its policies on permissible interconnections with local telephone circuits are obviously important. Major responsibility for EFT regulation may well go to the state public utility commission and the FCC especially if regional or statewide monopoly consortia emerge.

If EFTS is viewed as essentially a communication system and/or evolves so as to have monopoly characteristics, strong claim can be made that its regulation properly belongs with a state's public utility commission. Such commissions already deal with a variety of industries, their regulation affects

services purchased by individuals and various industries, and they are accustomed to dealing with interstate sale of services. Jurisdiction by the state utility commission and/or the FCC (which can claim precedence over state agencies in case of conflict) implies determination by specialists in communications regulation with regard to reasonable rates and terms, adequate service and fair access. Such jurisdiction would in no way preclude such bank regulatory agencies from exercising control over bank soundness or permissible powers.

I think that the attractiveness of mandatory sharing of EFTS would diminish considerably if it were understood that this would very likely lead to public utility regulation, to establish minimum standards of performance, guaranteed access to all and appropriate or reasonable prices in the absence of competitive forces.

Jurisdiction could also be placed in the hands of a consumer protection agency. These agencies are not regulatory bodies but rather serve as watchdogs or monitors of the public interest. They have investigative powers with ability to seek judicial (or legislative) action, but little if any power to adjudicate or regulate on their own and lack the ready access to records, etc., that bank regulators have. This may, of course, be the best reason for giving jurisdiction to such agencies on the grounds that there is as yet no clear picture of regulatory need. This would leave EFTS regulation in a status similar to that of most merchandise retailers who are not subject to specific industry regulation but who do have to comply with consumer protection regulations such as truth-in-lending or fair credit billing.

This approach would not seek to set out in advance an extensive set of restrictions or controls on EFTS but, rather, would establish a system for monitoring the EFTS and identifying areas where consumers were abused, with any specific statutes and regulations flowing from the identification of troublesome abuses. This approach provides maximum flexibility in a field which, from a regulatory point of view as well as technologically, is new and, therefore,

not fully understood in terms of needed regulation. It can also readily cut across industry lines and fits as well into a framework for regulating commercial banks as it does for retailers or others. It lessens the risk of regulation becoming a captive of the industry or the industries it regulates, but rather readily keeps in mind that its regulatory objective is the public interest. Finally, it maximizes competition by allowing completely free entry.

On the national level, a body like the NCEFTS could be established or this Commission's life could be extended for a five or possibly ten year period to monitor EFTS developments. Like the present Commission, it would hold hearings on areas of concern and potential problems and could recommend legislation or the need for further regulation if actual problems or abuses arose. The Commission would set no restraints on who could enter the field or the location of retail outlets, but would closely monitor competition and performance, especially price.

This approach would rely on the market to resolve any new public policy issues not embraced by the existing regulatory framework, but under close monitoring of developments. I am not proposing the absence of all regulation. What I am suggesting is that two levels of regulation already exist and will continue to operate in this field. Banks are already regulated and their bank regulators will continue to regulate what services they can offer and to monitor their effect on banking. The FCC and state public utility commissions will have regulatory jurisdiction over certain uses of communication lines.

What I am suggesting is that the location, ownership, and services available through an EFT facility should be left entirely to the marketplace to determine, with monitoring of developments by a national consumer-oriented commission. This approach assumes that an EFTS is basically a technological development which facilitates the offering and utilization of financial services through machines or terminals. It assumes that the impact of EFTS will be predominantly pro-competitive and that enforcement of the anti-trust laws

by the Justice Department will ensure that monopolistic arrangements will not be tolerated.

It need not be assumed that EFTS must be regulated because it relates to banking. This is especially true if the system, left unregulated, would develop along competitive lines with readily available alternatives for access, non-discriminatory pricing, and a wide variety of service options available to institutions, and, through them, to EFTS customers. It would seem more likely that this will result if the market determines the development than if bank regulatory agencies do.

What I am proposing is that the NCEFTS should not feel obliged by the end of its 2-year mandate to produce a legislative package to direct by statute the development of EFTS. In fact, it would be inappropriate for it to do so. Since EFTS does not now exist, the Commission would be legislating in the dark about potential rather than actual problems. This is an unusual procedure. Legislatures usually act only after a problem has actually occurred; they react to the real not the imagined. It would be far preferable for the Commission to hold hearings about areas of concern, examine these potential problems and then with a longer time mandate, monitor developments to see if any of these anti-consumer concerns materialize. If they do, then it would be appropriate for the Commission to suggest legislation to protect the public interest.

Massachusetts, of course, need not rely on a national consumer commission on EFTS to monitor developments. It can and should have its own public agency with consumer representation to watch developments here and to recommend needed legislation in case problems arise.

11 CHAIRMAN WIDNALL: As we close this morning's
12 meeting, we will adjourn until 1:30 this afternoon for lunch.

13 I thank all of you for being here and acting as witnesses
14 and any others who have been here listening very quietly to the
15 testimony.

16 (Whereupon, at 12:05 p.m., the hearings adjourned
17 for lunch.)
18
19
20
21
22
23
24
25

1 .AFTERNOON SESSION

2 1:40 p.m.

3 CHAIRMAN WIDNALL: This afternoon we're going to
4 hear from a number of witnesses, including a panel.

5 The first witness scheduled is a man who I
6 hope will forgive me if I mispronounce his name, Anthony
7 Derezinski.

8 Is that close?

9 MR. DEREZINSKI: Perfect.

10 CHAIRMAN WIDNALL: He's a state senator from
11 Michigan, and chairman of the committee that introduced
12 EFT legislation in that state.

13 Now, I would like to turn over any further
14 introduction to the chairman of our subcommittee, Vern Atwater.

15

16

17

18

19

20

21

22

23

24

25

1 (Witness sworn.)

2 TESTIMONY OF ANTHONY DEREZINSKI, SENATOR, STATE
3 OF MICHIGAN; CHAIRMAN, SENATE CORPORATION AND
4 ECONOMIC DEVELOPMENT COMMITTEE.

5 CHAIRMAN ATWATER: Please proceed, Mr. Derezinski.

6 MR. DEREZINSKI: Thank you, Mr. Atwater.

7 Mr. Chairman and members of the Commission, my
8 name is Tony Derezinski, and I'm chairman of the Michigan
9 State Senate Committee on Corporations and Economic
10 Development.

11 The issue of EFTS presented itself to the
12 Michigan legislature about the same time as I did, which was
13 about two years ago when I was elected to the state senate
14 and subsequently was assigned to the Committee on Corporations
15 and Economic Development.

16 At that time, a bill was about to be introduced
17 and then was introduced shortly after the legislative session
18 started called the Electronic Funds Transfer Facilities
19 Act, which would have addressed a number of issues which
20 you no doubt have been addressing yourselves to over the last
21 month, and particularly in the hearings this morning.

22 This bill went through the Committee structure
23 and was reported to the floor of the Michigan senate.
24 Then because of a rather healthy amount of money which was
25 felt needed in the bill to accomplish the ends desired,

1
2 it was sent to the Appropriations Committee. It
3 has resided there since then, and for all practical purposes
4 the bill will probably die with the end of this legislative
5 session.

6 A summary bill was introduced in the Michigan
7 House of Representatives and has not moved anywhere there.

8 However, in both Houses, I suspect early in the
9 spring legislation will be introduced to address the problem
10 of electronic transfer funds from a state viewpoint.

11 My concern, however, is not only with the various
12 substantive issues that you have addressed so far and that
13 we have addressed on the state level.

14 In addition to that, I come here, you might say,
15 as a born-again Federalist who sees a definite role for
16 state government in these issues. And I'm fearful of a lot of
17 the problems which I have been seeing in my position as a
18 state legislator which crops up in the federal system of
19 government with an ever-increasing role being played by the
20 federal government in areas that traditionally were reserved
21 to states.

22 This is not the first time I've testified in this
23 building. I was here about three months ago testifying on
24 a matter of cable television, where also I saw an intrusion
25 by the federal government in areas which I thought could better

1 be regulated by the states, and have also voiced concern in
2 other ways concerning other intrusions into areas which were
3 heretofore sacred to the state, such as commercial transactions
4 by the passage of regulations of the Federal Trade Commission
5 pertaining to the holder in due course doctrine.

6 So I definitely see in this issue, as well as
7 many others, a role for state government. EFTS presents a
8 tremendous new and varied approach to commercial transactions
9 in the United States.

10 Along with it, though, we have to realize that the
11 technology itself is neutral; and secondly, that with that
12 technology there is also great potential for possible abuse.
13 Computers can facilitate the gathering, the retrieval and
14 storing of information, but any information which is so stored
15 can also be subject to a lot of scrutiny by a lot of
16 individuals, and it also can be used for various purposes.

17 I see first of all a role for state government in
18 the area of privacy. The invasion of consumers' privacy
19 could happen, I believe, in two broad categories: the invasion
20 of consumers' privacy by private parties for commercial
21 purposes, and I would like to commend your attention to an
22 excellent article in the University of Maryland Law Review,
23 Volume 35 of 1975. Many of the technical issues that I
24 will be raising today are well covered in that article.

25 It is an excellent law review summary of the legal

1 aspects of this.

2 The development of the right of privacy has
3 primarily been taken care of by state courts, either in
4 statutes such as a New York statute which was enacted in
5 1903, protecting the right of privacy, or in case law such
6 as the case of Pavesich v. New England Life Insurance Company,
7 which was decided in 1905 in the State of Georgia.

8 There are basically two types of invasion of
9 privacy which are handled in the state courts on state
10 statutes which are involved here. First of all, appropriation,
11 and secondly, intrusion.

12 By analogy and by further extension of logical
13 principles which have been developed by state courts and
14 statutes, you can see that there is a certain property
15 interest in the way a person does his transactions.

16 For instance, if a person's bank account reflects
17 a great number of airline ticket purchases, that information
18 would be very valuable, let's say, to a luggage manufacturer
19 who would like to get that information and possibly solicit
20 that person's business for luggage.

21 This is a way the computers can be used.

22 And I think here if you also extend certain
23 principles logically which have already been enunciated, that
24 is, the commercial property which could be appropriated and
25 for other uses without the consent of the consumer.

1 Also, if that account were viewed as part of the
2 person's domain by a logical extension of certain principles
3 of privacy, I think you could see that that domain is intruded
4 by that gathering of information from his account and
5 subsequent use of it.

6 I think the basic mechanism, the legal principles
7 exist now in statute toward law ought to handle many of
8 the problems that are associated with EFTS. And I think here
9 also, then, the fact that we have the mechanisms and the terms
10 of various principles of law which have already been developed,
11 the states would have a definite role here.

12 And I would recommend that this area be handled
13 by state legislation to the greatest extent possible.

14 Another area of concern that I see regarding privacy
15 would be an invasion by governmental agencies. Again, this
16 probably has been gone over in great extent, but I think here
17 the role of the federal government is even as dramatic as the
18 role of state governments in terms of having some control
19 over our own possibilities by government in the area of
20 privacy from governmental intrusion.

21 However, I think the main reason and the main role
22 that I see for state governments in this area pertains to the
23 rights, duties and responsibilities of consumers in
24 transactions.

25 The issues raised in this section are particularly

1 significant, not only in terms of whether EFTS will provide
2 substantial benefits for consumers over the present paper
3 system, but also in terms of consumer acceptance, a matter of
4 concern to financial institutions.

5 I would like to touch briefly on some of these
6 areas and then talk about how to approach them.

7 Despite the myriad and obvious advantages EFTS
8 offers current financial institutions, consumers stand to
9 lose a great deal.

10 I'm only going to touch on just two as examples:
11 the ability to stop payment on checks and the loss of
12 float.

13 In terms of consumer protection, the stop payment
14 problem looms larger. Without this option, consumers are
15 essentially without a remedy short of extensive and expensive
16 litigation against merchants, landlords and others with whom
17 they do business.

18 Loss of this right would fundamentally transform
19 the economic bargaining power of consumers. It is essential
20 that any legislation regulating EFTS preserve this safeguard
21 for consumers.

22 One solution would be to require a depositor's
23 bank to recredit a previous debit entry, within a specified
24 time period, upon notification by the depositor.

25 The loss of float deprives consumers, to a

1 significant extent, of the ability to control their own
2 finances. This is not only a loss of personal control, but
3 also a loss of certain economic value.

4 I won't dwell on the moral aspects of the float,
5 because like it or not, however, it is part of our banking
6 system.

7 The problem could be solved by the bank offering
8 a delayed debit option or by use of the credit card with
9 automatic delayed debiting without charge. Neither of these
10 solutions is likely to appeal to business and financial
11 institutions.

12 However, for consumers to accept the loss of float,
13 other equivalent benefits should accrue to them.

14 The current system also offers consumers an easy
15 record-keeping mechanism, both for their own financial
16 planning and for other proceedings, such as lawsuits, disputes
17 with the IRS and the like.

18 In order to retain this advantage of record-keeping
19 that certain check policies now provide, any EFTS system
20 should be mandated to provide some substitute for the
21 cancelled check which will be universally recognized as proof
22 of payment and to provide the consumers with a periodic
23 statement of account, so that unauthorized debits can be
24 discovered.

25 Needless to say, such statements should be in a form

1 legible to the human eye and understandable to the noncomputer
2 expert.

3 I'm sure we have all experienced the frustration
4 of trying to decipher a computer printout masquerading as an
5 intelligible statement. None of us would willingly accept
6 this in lieu of cancelled checks.

7 I can only add a little personal experience I've
8 had from the view of someone who used to do probate law.

9 Many banks are now using a computer printout in
10 terms of managing accounts. This may be very well and good,
11 but it isn't much more difficult than the old way of preparing
12 statements of accounts that we used to experience.

13 If you look at the present system, you will find
14 that the Uniform Commercial Code addresses many of these
15 issues. For example, stop payment orders are covered in
16 Section 4-403 of the code. Contractual burdens, other
17 allocation of risk, and other mechanics of contractual
18 arrangements are all handled by the UCC.

19 This Code is a matter of state law. Standard
20 contractual relationships have traditionally been handled by
21 the states. Thus, I believe it appropriate for the issues
22 raised in this section, issues which essentially deal with
23 contractual relationships, should be dealt with at the state
24 level.

25 Obviously, uniformity is as desirable here as it is

1 in other areas of commercial law. The National Conference of
2 Commissioners on Uniform Laws is the appropriate body to work
3 out the details of the necessary legislation.

4 The existing Code would have to be stretched
5 considerably in order to accommodate the problems raised by
6 this new technology. Articles 3 and 4 deal with the fact
7 that people desiring to make payments, or promises to pay,
8 are looking at, writing upon, losing, stealing, signing,
9 forging, carrying about, revising, failing to complete, and
10 doing business in strange places with, and otherwise handling
11 paper, paper documents.

12 The underlying assumption of many of the provisions
13 of Articles 3 and 4 of the UCC is that the paper document
14 is readable by humans without the aid of machines. To bring
15 the magnetic tape of EFT systems under the Code's definition
16 of a "writing," which is contained in Section 1-201(46), which
17 is the definitional section, not only requires the skill of
18 a contortionist, but runs directly counter to the philosophy
19 of the Code which was "to avoid making practical issues
20 between practical men turn upon the location of an intangible
21 something...and to substitute for such abstractions proof of
22 words and actions of a tangible character."

23 This was out of the Comment, Section 2-101.

24 An excellent article, again dealing with these
25 problems, is the one I previously mentioned in Volume 35 of the

1 Maryland Law Review.

2 Rather than try to patch Articles 3 and 4 of the
3 current Code, we should recommend to the National Conference
4 of Commissioners on Uniform State Laws the creation of
5 another Article which can deal clearly and exclusively with
6 the new technology of EFT.

7 Another area which I would like to address myself
8 is that of security.

9 The security of EFT systems for consumers covers
10 a broad range of potential problems: unauthorized disclosure
11 of information, which I've previously mentioned; errors in
12 accounts; theft in the most traditional sense, at terminals
13 themselves; and computer theft, both of individual accounts
14 and the penetration of the entire system.

15 I will not reiterate here my comments on the
16 unauthorized disclosure of information, except to emphasize
17 the importance of the issue.

18 Obviously, errors will occur with the EFTS just as
19 they now occur with traditional paper systems. Anyone who has
20 ever had the experience with computerized billing shudders
21 at the prospect of what may happen with EFT unless safeguards
22 are actually build in.

23 What is critical here is that consumers have
24 adequate means of ascertaining when an error has been made in
25 their accounts and of obtaining redress.

1 As I have mentioned earlier, legislation mandating
2 periodic statements in a legible and understandable form
3 would meet this need. And again here, also, this could be
4 most easily handled through the Uniform Commercial Code.
5 The imposition of penalties for undue delay in correcting
6 errors in consumer accounts would be one way of encouraging
7 financial institutions to act promptly when errors are
8 reported by consumers.

9 Another aspect of security which is rarely touched
10 upon is the security of the consumer who withdraws cash at
11 an automatic teller machine in an "out of the way" location.
12 State criminal law cover the crime involved. The question
13 is how to prevent it from occurring.

14 One possibility is to regulate locations of ATMs,
15 lighting, the hours of operation and other security provisions.
16 In any event, this should be handled at the state level in
17 order to provide for responsiveness to local situations and
18 adequate enforcement.

19 The two areas most often thought of in connection
20 with EFTS and security are unauthorized penetration of the
21 consumer's individual account and large-scale penetration
22 of the entire system.

23 I am not a computer expert and can offer no
24 solutions to the technical problems involved in making the
25 computer systems more secure. However, I can outline some of

1 the problems and suggest ways in which the legal system
2 should respond.

3 Penetration of an individual account is most likely
4 to occur through a lost card or improper customer
5 identification. The cardholder's liability for a lost card
6 should clearly be defined.

7 One approach would be to assess liability against
8 the cardholder only if the card has been requested and applied
9 for, and if the card issuer has given adequate notice of
10 the cardholder's potential liability and provided him with
11 an addressed notification to be used in case of loss.
12 Liability could be limited to \$50 prior to notification of
13 this loss.

14 The problem of wholesale penetration of the system
15 is an enormous one. Computer crime is burgeoning. An article
16 on computer crime noted in the New York Times some time ago,
17 "Hardly any computer thefts were discovered during normal
18 security precautions or accounting controls, and that nearly
19 all of them were uncovered by happenstance. Some experts
20 estimate that the ratio of undiscovered to discovered crimes
21 may be on the order of 100 to 1."

22 Statutory and regulatory law are required both for
23 preventive measures and to assure that criminal law keeps
24 step with technology.

25 One matter to be considered is the point-of-sale

1 devices in retail stores These are on nonbank premises and
2 are operated by nonbank personnel. Will they be covered by
3 federal and/or state banking statutes?

4 This demonstrates the difficulty in approaching
5 the problem in traditional ways. EFT is a unique system
6 requiring us to re-think many of the categories we are
7 accustomed to using. We need to develop legislation that will
8 consider problems and solutions comprehensively. We should
9 not be and cannot be bound by the boxes of the past.

10 There is room here for both federal and state
11 action. Problems of contractual relationships and criminal
12 law should remain the province of the states. Finding a
13 solution to computer fraud which is often interstate in
14 nature, requires a cooperative effort by federal and state
15 legislatures.

16 In spite of the inapplicability of current law,
17 the problem of maintaining competition is one of those which
18 I think is going to be foremost. Here, also, I think we have
19 room for cooperative relationships in the area of competition
20 between the federal and the state government.

21 I think it can only be maintained by legislation.

22 Competition within the state, particularly, should
23 be handled by the state.

24 The McFadden Act, I believe, implicitly recognized
25 this when it left the question of branch banking to the states.

1 The court have been wrestling with the concept
2 of what constitutes a branch for years. The question has
3 arisen over devices ranging from deposit boxes to armored
4 cars to automatic teller machines.

5 I believe the ATMs and point-of-sale terminals
6 differ so greatly from the traditional concept of a branch
7 that our present legal mechanism is totally inadequate to
8 deal with it.

9 The potential for large financial institutions
10 to obtain significant economic advantages is a matter of
11 federal concern because of the interstate aspects.

12 The federal government should take a strong role
13 here in antitrust legislation and enforcement. There is,
14 however, still a role for state government in this area.
15 Local competition may best be analyzed and preserved by state
16 agencies.

17 One possible approach might be that taken in the
18 recently enacted amendments to the antitrust act which
19 provides for enforcement powers for state attorneys general.

20 I have focused on a number of problems presented
21 by EFT. Despite this, I remain firmly convinced that
22 computerized financial transactions are not only inevitable,
23 but hold great promise for consumers in terms of more rapid
24 and more universally accepted transfer of funds as well as
25 increased personal convenience.

1 I, myself, have held a debit card ever since such a system
2 was instituted in my home town, and have been very happy with
3 the service.

4 As with any technology, however, EFT is neutral
5 in itself. It is in the application that the potential for
6 significant benefits and significant injury lies. My purpose
7 in pointing out the problems in the areas of privacy,
8 commercial law and security is not to decry the advent of
9 EFT, but to call for state and federal action that will assure
10 that electronic fund transfer systems work to serve people.

11 As a state legislator, I view myself also as a
12 servant of the people in the narrower framework than the
13 national legislature.

14 However, within that framework, I think the
15 responsibility of state legislators on state government is
16 just as meaningful and can provide in those areas which I
17 have designated a probably more responsive service than can
18 the federal government.

19 And I would like to see the role of state
20 government in this area maintained and perhaps strengthened
21 under any response that this Commission comes up with for the
22 federal government to adopt.

23 Thank you.

24 CHAIRMAN ATWATER: Thank you very much,
25 Mr. Derezinski.

National Commission on Electronic Fund Transfers
Users Committee Public Hearings
"Consumers Issues in EFT"
October 26 and 27, 1976
Washington, D.C.

The documents which follow are submitted for the record
of this hearing by:

Anthony Derezinski of
Michigan State Senate

TESTIMONY ON
ISSUES RELEVANT TO
THE INTERESTS OF CONSUMERS
BEFORE THE
NATIONAL COMMISSION ON
ELECTRONIC FUND TRANSFERS

October 26, 1976

Mr. Chairman and members of the Commission: My name is Anthony Derezinski and I am a state senator from Michigan. I am chairman of the Senate Corporation and Economic Development Committee, which reviews all bills relating to financial institutions.

EFTS emerged as a major issue in the legislature at virtually the same time that I was elected to the Michigan Senate and assigned to the Corporations and Economic Development Committee.

The Electronic Funds Transfer Facilities Act was introduced March 25, 1975, and assigned to my committee. After a number of hearings, which brought out many of the issues you've undoubtedly been hearing about, a substitute bill was reported out to the Senate. That was the end of the trail for EFTS in Michigan--at least for this legislative session. The bill was referred to the Appropriations Committee on July 15, 1975, and no action has been taken since. A similar bill introduced in the House has not been acted upon.

There is another reason, besides my strong interest in EFTS as a substantive area, for my appearance here today. I am gravely concerned about the broader issue of federalism and federal pre-emption of areas which properly belong to the states.

I am aware that certain issues demand a federal approach because of the need for uniformity of standards across the country.

I am also aware that it is the lack of appropriate action by state legislatures which has sometimes created a void into which federal power has flowed.

Electronic fund transfer systems offer many advantages for all elements of society--consumers, businesses, and financial institutions. We must remember, however, that EFTS is only a technology. Like science, it is neutral in and of itself. It is the application of EFTS that has the potential for both beneficial and detrimental impact. I think it's important that we identify possible problems and solutions now so that EFTS can fulfill its promise.

With this as prelude, I would like to comment on several of the substantive issues relevant to the interests of the consumer in the development of electronic fund transfer systems and to delineate those areas where I believe state government could play a more responsive role than the federal government.

I. Privacy

The potential that EFT brings for abuse of consumers' privacy is enormous. The facility with which computers can gather, store, and retrieve information, as compared with traditional paper records, presents a difference of such magnitude as to be one of kind and not of degree. The mis-named Bank Secrecy Act of 1970 assures that data on financial transactions will be preserved and disclosed to government officials. Where information is kept, it will be sought, even though the original reason for keeping the information may be far afield from the reason it is sought.

-3-

Computerization of records can only accelerate this tendency by making the information more easily accessible.

Invasion of consumers' privacy can be divided into two broad categories: (1) Invasion by private parties for commercial purposes, e.g. a merchant buys a list of persons who have purchased a certain number of airline tickets in the last year in order to solicit them for luggage sales. (2) Invasion by government agencies for legitimate (detecting tax evasion) and illegitimate (surveillance of persons belonging to dissident groups) purposes, e.g. the agency obtains a listing of political contributions made by certain individuals. These two kinds of invasion of privacy need to be considered separately.

The first kind of invasion of privacy, i.e. by private parties for commercial purposes, has traditionally been handled at the state level, either through the development of the common law or by statute. New York was the first state to enact a statute which made the use of the name or picture of any person for advertising purposes without written consent a tort (N.Y. Sess. Laws 1903, Chapter 132). Similar acts were adopted in Oklahoma, Utah, and Virginia. Pavesich v. New England Life Insurance Company, 122 Ga. 190 (1905), recognized the existence of the right of privacy in a case where the defendant's insurance advertising made use of the plaintiff's name and picture, as well as a spurious testimonial.

Development of the law of privacy in the tort area has centered around four areas, two of which are applicable in the matter we are considering today: (1) appropriation, in which a

person's name or likeness is appropriated by a commercial concern for its own benefit and (2) intrusion, in which an intrusion is made upon a person's physical solitude or private conversation. Although neither of these two categories are directly applicable, both can be extended by analogy to the problem at hand.

By extracting information about the consumer's buying habits and selling it to an interested third party, a bank (or other financial institution) is appropriating something unique about the consumer and using that unique information for its own pecuniary benefit. Similarly, assuming, arguendo, that a consumer's bank account is an extension of his or her domain, then an intrusion into the account is a tort.

My purpose in bringing these analogies to your attention is not to make a legal argument that this is the way in which the tort of invasion of privacy would necessarily develop, but to demonstrate that there is already a mechanism in existence, tort law, which could handle many of the problems involved in invasion of consumers' privacy by private parties.

Tort law has traditionally been handled at the state level, either through the common law as applied in state courts or by state statute. Therefore, I recommend to the Commission that the provision of remedies to the consumer for invasion of privacy for commercial purposes be left to the states.

The second area of invasion of consumers' privacy, i.e. by government agencies, is potentially of far greater concern, both for individual consumers and for the nation as a whole. Access by the government into detailed information on citizens'

financial transactions presents a horrifying spectre of political control. The Bank Secrecy Act allows government access to every financial transaction made through a financial institution where records of such transactions "have a high degree of usefulness in criminal, tax, or regulatory investigations" (12 USC §1829b(a)(2)). Watergate and the revelations of FBI criminal activity have demonstrated how tortured a reading high government officials can make of statutory authority.

The potential impact of such information is made clear by former Justice Douglas in his dissent in California Bankers v. Schultz, 416 US at 85:

In a sense a person is defined by the checks he writes. By examining them the (government) agents get to know his doctors, lawyers, creditors, political allies, social connections, religious affiliation, educational interests, the papers and magazines he reads, and so on ad infinitum. . . . (T)hese other items will enrich that storehouse and make it possible for a bureaucrat -- by pushing one button -- to get in an instant the names of the 190 million Americans who are subversives or potential and likely candidates.

Justice Douglas' concern is reinforced by the growing volume of literature on invasion of privacy by computer technology. I particularly recommend Arthur Miller's The Assault on Privacy.

It is essential for both state and federal government, especially the federal government because of its more extensive computer records, to address this issue. Government bears a heavy responsibility--indeed, a sacred duty--to protect the privacy of its citizens from its own intrusions.

II. Rights, Duties and Responsibilities of Consumers in Transactions

The issues raised in this section are particularly significant not only in terms of whether EFTS will provide substantial benefits for consumers over the present paper system, but also in terms of consumer acceptance -- a matter of concern to financial institutions. Let me touch briefly on some specific areas, and then talk about how to approach them.

Despite the myriad and obvious advantages EFTS offers financial institutions, consumers stand to lose a great deal. Two current benefits come immediately to mind: the ability to stop payment on checks and the loss of float.

In terms of consumer protection, the stop payment problem looms larger. Without this option, consumers are essentially without a remedy (short of expensive litigation) against merchants, landlords, and others with whom they do business. Loss of this right would fundamentally transform the economic bargaining power of consumers.

It is essential that any legislation regulating EFTS preserve this safeguard for consumers. One solution would be to require a depositor's bank to recredit a previous debit entry, within a specified time period, upon notification by the depositor.

The loss of float deprives consumers, to a significant extent, of the ability to control their own finances. This is a loss not only of personal control, but also of economic value. The problem could be solved by the bank offering a delayed debit option or by use of the credit card with automatic delayed debiting without charge. Neither of these solutions is likely to appeal

to business and financial institutions. However, for consumers to accept the loss of float, other equivalent benefits should accrue to them.

The current system also offers consumers an easy record-keeping mechanism, both for their own financial planning and for other proceedings (lawsuits, disputes with the IRS, etc.). In order to retain this advantage, any EFT system should be mandated to provide some substitute for the cancelled check which will be universally recognized as proof of payment and to provide consumers with a periodic statement of account, so that unauthorized debits can be discovered. Needless to say, such statements should be in a form legible to the human eye and understandable to the non-computer expert. I'm sure we have all experienced the frustration of trying to decipher a computer print-out masquerading as an intelligible statement. None of us would willingly accept this in lieu of cancelled checks.

I've identified some of the areas of concern. How should they be addressed?

If you look at the present system, you will find that the Uniform Commercial Code already addresses many of these issues in the current system. For example, stop payment orders are covered in Section 4-403 of the Code. Contractual burdens, allocation of risk, and other mechanics of contractual arrangements are all handled by the UCC.

The Code is a matter of state law. Standard contractual relationships have traditionally been handled by the states. Thus, I believe it appropriate for the issues raised in this

1 Are there questions?

2 Mr. Wegner?

3 MR. WEGNER: Senator, I don't mean to imply an
4 answer in my question, but I heard some remarks made this
5 morning by Mr. Marson that had to be intended to aid in
6 the preparation of federal legislation to insure the rights
7 of privacy with respect to government intruding into financial
8 records.

9 If I understand your remarks correctly, you are
10 advocating that this protection is a matter best left to the
11 states, and you may be entirely right. But I think it would
12 be helpful to the Commission to get an understanding from
13 you, and in fact from anyone else that is going to testify
14 before us today, as to what criteria we should employ in
15 matters like this.

16 In considering this kind of a question personally,
17 I tend to look at issues which I perceive to be basically
18 lodged in the Constitution, such as human rights and the
19 right to privacy, rights which are more fundamental in
20 character and perhaps best treated by some sort of universal
21 application that would affect uniformly all people. In
22 other areas, where there appears to be no one best or
23 simple answer to
24
25

1 things, a variety of experimentation or a diversity in
2 design and structure of the law may in fact produce within
3 our society answers that we otherwise would have missed
4 if we just had one catchall piece of legislation.

5 How do you view this? What criteria do you apply
6 to this kind of judgment?

7 MR. DEREZINSKI: Well, I think the starting-off
8 point should be existing legal doctrines.

9 Now, you mention the right of privacy in the
10 Constitution, and I suppose some of the legal precedents
11 would be Griswold v. Connecticut and other cases like that.
12 The right of privacy, however, is one that has been
13 fairly well developed by state tort law long before
14 Griswold, which I think was decided in 1959.

15 Cases I previously mentioned were decided around
16 the turn of the century, indicating that a person did have
17 a right of privacy.

18 Now, those cases, either in state statute or
19 common law development, primarily concerned the nongovern-
20 mental aspects of privacy. And I think here is where
21 the states probably can develop legal doctrines as they
22 have been in the past.

23 Now, you also mentioned governmental invasions of
24 privacy which is a real problem. And there, I think, as
25 my testimony indicates, there is definitely a federal role

1 to protect the citizens against itself and, of course, on the
2 state level, too.

3 But I think we have to start off with current
4 legal doctrines, and go from there to where we want to go.

5 Now, this philosophy, I think, also applies in the
6 commercial area, and that is why I stress the development of
7 commercial legislation such as the Uniform Commercial Code
8 which is basically, even in the Constitution, left primarily
9 as a matter of state law unless you stretch the interstate
10 commerce clause to get into that area.

11 But my initial criteria would be existing
12 legal doctrines to see how they apply first. Before you jump
13 into it on the federal level, you should first see where you
14 are coming from.

15 Privacy -- I think the major threat to it is
16 probably federal governmental invasions. And this, I think,
17 is where the federal government obviously has a role, and
18 they are going to have to make some decisions. But where it
19 comes to commercial invasions of privacy, there I think the
20 states could best be left to handle it.

21 MR. WEGNER: That's very helpful.

22 Thank you.

23 CHAIRMAN ATWATER: Mr. Worley?

24 MR. WORLEY: Yes.

25 Senator, in your testimony you point out quite

1 properly that one matter to be considered is the point-of-sale
2 devices in retail stores. You point out that these are
3 on nonbank premises and are operated by nonbank personnel.

4 You raise the question whether they should be
5 covered by federal and state banking statutes.

6 Now there is a school of thought that feels they
7 should not be regulated by either, and I wonder if you would
8 comment further on that.

9 MR. DEREZINSKI: Okay.

10 My remarks there pertain to criminal law, what
11 happens when you have a theft from one of those devices,
12 let's say, located in a Penney's store.

13 If the theft occurs, should federal criminal
14 liability attach at that point?

15 It is not on the premises of a bank. Is it a bank
16 robbery or a robbery of an individual who was stolen from?
17 Is it a robbery of Penney's?

18 In addition to that, was the person operating it
19 an insider, which has all sorts of ramifications in terms of
20 how you proceed under criminal law.

21 I think these are some of the issues which would
22 have to be addressed.

23 I was talking at that point in terms of bank
24 robbery statutes. Again, here, I think the basic approach
25 to robbery problems or theft in general should be state law.

1 Now, you talk about in terms of regulation, let's
2 say, of automated tellers or point-of-sale devices in
3 supermarkets or in other retail establishments. There, too,
4 I think the matter should be one of regulation by the state
5 government because I think you are talking about competition
6 in this situation.

7 I recognize full well that they could be wired
8 up nationally. I just read in the New York Times a while
9 ago how American Express is now allowing the purchase of
10 American Express checks at a number of locations in different
11 states.

12 Well, that is an interstate aspect, too, but the
13 impact it has competitively is on a local level.

14 Take, for instance, branching, the concept of
15 branching as it is now used in the McFadden Act. How does that
16 impact?

17 I think it impacts on the local competitive problem
18 more so than it does nationally. Here the main issue you are
19 talking about is competition, and I think the primary response
20 should be to the local competitive picture, but I also
21 recognize the need for the secondary response which is
22 competition on a nationwide level where there is definitely
23 a role for the federal government.

24 I cannot deny that.

25

1 MR. WORLEY: Just to follow that up, do I understand
2 that you bring into the competitive picture

3 regulation of these point of sale terminals from
4 the standpoint of their deployment, rather than regulation of
5 them once they are in the retail premises from an operating
6 standpoint?

7 MR. DEREZINSKI: I think I'm talking
8 about both. I think both have to be addressed. First, in terms
9 of competition. For
10 instance, right now in Detroit we are having a situation where
11 the National Bank of Detroit and Michigan National are both
12 vying for supermarket business. Michigan National Bank is now
13 implementing a check authorization service. And it has been
14 viewed that this is not a branch operation because all it is
15 is check verifying.

16 Well, once it is established technologically and, I
17 think, also from the viewpoint of function, it would be easy to
18 transfer that into some sort of an EFT system, not only check
19 verification, as the service offered.

20 Similarly, National Bank of Detroit is also working
21 with other supermarket chains to install their mechanisms.

22 Now, I think, here, in terms of competition, there
23 is definitely room for regulating it, either on the issue of
24 sharing, or particularly the issue of sharing as to what banks
25 get to operate, savings and loans, credit unions, get to

1 operate in that particular machine or that particular store
2 chain.

3 But, secondly, I also see the need for regulation as
4 to what happens at the supermarket in terms of safeguards for
5 the consumers. And I think it is in the area of consumer
6 protection when I would definitely see a role for laying down
7 some ground rules, even as applied to basically retail
8 situations.

9 CHAIRMAN ATWATER: Are there other questions?

10 Yes, Mr. Rogers.

11 MR. ROGERS: Senator, I believe you made the state-
12 ment that you would see ATMs and POSs as somewhat less than
13 branches.

14 Have you identified, in terms of new criteria, what
15 you would substitute for branch deployment criteria in this
16 particular instance?

17 MR. DEREZINSKI: What I said basically was, the
18 concept of branch, in its traditional sense and how it was
19 developed, just does not fit. The old idea of branch, the
20 essence of the idea, that the word "branch" being used in the
21 McFadden Act, I think, is basically a physical definition; it
22 is not a functional definition.

23 In our Michigan situation, our Commissioner on
24 Financial Institutions has attached certain rules to the
25 definition in order to make it more functional and sensitive

1 to transactions which happen there. And I know that the federal
2 definition also includes functional language where money changes
3 hands and what have you. But the basic concept is still physical.
4 With the machines and such, that's just not that relevant any-
5 more, where they are set up or how they could be operated. I
6 think we have to move to an even more functional analysis of it,
7 and what that particular definition will be at this time, I
8 don't know. But I think it has to be more functional in terms
9 of the transactions that take place. What that will be, I
10 don't know at this point.

11 How we approached it in the Michigan legislation
12 which went through was basically to provide for the establish-
13 ment of a new type of corporation any time that anyone gets
14 into the electronic transfer funds business, be it on, let's
15 say, a retail basis, as Mr. Worley was indicating, or as a
16 straight financial institution, which we are now talking about,
17 or S&Ls or credit unions, for that matter. It has to be done
18 in terms, I think, of a function, what function takes place.

19 CHAIRMAN ATWATER: You have indicated that you would
20 look, on the issue of consumers' rights and responsibilities,
21 to the states for the initiative, and that would require some
22 revision of the Uniform Commercial Code, Sections 3 and 4.

23 Precisely, how do you visualize that change coming
24 about?

25 I understand this afternoon we will hear testimony

1 by Dr. Haydock that probably the existing Articles 3 and 4 of the
2 UCC are adequate to cover EFT transactions, or if they are not,
3 can be expanded to incorporate it. You have made a formal
4 recommendation for a new section, as I understand it.

5 MR. DEREZINSKI: That's correct, Mr. Atwater. This
6 is the area where I see the clearest role for state government.
7 I have done some research into this to try to find out how it
8 fits right now and some of the problems that you have in trying
9 to fit this new technology to the definitions, and the patina
10 of case law that has developed with Sections 3 and 4.

11 Basically, the problem is that Sections 3 and 4 deal
12 primarily with written instruments, and an electronic impulse
13 or an electronic impulse recorded on a tape is not a written
14 instrument.

15 If you start off with that premise, you see all of
16 the ramifications that flow from it in terms of a person being
17 able to read a signature and tell whether it is a forgery. The
18 whole concept of "know your endorser" is out the window. The
19 personal identification number is not the same thing as a
20 signature. An impulse on a tape which has to be read by a
21 machine just does not do the same thing as reading a check to
22 see whether it is altered or not or whether the person who
23 signed it is in fact the person who has an account.

24 I think, given the definitions as they are now, and
25 the whole concept of the Uniform Commercial Code, which is

1 meant to facilitate commercial transactions, that Section 3 and
2 4 just don't work and that we will have to develop an entirely
3 new article, possibly as an optional article, for those states
4 who see EFTS coming into their jurisdictions.

5 That could be done by the Commissioners on Uniform
6 State Laws which is in existence, which came up with the
7 original Uniform Commercial Code and many other uniform laws
8 which have been adopted by the states. This, I think, is the
9 best approach to go. And I would strongly recommend that this
10 Commission, basically, turn this aspect of the problem over to
11 the states to adopt legislation.

12 CHAIRMAN ATWATER: Thank you very much, Senator.

13 Are there other questions by the Commission?

14 (No response.)

15 CHAIRMAN ATWATER: Thank you for your testimony.

16 MR. DEREZINSKI: Thank you very much.
17
18
19
20
21
22
23
24
25

CHAIRMAN WIDNALL: The next witness is Roberta Wieloszynski.
(Witness sworn.)

1 CHAIRMAN ATWATER: We would appreciate it,
2 Ms. Wieloszynski, if you would proceed with your testimony, and
3 then there will be questions to follow.

4 Thank you.

5 TESTIMONY OF ROBERTA WIELOSZYNSKI, DIRECTOR,
6 SYRACUSE (NEW YORK) CONSUMER AFFAIRS OFFICE.

7 MS. WIELOSZYNSKI: My name is Roberta Wieloszynski,
8 and I'm the Director of the Syracuse Consumer Affairs Office in
9 Syracuse, New York.

10 My introduction to electronic funds transfer came at
11 a conference at the University of Wisconsin, Center for
12 Consumer Affairs, about a year and a half ago, and it was a
13 very interesting conference, except for the workshop on EFT or
14 TFE or whatever it was, and I took it back and filed it under
15 "science fiction" and forgot about it.

16 And then, lo and behold, in December of last year,
17 two EFT systems cropped up in Syracuse, a POS operated by a
18 commercial bank, First Trust and Deposit, followed about two
19 months later by a savings bank offering a pay-by-phone system.
20 Syracuse has a reputation as a test center, so

21 I have had two systems to look at.

22 I am here today to propose that legislation be
23 designed and implemented to control the development of
24 electronic funds transfer system technology, not to impede the
25 development of that technology, but to insure that its

1 development paces the public interest.

2 My comments are based on a continuing experience with
3 EFT on two different levels in Syracuse: a bill-paying service
4 offered by a local savings bank and a point-of-sale terminal
5 system operated by a local commercial bank.

6 My staff and I have received
7 the courtesy and cooperation of both banks throughout our
8 efforts to explore the systems. In a very real way, I think
9 that First Trust and Deposit Company and Syracuse Savings Bank
10 in Syracuse have shown a high regard for the public interest.
11 With the exception that the banks don't believe that legislation
12 is necessary, our goals are remarkably similar.

13 Actually, if there has been any frustration in my
14 exchanges with the banks in regard to EFT developments, it's
15 been due directly to the conflict to the conflict between our
16 shared concerns and our individual methods for dealing with
17 those concerns.

18 Bankers who are developing EFT systems seem to feel
19 confident that any problems that now exist or may develop can
20 be handled without outside intervention, mainly through internal
21 policy procedures.

22 In contrast, bankers who are not developing EFT
23 systems but who feel the competitive pressure to do so, are not
24 quite as enthusiastic about EFT or their ability to deal with
25 its implications

1 In any case, my interest and my concern is based on
2 a question: Are we in control of EFT developments, or are we
3 merely being dragged along by those developments?

4 No matter how that question is answered, we have to
5 face some risk that we will either fail to deal with problems
6 which can be dealt with now, or we will spend our energies and
7 resources to deal with problems which don't, or won't, exist.

8 Perhaps in this instance our awareness of potential
9 trouble is enough to guarantee that we can identify and resolve
10 problems as they actually occur, as the bankers suggest. But I
11 believe the spectre of legislation, particularly national
12 legislation -- and the bankers do perceive it as a spectre --
13 has undercut their ability to recognize the value of legislation
14 as a means by which some problems can be avoided before they
15 become problems. The bankers identify their own policies and
16 marketplace conditions which they believe apply certain
17 guarantees to the development of EFT in the public interest.
18 But they reject the suggestion that their policies and those
19 marketplace conditions should be endorsed and supported by law.

20 Since we frequently make law without providing a way
21 to make the law work, I'm sympathetic to the uneasiness that
22 bankers feel in response to suggestions that burdensome banking
23 law be made even more burdensome. But I also recognize that we
24 have an opportunity to make good law, and an obligation to try
25 to make the law work, that can be of benefit to everyone and

1 every institution affected by EFT technology.

2 Frankly, I would rather that this effort come from
3 the banks themselves. They're the experts on EFT. They would
4 know best how to translate their intentions and concerns into
5 reasonable and workable law. But at the moment, this looks
6 very much like an opportunity that the banks will refuse to
7 exercise, at least until it is exercised by someone else, at
8 which point, defensive counterproposals by the bankers will
9 merely serve to establish an adversary climate that can be
10 highly counterproductive.

11 In any case, I would still like to outline the kind
12 of legislation that I think the bankers should support, even if
13 they won't initiate it.

14 If a credit card is lost or stolen, a consumer is
15 liable for no more than \$50. But no law exists which extends
16 this protection to holders of EFT debit cards. But when
17 I suggest that they should tell people they have this kind of
18 protection, the bankers tell me they can't do that because then
19 some customers may try to take improper advantage of this
20 protection. Of course, thieves may already know.

21 But clearly, if people don't know they're protected
22 they can't use that protection. And this policy still leaves
23 the burden of proof on EFT debit card holders who would be
24 forced to prove that they, themselves, did not improperly
25 authorize someone else to use their cards, or are trying to

1 improperly hide their responsibility for transactions they
2 actually made themselves.

3 Another problem is the security of information
4 developed on consumers by their use of EFT debit cards. That
5 information should be protected from the excesses of snoops,
6 both governmental and private, with exceptions clearly
7 delineated by safeguards.

8 For example, government at any level should be
9 prohibited access to EFT records, except in cases of investiga-
10 tions into serious criminal activity. But even here, those
11 under investigation should be given an opportunity in court to
12 argue against access by government to their EFT records. And
13 that access should only be granted by a court order.

14 Access by private persons or agencies should be
15 permitted only upon the personal, written authorization of the
16 person whose records are being sought. To give this authoriza-
17 tion meaning, a consumer's refusal to permit this kind of
18 access should not be used against him. For example, an employer
19 should not be permitted to withhold employment, or a store, for
20 example, should not be permitted to withhold credit from any
21 person who exercises the right to keep EFT records confidential.

22 The bankers tell me that these kinds of restrictions
23 don't apply now to other kinds of records, particularly bank
24 records, which the courts have ruled are not the property of
25 the people on whom those records are developed. They suggest

1 that I am proposing more protection for EFT records than apply
2 to to the records developed in the kinds of transactions which
3 could be replaced by EFT. In this instance, I am.

4 First, I think that there should be protection of
5 information developed on consumers, no matter where it comes
6 from. But more than that, EFT develops information on people
7 in such an easy-to-use, and abuse, form that I don't think
8 assertions of policy are enough. It must be protected.

9 Right now we have protection for consumers which
10 effectively permits them to withhold payments for goods bought
11 through credit which are the subject of disputes between
12 consumers and retailers. This should be extended to include
13 EFT transactins that now involve a consumer's use of line of
14 credit. And it should be applied to EFT transactions in the
15 future which may involve the actual use of EFT debit cards for
16 credit purposes directly.

17 To the extent that EFT debit cards may be used
18 directly for access to credit, I also think it's important that
19 legislation be drafted to preserve one diversity of credit
20 opportunities which now exist.

21 For example, the bank operating a point-of-sale
22 system in Syracuse may offer its system as an umbrella credit
23 source for all of the stores which are providing terminal services.
24 But the bank should not be permitted to substitute its own
25 standards for credit approval for those which now apply in each

1 of the stores. The stores should be required to set their own
2 approval and operational standards, whether or not they want to.

3 With this protection subscribers of the system would
4 have the convenience of one card for cash and credit access in
5 all of the stores and the bank, but those who now could get
6 credit at one store but not another would still have this
7 opportunity.

8 In another area, if a credit card is stolen, prompt
9 action by a consumer means that that consumer doesn't lose any-
10 thing. If a check is stolen and forged, the bank, not the
11 consumer, accepts the loss. But EFT debit cards introduce a
12 new element. Since transactions are recorded instantaneously,
13 the problem a consumer must face is to have funds restored.
14 And since funds taken illegally from an EFT account can't be
15 used by a consumer until they are restored, a consumer may find
16 he is accruing interest penalties because bills can't be paid.
17 Indeed, since the money isn't available, a consumer can't use
18 it for any of the proper purposes it was intended for.

19 This should be dealt with by legislation that also
20 protects consumers against the consequences of simple errors
21 which occur beyond their control. No matter what the cause, if
22 the consumer's account is improperly debited, and the consumer
23 did not contribute knowingly to the problem, the bank should
24 cover all losses and incidental expenses which occur or, for
25 that matter, the stores should, if that's appropriate.

1 These and other problems are national problems.
2 Whatever the ultimate impact of EFT technology, the impact
3 will be national. So I think the remedies applied to those
4 problems should be national. I'm afraid that any attempt to
5 permit the states to deal with EFT on an individual basis will
6 merely result in a hodge-podge of action and inaction extending
7 from too much to too little on the model that already exists
8 for other state banking law.

9 I'm also afraid that the marketplace, itself, is
10 ill suited to the development of natural controls on EFT
11 development. The marketplace is a vehicle for sales and
12 selling, not for restraint. If the marketplace is permitted to
13 govern the development of EFT technology, we can count on that
14 marketplace to focus on not those of us to whom that technology
15 has been introduced but those of our children who will be growing
16 up with EFT as a fact of their lives. In fact, after I
17 submitted this testimony to the Commission in advance, I got a
18 complaint, my first complaint on EFT, which came from a mother
19 in Syracuse who was shocked by First Trust and Deposit intro-
20 ducing coloring books to children on EFT. So it is being aimed
21 at the children already.

22 Just let me point out that the introduction of credit
23 went through much the same kind of transition. EFT presents a
24 very real potential for a major shake-up in our economic system.
25 Our attempts to deal with EFT developments should be no less

sp14 1 broad. And in a very real way, EFT has given us an opportunity
2 to deal with many problems that should have been handled before
3 in other circumstances but have not been. The security of
4 information is but one of these.

5 In thousands of years, the most that's ever been
6 done to the symbols we use for money is to change what they look
7 like or what they represent. But finally, thanks to the
8 computer, we've discovered a way to do away with symbols
9 altogether. We can now imagine a system in which earnings are
10 deposited automatically, in which prices and values can be
11 established and assessed electronically, and in which money can
12 be exchanged without ever being seen or touched. We're already
13 doing the first with Social Security payments, the second with
14 the Universal Product Code, and the third with EFTS.

15 It takes no great imagination to expect these and
16 other systems to grow together. It also takes no great imagina-
17 tion to wonder at the implications, both good and bad, of this
18 kind of unified cash and credit system. The trend in our
19 society is to bigger and more comprehensive systems, not to
20 smaller and more diverse systems. We tend to forget that the
21 aim of competition is to eliminate competition, something that
22 anyone who has played a game of Monopoly can understand. As
23 the bankers I've talked to suggest, we may never entirely lose
24 the opportunities and alternatives that seem to be threatened
25 by EFT technology. But it is certain that to the extent these

1 opportunities and alternatives remain, they will remain in a
2 context which will have changed substantially because of EFT
3 development. Right now we have the chance to direct those
4 changes into channels that we can control. I suggest that we
5 do it.

6 CHAIRMAN ATWATER: Thank you very much. I must
7 admit, you have added at least one dimension that wasn't there
8 before. Children had not been in our vista until your
9 presentation.

10 MS. WIELOSZYNSKI: I wish I could have brought you
11 the coloring book. I couldn't get hold of it in time.

12 CHAIRMAN ATWATER: Are there questions by the
13 Commissioners?

14 Mr. Wegner?

15 MR. WEGNER: Just the observation that I think a
16 coloring book and a box of crayons ought to be made available
17 to each Commissioner.

18 (Laughter.)

19 CHAIRMAN ATWATER: Mr. Worley.

20 MR. WORLEY: There was a reference made in your
21 testimony -- and I'm quoting now -- "a store, for example,
22 should not be permitted to withhold credit from any person who
23 exercises the right to keep EFT records confidential."

24 I wonder if you would elaborate on that a little
25 bit with respect to EFT records, that might indicate

1 a bad credit record or an unwillingness or inability to pay
2 their bills.

3 MS. WIELOSZYNSKI: Well, I think that, as the
4 Senator mentioned previously,
5 existing law for credit cards and for checks should
6 be applied to EFT now. And we have the Equal Credit Opportunity
7 Act and the Fair Credit Billing Act. In the case of the Fair
8 Credit Reporting Act it took numerous complaints and problems.
9 People who could not get employment could not understand why
10 they could not get employment. I think that information on
11 consumers in an electronic funds transfer system is in a
12 ready-to-be-abused form if it is given out, and I think it
13 should only be given out at the written authorization of the
14 consumer.

15 The bankers do suggest now that they are not giving
16 out information, that their bank policy prohibits that now.
17 My suggestion is that you back up the bank policy or store
18 policy with the force of law.

19 MR. WORLEY: I'm really interested in your feeling
20 with respect to the free flow of credit
21 information that supports our credit system. I'm a little
22 apprehensive that in the process here we may restrict the free
23 flow of credit information, and I'm really interested in
24 whether that is your recommendation. Is that what you are
25 addressing yourself to? Or are we in a different area here?

1 MS. WIELOWZYNSKI: I think the same standards
2 that credit reporting agencies are subjected to should apply
3 to EFT records. That information is passed around now, yes,
4 but the consumer is knowledgeable that the information is
5 being passed around and can challenge the information. And
6 I think that the same standard should apply to the development
7 of EFT technology and the passing around of these comprehensive
8 records on people.

9 And, as has been mentioned by other speakers, and
10 as I mentioned in supporting testimony, I'm concerned about the
11 idea of somebody having many car problems in a year and that
12 information being sold to a new car dealership. The bankers
13 don't do that now. But I think they should be restricted from
14 doing that. And that is another area, the privacy of infor-
15 mation, mailing lists. But that has been mentioned by other
16 speakers.

17 MR. WORLEY: But I want to be sure that I am clear
18 that you are not suggesting in this area that a customer who
19 has a bad credit record should have an opportunity to restrict
20 that information to the credit grantor public in the interest
21 of privacy.

22 MS. WIELOSZYNSKI: My concern is that they have
23 the opportunity to challenge that information if they are
24 notified that the information is being exchanged.
25

1 MR. WORLEY: Thank you.

2 CHAIRMAN ATWATER: Yes, Mr. Tangney.

3 MR. TANGNEY: In your testimony you talked about
4 all of the legislation that you think is needed. Yet, specifi-
5 cally, where is it specified that if we move from a paper
6 system to EFTS is the consumer not protected?

7 You talked about a depository -- and I mentioned
8 this before, as did several speakers. Today, if a bank or a
9 depository institution does something with someone's money
10 without specific instructions, the bank is responsible.

11 In other words, if someone stole a card, went in
12 and took \$100 out of a customer's account, that customer did
13 not authorize it, the bank is responsible. It's difficult for
14 me to see where legislation is needed, particularly when no
15 problems have developed. I mean, you can produce legislation
16 if problems develop. Why anticipate it?

17 I am asking you, isn't there adequate protection
18 today?

19 MS. WIELOSZYNSKI: In discussion with bankers,
20 I think it is divided fifty-fifty with bankers..

21 I spoke to the New York State Bankers Association
22 a couple of weeks ago, and the bankers were arguing amongst
23 themselves about the need for legislation, not having legis-
24 lation, whatever.

25 In Syracuse, with the Syracuse Savings Bank

1 pay-by-phone system that they are operating, the banks have
2 recognized the problem of liability. If a consumer says that
3 they authorized payment on a department store bill or on an
4 insurance bill, if they have no record of that, it is the
5 bank's word against the consumer's. Recognizing their
6 responsibility, the bankers have excluded insurance companies
7 from participating in the system because the president of
8 the bank, who relayed this to me personally, is concerned with
9 what happens if the consumer says, "I authorized payment on
10 my All-State policy," and the bank says, "I'm sorry you
11 didn't," and the policy lapses and the house burns down,
12 who is responsible? Well, the banks would like to let insurance
13 companies participate, and apparently the insurance companies
14 are chomping at the bit to get in on the system. They are
15 being excluded from it, but they are not being excluded from
16 it legally. If the banks chose to change their policy, they
17 could let them participate tomorrow.

18 Now, that's on a higher level. If you take it on
19 a lower level, suppose that the person authorizes payment on
20 a department store bill and the bank says that they didn't,
21 then the consumer is in the position of paying the finance
22 charge on their bill. And who is liable? Who is responsible?
23 It is the consumer who has the burden of proof, not the bank.

24 MR. TANGNEY: But that's true today in the paper
25 system. Everything you said today is true under the paper

1 system. There is no change. Today there are millions and
2 millions of pre-authorized insurance premiums that go through
3 electronic funds transfer. The bank is responsible
4 to prove that the consumer authorized it. If the bank cannot
5 prove that the consumer authorized it, then they cannot do it.

6 MS. WIELOSZYNSKI: If you send in a check to your
7 insurance company, you get a canceled check back, which is
8 legal proof of payment. You wrote out the check and signed
9 your name and they endorsed the check and signed their name.
10 You have proof that you paid them. If you, over the telephone,
11 say, "Pay my insurance coverage," you don't have a record. In
12 fact, the banks were also considering making
13 recordings. They have not made a decision on that yet. And I
14 asked the bankers if the consumer would have access to those
15 recordings as well as the bank, and they haven't decided even
16 whether they are going to record yet, much less whether the
17 consumer has access.

18 If I may also add to that, the bankers, in the case
19 of Syracuse -- and I'm only going by the systems that I have
20 been observing -- in their promotional materials they have a
21 list of the advantages to the consumer and the advantages to
22 the merchant. And I have talked to retailers and merchants
23 and consumers about it, and we did a survey of 47 people using
24 the system. One of the marketing messages is that you don't
25 have to carry around your checkbook. That's one of the

1 advantages of using the system. Well, you do have to carry
2 around your EFT card, and if you don't carry around your check-
3 book, if you wrote out a check yesterday to your landlord to
4 pay your rent and you had sufficient funds in your account and
5 then you go into a department store in Syracuse the next day
6 and it instantaneously accesses your account and transfers it
7 to the store and then your rent check bounces, you had better
8 carry your checkbook around with you. And you had better have
9 an up-to-date balance.

10 MR. TANGNEY: The exact same thing happens today.
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

1 CHAIRMAN ATWATER: Ms. Reed?

2 MS. REED: Yes.

3 You stated that government at any level should be
4 prohibited to EFT records, but you made an exception in the
5 case of investigation into serious criminal activity.

6 How would you define "serious criminal activity,"
7 and what would be the threshold before access would
8 be provided?

9 MS. WIELOSZYNSKI: I expanded on this in my
10 supplementary testimony, which I can't find; I'm sorry.

11 The gist of it -- and there are a couple of pages
12 on it -- I believe that a court order should be required for
13 the government to go in and access somebody's account; that
14 is, if it is for a criminal prosecution. But, in the case of
15 a private institution, our suggestion is that it be at the
16 written authorization of the consumer.

17 CHAIRMAN ATWATER: Thank you very much.

18 Are there other questions?

19 Mr. Beech?

20 MR. BEECH: On page 4 you talk about the disputes
21 between consumers and retailers and extending the protection
22 that now exists over to lines of credit.

23 Am I correct in what you mean by this? If I use
24 a line of credit at a credit union to make a purchase at a
25 retail store, and I am dissatisfied with the goods, I would

1 withhold the payment to the credit union?

2 MS. WIELOSZYNSKI: Yes. The same protection that
3 you have in using a credit card now. The debit cards that
4 were sent out in Syracuse, I believe 10,000 -- no, it's higher
5 than that -- 20,000, I believe, were sent to people unsoli-
6 cited. They were not sent out to people who had line-of-
7 credit authority; unsolicited, because I think the bankers
8 amongst themselves felt that that would be considered a credit
9 card.

10 In their initial advertising, they said that it
11 is not a credit card, that it is an additional use of a piece
12 of plastic. In the
13 ads they are running this week -- it is replacing credit cards
14 and checks. They have kind of made a transition there.

15 CHAIRMAN ATWATER: Any other questions by the
16 commissioners?

17 MR. TAYLOR: I was interested in a statement you
18 made concerning standards of credit worthiness, vis-a-vis
19 banks and retailers. Were you suggesting that they should
20 have identical standards of credit worthiness? And, if that
21 is what you are suggesting, why?

22 MS. WIELOSZYNSKI: I am suggesting the opposite,
23 that the diversity of credit standards be preserved under
24 electronic funds transfer. The same thing with the finance
25 charges.

1 In Syracuse we did a survey a couple of months ago
2 on different finance charges that retailers have. There are
3 three different methods of accruing interest: the previous
4 balance method, the adjusted balance method, the average daily
5 balance method. And we are suggesting that those, even the
6 method of accruing finance charges, be preserved and not one
7 system developed, that people who may be able to get credit
8 now at one particular store, not at another, will not be
9 exempted from getting credit because there is only one
10 standard. I think that would be a very negative effect.

11 MR. WORLEY: To follow up on that point, in your
12 testimony -- and I'm quoting a sentence -- "The stores should
13 be required to set their own approval and operational
14 standards, whether or not they want to." I wonder if you
15 would elaborate on that a little bit. I don't know whether
16 to be frightened by that or not.

17 MS. WIELOSZYNSKI: That would be a difficult thing
18 to prove, but I want to insure that the stores have the
19 opportunity to preserve their own standards, that a banker
20 doesn't come in with a piece of plastic which is very at-
21 tractive, that can do everything, and that it starts limiting
22 the kinds of opportunities that people have for
23 different kinds of credit. You can't insure that the store
24 is not going to go along with, perhaps, a suggested bank
25 policy for credit standards, but I would like to give them the

1 opportunity to have their own, to preserve the diversity of
2 credit opportunities.

3 CHAIRMAN ATWATER: Thank you very much, Ms.
4 Wieloszynski.

5 I think we have completed the time that we can work
6 on this issue. We appreciate very much your excellent
7 testimony.

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

National Commission on Electronic Fund Transfers
Users Committee Public Hearings
"Consumers Issues in EFT"
October 26 and 27, 1976
Washington, D.C.

The documents which follow are submitted for the record
of this hearing by:

Roberta Wieloszynski of
Syracuse, N.Y. Consumer Affairs Office

My name is Roberta Wieloszynski. I'm the Director of the Syracuse (New York) Consumer Affairs Office.

I'm here today to propose that legislation be designed and implemented to control the development of electronic funds transfer system technology... not to impede the development of that technology... but to ensure that its development paces the public interest.

My comments are based on a continuing experience with EFT on two different levels in Syracuse: a bill-paying service offered by a local savings bank, and a point-of-sale terminal system operated by a local commercial bank.

I should add here that my staff and I have received the courtesy and cooperation of both banks throughout our efforts to explore the systems. In a very real way, I think that First Trust and Deposit Company and Syracuse Savings Bank in Syracuse have shown a high regard for the public interest. With the exception that the banks don't believe that legislation is necessary, our goals are remarkably similar.

Actually, if there has been any frustration in my exchanges with the banks in regard to EFT developments, it's been due directly to the conflict between our shared concerns and our individual methods for dealing with those concerns.

Bankers who are developing EFT systems seem to feel confident that any problems that now exist (or may develop) can be handled without outside intervention... mainly through internal policy procedures.

In contrast, bankers who are not developing EFT systems, but who feel the competitive pressure to do so, are not quite as enthusiastic about EFT... or their ability to deal with its implications.

In any case, my interest and my concern is based on a question: are we in control of EFT developments... or are we merely being dragged along by those developments?

No matter how that question is answered, we have to face some risk that we will either fail to deal with problems which can be dealt with now... or we will spend our energies and resources to deal with problems which don't... or won't... exist.

Perhaps in this instance, our awareness of potential trouble is enough to guarantee that we can identify and resolve problems as they actually occur... as the bankers suggest.

But I believe the specter of legislation, particularly national legislation... and the bankers do perceive it as a specter, has undercut their ability to recognize the value of legislation as a means by which some problems can be avoided... before they become problems. The bankers identify their own policies and marketplace conditions which they believe apply certain guarantees to the development of EFT in the public interest. But they reject the suggestion that their policies and those marketplace conditions should be endorsed and supported by law.

Since we frequently make law without providing a way to make the law work... I'm sympathetic to the uneasiness that bankers feel in response to suggestions that burdensome banking law be made even more burdensome.

But I also recognize that we have an opportunity to make good law, and an obligation to try to make the law work, that can be of benefit to everyone and every institution affected by EFT technology.

Frankly, I would rather that this effort come from the banks, themselves. They're the experts on EFT. They would know best how to translate their intentions and concerns into reasonable and workable law.

But at the moment, this looks very much like an opportunity that the banks will refuse to exercise... at least until it's exercised by someone else. At which point, defensive counterproposals by the bankers will merely serve to establish an adversary climate that can be highly counterproductive.

In any case, I'd still like to outline the kind of legislation that I think the bankers should support, even if they won't initiate it.

If a credit card is lost or stolen, a consumer is liable for no more than \$50. But no law exists which extends this protection to holders of EFT debit cards... although the cards, when used in conjunction with checking account line-of-credit, are credit cards.

The bankers I've talked to suggest that it is their policy to make up all losses to EFT debit card holders. But when I suggest that they should tell people they have this kind of protection, the bankers tell me they can't do that... because then some customers may try to take improper advantage of this protection. (Of course, "theives" may already know.)

But clearly, if people don't know they're protected, they can't use that protection. And this policy still leaves the burden of proof on EFT debit card holders, who would be forced to prove that they, themselves, did not improperly authorize someone else to use their cards... or are trying to improperly hide their responsibility for transactions they actually made themselves.

Another problem is the security of information developed on consumers by their use of EFT debit cards. That information should be protected from the excesses of snoops... both governmental and private... with exceptions clearly delineated by safeguards. For example, government at any level should be prohibited access to EFT records, except in cases of investigations into serious criminal activity.

But even here, those under investigation should be given an opportunity in court to argue against access by government to their EFT records. And that access should only be granted by a court order.

Access by private persons or agencies should be permitted only upon the personal, written authorization of the person whose records are being sought. To give this authorization meaning, a consumer's refusal to permit this kind of access should not be used against him. For example, an employer should not be permitted to withhold employment, or a store for example should not be permitted to withhold credit, from any person who exercises the right to keep EFT records confidential.

The bankers tell me that these kinds of restrictions don't apply now to other kinds of records... particularly bank records, which the courts have ruled are not the property of the people on whom those records are developed. They suggest that I'm proposing more protection for EFT records than apply to the records developed in the kinds of transactions which could be replaced by EFT.

I am.

First, I think that there should be protection of information developed on consumers... no matter where it comes from. But more than that, EFT development of information on people in such an easy to use (and abuse) form that I don't think assertions of policy are enough. It must be protected.

Right now we have protection for consumers which effectively permits them to withhold payments for goods bought through credit which are the subject of disputes between consumers and retailers. This should be extended to include EFT transactions that now involve a consumer's use of line-of-credit. And it should be applied to EFT transactions in the future, which may involve the actual use of EFT debit cards for credit purposes directly.

To the extent that EFT debit cards may be used directly for access to credit, I also think it's important that legislation be drafted to preserve the diversity of credit opportunities which now exist.

For example, the bank operating a point-of-sale system in Syracuse may offer its system as an umbrella credit source for all of the stores which are providing terminal services. But the bank should not be permitted to substitute its own standards for credit approval for those which now apply in each of the stores. The stores should be required to set their own approval and operational standards... whether or not they want to.

With this protection, subscribers of the system would have the convenience of one card for cash and credit access in all of the stores and the bank... but those who now could get credit at one store but not another would still have this opportunity.

In another area, if a credit card is stolen, prompt action by a consumer means that that consumer doesn't lose anything. If a check is stolen and forged, the bank, not the consumer, accepts the loss. But EFT debit cards introduce a new element. Since transactions are recorded instantaneously, the problem a consumer must face is to have funds restored. And, since funds taken illegally from an EFT account can't be used by a consumer until they are restored, a consumer may find he's accruing interest penalties because bills can't be paid. Indeed, since the money isn't available, a consumer can't use it for any of the proper purposes it was intended for.

This should be dealt with by legislation that also protects consumers against the consequences of simple errors which occur beyond their control.

No matter what the cause, if a consumer's account is improperly debited, and the consumer did not contribute knowingly to the problem, the bank should cover all losses and incidental expenses which occur.... or, for that matter, the stores should, if that's appropriate.

These and other problems are national problems.

Whatever the ultimate impact of EFT technology, that impact will be national.

So I think the remedies applied to those problems should be national.

I'm afraid that any attempt to permit the states to deal with EFT on an individual basis will merely result in a hodge-podge of action and inaction extending from too much to too little... on the model that already exists for other state banking law.

I'm also afraid that the marketplace, itself, is ill-suited to the development of natural controls on EFT development. The marketplace is a vehicle for sales and selling... not for restraint. If the marketplace is permitted to govern the development of EFT technology, we can count on that marketplace to focus on... not those of us to whom that technology has been introduced... but those of our children who will be growing up with EFT as a fact of their lives.

Just let me point out that the introduction of credit went through much the same kind of transition.

EFT presents a very real potential for a major shake-up in our economic system. Our attempts to deal with EFT developments should be no less broad. And, in a very real way, EFT has given us an opportunity to deal with many problems that should have been handled before in other circumstances but have not been. The security of information is but one of these.

In thousands of years, the most that's ever been done to the symbols we use for money is to change what they look like or what they represent. But finally... thanks to the computer... we've discovered a way to do away with symbols altogether.

We can now imagine a system in which earnings are deposited automatically ... in which prices and values can be established and assessed electronically... and in which money can be exchanged without ever being seen or touched.

We're already doing the first with Social Security payments... the second with the Universal Product Code... and the third with EFTS.

It takes no great imagination to expect these and other systems to grow together. It also takes no great imagination to wonder at the implications... both good and bad... of this kind of unified cash and credit system.

The trend in our society is to bigger and more comprehensive systems... not to smaller and more diverse systems. We tend to forget that the aim of competition is to eliminate competition... something that anyone who has played a game of Monopoly can understand.

As the bankers I've talked to suggest, we may never entirely lose the opportunities and alternatives that seem to be threatened by EFT technology. But it is certain that to the extent these opportunities and alternatives remain, they will remain in a context which will have changed substantially because of EFT development.

Right now, we have the chance to direct those changes into channels that we can control. I suggest that we do so.

Roberta B. Wieloszynski

Director

Syracuse (N.Y.) Consumer Affairs Office

(315) 473 3240

1532

1

The following is a supplemental discussion of those issues surrounding EFTS which may require national legislative solutions.

Privacy

Consumers today have little practical control over the collection and dissemination of information distilled from their private lives as a consequence of their interaction with the society they're a part of.

Birth notices, credit applications, employment histories, even obituaries are noted and filed in a fragmentary but comprehensive system of information which is relatively easy to penetrate. That penetration now takes place on a variety of levels.

Mailing lists are compiled from magazine subscription lists. The Internal Revenue Service may compel banks to surrender the financial records of bank customers. Credit institutions trade dossiers on consumers back and forth at will. In the examination of prospective employees, government and private agencies alike probe routinely into social, economic, medical, and criminal information resource centers that the objects of such investigations, themselves, may not even know exist.

The information uncovered is useful on two levels. First, the details of a consumer's social record, economic history, and other elements of personal information can establish a model for anything from sales techniques to surveillance. But second, even if the details are not discernable, the broad categories of activities and associations to be established by an inspection of personal records can still be used to build a descriptive pattern. Knowing that a consumer bought an expensive foreign car is just as valuable as knowing the actual price paid for the car. Often just knowing which stores are patronized by a consumer can be valuable.

Virtually every change in our economic system has added a new source of information to be concerned about. The advent of credit is one change. The computer is another.

An extension of the development of the computer, EFT technology has added one more dimension to the problem... the consolidation of multiple information sources into a single source.

Privacy has always been threatened by the assembly and use of information without the knowledge or consent of the people on whom the information is gathered... or when people are compelled to submit to an investigation, the results of which will not be conveyed to them.

But EFT technology seriously erodes any inherent protection consumers have enjoyed purely because of the fragmented nature of information sources. No information is more readily available than it is in a computer-based storage system which can be programmed to perform a variety of collection, sorting, and information transfer functions automatically. And no information is more valuable in the development of a pattern of a person's life than information which details economic habits.

It can be suggested with some certainty that most people would strongly object to the publishing in the daily newspaper of their earning and spending records. But in terms of those who could benefit from access to this information, publishing a consumer's economic history in the newspaper wouldn't represent much of an additional threat.

Given the potential quantity and quality of the information to be developed on people through their use of EFT systems, and the inherent lack of control people will have over that information, several rights should be established to protect EFT information records and the privacy of the people those records represent.

Access to such information should be restricted by law. People should be informed when exceptions are to be applied. And people should be permitted to challenge and block access that they believe is inappropriate.

And whenever information is to be given to others, the same information should be provided to the people involved.

Some people may have no objection at all to the dissemination of their records to others. Some may not want to know when their records have been requested, who has requested them, or why they've been requested. But they should have the opportunity to know. With that opportunity, they have a choice. Without it, they don't.

Point-of-sale systems in particular may seem to enhance confidentiality by reducing the number of persons who have access to information developed through such systems. But the number of people who have access to EFT records has no bearing on whether or not the IRS can get access to those records... whether or not the bank, itself, can make special use of the records... or whether or not a consumer could be coerced by special circumstances into giving someone else access to those records.

Right now, the IRS can get access to EFT records. Right now, a bank can use EFT records to determine a consumer's credit worthiness. And right now, EFT records could be obtained by prospective employers or those who extend credit by making access a condition of employment or credit.

It's true that consumers do have access to credit because they make information on themselves available to lending and credit-approval agencies... consumers have gained some cost benefits from the use of computers in business and industry... Consumers are protected against certain forms of discrimination and criminal activity because information is available to investigators.

But trade-offs which establish benefits must be balanced by limits which guard against excesses.

Generally, banks can be expected to support policies which would resist encroachments on consumer information rights. But as one recent Supreme Court decision made plain, by rejecting the contention that bank records are private, bank policy alone is insufficient protection.

More is necessary.

Summary

Computerized banking systems can develop information on consumers which is in a form that is easy to use and abuse. As EFT systems grow to include more services, they will encompass more information. That will increase both the value of EFT records and the pressure to get access to such records.

EFT records are now considered the property of the banks which hold them. The public is denied an effective measure of control over the use of those records.

Specific problems can be identified:

People need not be informed when access to their records has been requested or granted.

Beneficial limitations to access have not been established as a matter of law.

Additionally, protection granted by law to consumers for certain kinds of information apparently are not extended to the same kinds of information when that information is gathered in an EFT system.

For example, a consumer may challenge the accuracy of information in credit reporting agency files. But it presently appears that the same information, assembled in an EFT system, and used for the same purposes, might not be covered.

Recommendation

Legislation should be adopted which limits access by persons or agencies, private or governmental, to EFT generated or assembled information.

Government should be permitted access only in connection with investigations of serious crimes. Procedures should require a court proceeding which permits a person to challenge a governmental request for access to EFT records.

Private persons and agencies should be permitted access to EFT records only upon the express, written permission of the person whose records are being sought. To give this control meaning, a consumer who refuses to give access to EFT records to a private person or agency should not be subject to retribution.

For example, an employer should not be permitted to withhold employment from a person solely because the employer is denied access to that person's EFT records. A store should not be permitted to deny credit to a person only because the store is denied access to that person's EFT records.

The legislation should provide for criminal penalties for those who permit the unauthorized dissemination of EFT records. But civil procedures should also be established to provide for civil damage lawsuits aimed at all persons or agencies which participated in the illegal dissemination.

Additionally, legislation which now protects consumer information in other contexts should be extended to include information of the same sort which is made part of EFT records and used for similar purposes. If a consumer should give permission to a store to use EFT records for credit purposes, the consumer should be given the opportunity to examine and challenge those records for accuracy... particularly since there is no guarantee that only information developed through an EFT system would be made part of those records.

Comments

It's true that controls like these have not been provided for information developed through a consumer's use of cash, or checks, or credit cards, per se. But that is no argument against establishing these controls for information to be generated through the use of EFT systems.

EFT presents special potential risks to privacy and the security of consumer information. Special action should be taken to eliminate these risks.

Consumer Choice

EFT is the first development in banking and finance which has the capacity to substantially reduce the use of all other forms of economic exchange... including checks, cash, credit cards, loans, travelers' checks, and more.

Ultimately, EFT could not only reduce these alternatives, it could well replace most of them.

Essentially limited at present to an electronic means to reduce a bank's load of paper transactions, through either point-of-sale terminals or telephone bill-paying services designed to replace checks, EFT technology can easily encompass credit. Linked to automated payroll deposit services and computerized price-inventory systems like the Universal Product Code, an EFT network could provide virtually every type of personal economic service, with access requiring only a single authorization card, perhaps called a "uni-card."

The potential attractiveness to consumers of a single card which can perform the work of many cards, as well as cash and checks, is self-evident. But to achieve this kind of convenience at the expense of the multiplicity of standards and opportunities that individual credit sources and money alternatives now provide may also present more dangers than benefits.

A uni-card might not eliminate checks. But a checking account may be a service that is only available at some special charge... above that which now is applied to checking services. Clearly, as the machinery set up to handle checks begins to handle fewer and fewer checks, the cost of handling each remaining check is increased. Ideally, the need for machinery (including people) will be reduced as the need for paper transactions is reduced. But eventually, a level will be reached at which the service becomes a frill that is comparatively expensive to provide.

CONTINUED

3 OF 6

And, of course, once an alternative EFT service exists on a large enough basis, checking account service charges can be raised to some level that will serve as a further inducement for a change-over to EFT.

Additionally, the extent to which a bank, or a retailer, for that matter, must actually handle cash is another consideration. Cash that's kept in a vault is both safer and subject to fewer handling charges than cash which must be handled and exchanged. Tellers and guards cost money. Cash can be lost or stolen.

With sufficient facilities, an EFT system could so substantially reduce the need for the exchange of cash from hand to hand that terminal points could easily replace branch banks.

If EFT doesn't replace cash, we might well find that there's a charge connected with asking for and using cash in an EFT-based economic system.

But while eliminating one kind of criminal by eliminating cash and checks, at least to a substantial degree, the advent of a uni-card could also lead to the appearance of a new kind of criminal, one adept at the manipulation of computers and uni-cards, rather than combination safes and locked doors.

Instead of being required to steal cash, checks, and credit cards, a thief would find one card giving access to a consumer's entire assets. At one level, security is increased. At another, it is decreased. The trade-off could easily be counterproductive.

But specifically with regard to credit, a uni-card could easily replace individual standards for credit along with the individual cards which now serve those standards.

Small stores, large stores, national credit companies, banks, finance companies, all have relatively different standards which must be met by those who seek credit. All may also use a variety of methods for computing interest charges.

Right now, some people may qualify for credit from any of these sources. Some people may qualify for credit from some of these sources. Some people may qualify at only one store or bank. And others may not meet the standards of any of these sources.

In a uni-card system which serves many sources on the basis of one set of standards, people who now have at least limited access to credit might be denied credit altogether.

The variety of interest rate systems could be replaced, as well, by a single system, with users of uni-card credit services denied the choice of lower cost credit services.

Normal marketplace influences might be expected to encourage many credit sources to maintain their own credit card services, if only because of the personal consumer identification that is maintained with a store through its credit cards.

But a credit card system is expensive to maintain. Few if any store credit cards provide high enough interest rates to ensure some level of noticeable profitability. And a store which operates its own card system also assumes its own risks for losses to thieves and deadbeats.

A uni-card credit system offered by a bank might, for both cost and reliability considerations, be too attractive to be ignored by many credit sources.

It would be relatively easy for any bank which offers both EFT services and BankAmericard or Mastercharge to combine these two services. But more simply, a bank might just promote its line-of-credit service as an integral part of its EFT services.

Specific developments along these lines are difficult to project with certainty. But the implications are worthy of some consideration.

Summary

The future result of the development of EFT technology may be a major readjustment in the shape of the national economy. Combining compatible computer-based systems can produce a new system of exchange based on a single card that can be used in place of cash, checks, credit cards, and other devices. These common economic symbols may not entirely disappear, but their continued existence may involve special consumer expenditures which are intended to encourage their replacement by an EFT system.

Beginning as merely one more choice for consumers, EFT could become the means by which other choices are lost, or by which the added expense of these choices denies them to many people.

Appearing at first glance to be a more secure method for handling money, EFT may merely turn out to be a more complex focus for specialized criminals who, if they obtain access to EFT accounts, will have obtained access to a more complete assembly of consumer resources than has been available to thieves until now.

Recommendation

A diversity in symbols is considerably less significant a consideration in regard to credit than a diversity in standards which give a maximum number of people access to credit.

Legislation should prohibit the development of broad credit standards that are to be applied beyond any individual credit source. Briefly, a retail outlet which chooses to adopt an EFT card for credit purposes must be required to set its own standards for credit to be offered through the cards, and, in keeping with current state law, its own methods for computing finance charges.

To deal with a problem which exists even now, legislation should require that consumers are informed whenever a transaction will access their line-of-credit authority.

It should also be made possible for a consumer to obtain an up-to-date cash/credit balance report in connection with transactions.

To the extent that branch banks may be eliminated in favor of computerized terminal centers, legislation should require that EFT services be developed to encompass those services which would also be lost. Minimum service standards for EFT terminals which replace branch banks should include the basic list of loan, consumer credit, and cash/checking-related services, account information, and advice that would otherwise be lost.

Provision should be made for the impact of EFT service costs on retailers. If retailers or others who are called upon to operate EFT terminals are to bear staffing and other operational costs, and if those costs are to be assessed by those operating the terminals, rather than having them defrayed by a bank through cost-benefit savings, those costs should be assessed to users of the terminals... not to the store's general customers through the prices they pay in the store.

The costs associated with EFT should not be hidden in general prices for goods and services.

This may somewhat balance the tendency for banks to use service charges as a device to encourage the use of EFT facilities, rather than cash or checks.

Comments

The issue of security will be dealt with elsewhere.

It may be impossible, indeed improper, to legislate against the impact of EFT technology on symbols like cash and checks. But every effort should be made to make sure that such a transition is not pressed on the public by indirect pressures. Obviously, cash and checks, for example, now cost people something. Nothing is free. But they should not cost something more to encourage their elimination.

To the extent that automatic payroll deposit systems may be combined with developments like the Universal Product Code and EFT, some regard should also be paid to the impact of purely electronic systems on prices. Prices, for example, would tend to lose their impact in a system in which they are assessed and collected electronically. Only when money physically changes hands do prices have real meaning.

One of the last places that cash is still required is the supermarket. Prices in supermarkets do have impact. Supermarkets are constantly under fire for their pricing and marketing practices.

Yet supermarkets are switching to the Universal Product Code system... not one by one... but chain by chain. Supermarkets are opposing legislation that would require them to keep readable prices on their products. And supermarkets are the biggest customers for point-of-sale terminals.

Major changes are taking place that have nothing to do with EFT development, but which together with EFT carry serious implications for choices and opportunities that most people today take for granted.

If developments are permitted to go forward solely on the basis of decisions of costs and savings, consumers will lose choices that should be preserved at almost any cost.

Consumer Rights and Responsibilities

On the one hand, the development of EFT appears to be proceeding largely outside the scope of current consumer protection legislation. On the other, that development also appears to be proceeding with insufficient emphasis on information that would help consumers protect their rights and meet their responsibilities in the confusion which can... and often does... exist now.

To the extent that there is confusion, it stems from the use of an EFT card in place of cash in some circumstances, in place of checks in the same

or different circumstances, or in place of credit cards in others.

When used in place of a credit card, as in the use of an EFT card for purchases that tan into a line-of-credit, EFT is outside protective legislation which permits payments to be withheld during disputes over goods bought with credit cards. In Syracuse, the bank providing EFT point-of-sale services maintains the bank's Key Cards are not credit cards. But the bank has also refused to send the cards unsolicited to people whose checking accounts provide line-of-credit authority. Clearly, when used with these accounts, the card can be a credit card.

On the one hand, the banks says the cards are not credit cards. On the other, it acts as though they are.

When used in place of checks to obtain cash, an EFT card and associated codeword (or other identification devices) substitute a piece of plastic and a piece of specialized knowledge (the codeword) for the security inherent in an identification procedure that requires a signature and an identification check to verify that signature. A thief who has stolen a book of checks must have some skill to forge signatures on those checks and to pass identification procedures. The same thief who has stolen an EFT card and obtained its associated codeword (perhaps because the word was written down and carried in a wallet) needs no special skills to present the card and codeword at any computer terminal.

In the one case, there is no automatic acceptance. In the other there is. In the one case, a classical case of forgery is involved, with liability well established. In the other, although a signature may be required on a transaction slip, with this constituting forgery, liability is far from clear-cut.

The bank in Syracuse maintains that signing someone else's name to a transaction slip constitutes a forgery. But suppose a thief merely scribbles

an unrecognizable signature? And currently in New York State and others, there is no requirement for any signature at all on a transaction slip. A bank in New York State could eliminate this provision from its transaction procedures.

The misappropriation and use of an EFT card clearly would violate some law or other. But some confusion surrounding the verification procedures, or lack of them, which are now associated with EFT in Syracuse, at least, leaves liability at issue.

Would a consumer be required to prove that an illegal use of a card was unauthorized? Could this be proven? Would the store be held liable for consumer or bank losses to the illegal use of a card? If a bank now accepts liability for losses due to thefts now, will it be required to do so in the future?

When used in place of cash in the direct purchase of goods or services, an EFT card can contribute to the obscuring of errors that would have been visible in the hand-to-hand exchange of cash. This can particularly be a problem in the atmosphere of a retail outlet which is either hectic or psychologically designed to repress caution and judgement, as in the impulse-emphasizing atmosphere of a supermarket.

An overpayment or an underpayment could go undiscovered by a consumer, only to become an issue of contention later. If the consumer contributed to that error, he will find no defense in assertions that the confusion of a store's surroundings helped make the error possible. If a consumer merely failed to detect the error, and it is ultimately corrected, that consumer has still experienced an inconvenience that might not have existed to begin with in a cash transaction.

In point-of-sale systems, there is no clear liability established for errors which might transfer more or less funds from a subscriber's account to a retailer's account, or for debits that occur as the result of an error, and which deny a subscriber the use of funds that would have been available otherwise. There is no way to redress errors which could embarrass a subscriber; for example, an error which fails to approve a transaction that should have been approved... or one that approves a transaction that should not have been approved.

In the Syracuse point-of-sale system, for example, it is possible for a transaction to be approved even though outstanding checks which have not yet been cleared do not leave enough funds in a checking account to cover the transaction. If a consumer fails to maintain an up-to-date balance, the use of EFT can lead to bounced checks. Yet, when the system was first promoted, people were told that they need not carry their checkbooks with them.

A bill-paying service which fails to pay a bill on time could subject a subscriber to an interest penalty that was not warranted. The bank operating the bill-paying service in Syracuse has acknowledged this problem by refusing to permit insurance premium payments through its system. The bank recognizes that it may be held liable for the consequences of a missed payment, a cancelled insurance policy, and any subsequent uninsured loss that may result. But there is still no clear liability for who bears the consequences of errors in other instances. Those consequences can include unnecessary fees or interest penalties and the loss of the use of funds which should have been available to a consumer. And a bank could argue that a consumer assumes all liabilities in connection with the use of either point-of-sale or bill-paying services.

The issue of liability is clearly evident in the EFT card-credit card comparison.

Even when EFT cards can be used as credit cards, they may not be covered by credit card liability limitations which protect consumers against the losses that result from an unlawful use of credit cards. If a credit card is stolen, a consumer can be assessed no more than \$50, no matter how high a bill results from a card's use by a thief. This protection does not necessarily apply to EFT cards.

In Syracuse, the bank asserts that it would assume full liability for losses that would occur through the theft of an EFT card. The bank has established a limit to the number of transactions to be permitted without question in any one day and the maximum amount of cash to be withdrawn from a single account at any one time or in any single day.

But the bank has not provided its customers with this information. And the bank's policies could change at any time. And other banks may establish significantly different procedures.

Summary

EFT technology, to the extent it replaces (or can replace) cash, checks, credit cards, or other economic tools, is developing outside the scope of consumer protection legislation.

Questions of liability are either unanswered, or only partially answered by individual policies at individual banks.

Adequate information from which consumers could act to protect their rights and meet their responsibilities has not been provided for those using EFT systems, or being encouraged to use the systems.

Recommendation

Legislation should be prepared which extends all pertinent law dealing with checks and credit cards to cover EFT transactions which perform the

same jobs as checks or credit cards. This should include the liability limitations established for credit cards and a ban against the unsolicited distribution of debit cards. It should also include provisions which permit consumers to recover funds spent on goods or services which are successfully disputed; or, in the case of actual credit transactions, it should provide for the withholding of payments until disputes are resolved.

Legislation should be drawn which establishes clear lines of liability. Provisions here should permit consumers to recover all losses and expenses which are incurred as the result of errors to which they have not substantially contributed.

Legislation should also be established to give the burden of proof to banks with regard to fraud in EFT systems which require no proof of identity for customers beyond cards and codewords (or other specialized knowledge).

Legislation should be prepared which requires banks to prepare detailed descriptions of all rights and responsibilities for all parties to EFT transactions. Both consumers and retailers providing EFT services for banks should be clearly advised on all risks their participation may entail.

Comments

Some attention should be paid to the use of records generated by EFT systems as proof of payment or other activity. Legislation might be designed to establish appropriate guidelines, but the courts may be a more appropriate forum for this issue.

Basically, when a consumer engages in a transaction directly with a retail store, a check or a receipt is involved which is mutually acknowledged by both parties. This is not necessarily the result in transactions occurring through a point-of-sale terminal.

For example, both the store and a consumer get a copy of the initial transaction slip. But subsequent statements issued to each by the bank could indicate different information than appeared on one or the other of these slips.

In this case, it is not certain which records would be accepted as accurate by parties to a dispute.

Additionally, it's possible that a consumer and a retailer may get a copy of a transaction receipt which accurately reflects the substance of a transaction, but either more or less money is actually transferred to a store's account from a consumer's account than the copies of the receipt indicate was transferred. This situation would seem to indicate that the transaction receipts are not certain enough to be used as proof... if only because they don't reflect all pertinent circumstances in a transaction.

On the other hand, the statement covering the transaction which is later issued by the bank to each of the parties involved will merely detail the amount transferred, without serving as a means by which it can be proved one way or the other that the amount was... or was not... the proper amount.

Clearly, a check or receipt and an itemized bill which are available for comparison are not precisely replaced by records generated through the use of EFT systems.

Security

A clerk assigned to a point-of-sale terminal at a store in Syracuse, when questioned about the use of codewords as a security measure, insisted that she could not tell what codeword people were using because there are three letters on each pin pad button, and she couldn't see which letters they were using. It's doubtful that a thief would fail to notice that it's only necessary to see which buttons are pushed and to note the sequence used in order to completely eliminate a codeword as a security device.

A few moments spent in casual observance of transactions, followed by the theft of a wallet is all a thief needs to transfer any security from a card-holder to himself.

But that is only half of the EFT security problem.

The greater threat probably comes from the possible illegal access to be gained internally... either through the actions of employees or their cooperation with others.

This latter problem is not unique to EFT. And a variety of law exists to proscribe and punish such activity. But as computers are given more economic responsibilities, and as computers assume more functions in direct public contact, the ramifications of crime committed by expert technicians takes on a special significance.

As was noted elsewhere, an EFT computer can bring a variety of consumer economic resources together, making them vulnerable in a single instance of criminal activity. A computer can also be used to hide an illegal entry to these assets in a variety of ways for varying lengths of time. Records can be doctored, fake accounts established, or funds transferred from account to account to account to confuse security measures.

It is unlikely that consumers will lose their funds directly to widespread or large internal thefts. But the costs of security measures substantial enough to shortcircuit the substantial rewards to computer criminals could lead to unexpected indirect losses to consumers. Whatever a bank loses to internal thieves or to security measures designed to control internal thefts, those losses will be reflected in operational costs that ultimately could be passed on to consumers, much as the banks now insist savings will be passed on.

Undoubtedly, the security problem will be confused by the tendency for some people to "lend" their EFT authority to family members or friends. At the least, this will leave honest people unable to account for all transactions made with their approval.

With regard to breaches of security which occur outside the system, the only indication a consumer will have of illegal access to his EFT account is the comparison to be made between personal receipts of transactions, and the bank's periodic statements.

If a consumer keeps all receipts, and if a bank issues statements frequently, and if a consumer makes an effort to compare the two, illegal transactions which occur through misuse of an EFT card will be apparent. But some people presently fail to keep good records, or to work with those records to protect themselves. This will continue to be a problem. Some people will continue to let others use their EFT cards and security words, or to lose track of them. Many husbands and wives share credit cards. They may share debit cards the same way, instead of obtaining individual cards. Others will carry their codewords in wallets along with cards.

Beyond these problems, banks are not required to issue periodic or comprehensive EFT statements. In Syracuse, in fact, the bank offering POS services claims that its statements are so undetailed that they enhance, rather than detract from privacy; although in terms of security, the information that's missing from those statements is detrimental.

With proper safeguards against the dissemination of EFT records, detailed statements issued to consumers can serve valuable security purposes.

With regard to breaches of security which may occur internally, the detection of such breaches will depend upon the security controls and safeguards established internally to deal with this problem. And it will be a special problem as more banks plug-back EFT operations or turn to third-party hardware or software providers.

Recommendations

Legislation should be established which sets standards for the security of computer-based EFT systems, and which provide for the periodic review of adequacy and compliance.

Legislation should require that statements on EFT transactions be issued to consumers at least monthly, and that the statements detail the time, place, goods or services, type of transaction and amount involved in each transaction. Each statement should include a copy of all receipts issued for each transaction.

Legislation should prohibit the use of EFT devices, except by those to whom they are specifically issued.

Additionally, as referred to in recommendations concerning consumer rights and responsibilities, until a positive identification-security system is developed, as long as no proof of identity is required in EFT transactions beyond the possession of a card and the knowledge of some codeword, banks should assume all liability for losses that the banks cannot prove were induced by direct action by a consumer. In this case, a consumer who can be shown to have knowingly permitted another to use his EFT authority will be held responsible for such losses.

Comments

It should be recognized that security is a shared responsibility. Consumers, retailers, banks, and other agencies which may be involved in EFT services have obligations to serve. But it should also be recognized that in their efforts to develop and sell EFT services, the banks bear the primary responsibility for security.

To meet this responsibility, it is suggested that in their attempts to sell the system to retailers, banks not overlook or ignore certain measures that can be taken to enhance security. One is a requirement that store personnel be required to make periodic, random identification checks of EFT card users. Another is to emphasize security in advertisements aimed at the public and retailers.

CHAIRMAN WIDNALL: The next witness is Stephen Mueller, Vice President of the Transamerica Finance Company, speaking on behalf of the National Consumer Finance Association. Would you come to the table to be sworn?
(Witness sworn.)

1 TESTIMONY OF STEPHEN E. MUELLER, VICE PRESIDENT,
2 SYSTEM DEVELOPMENT DIVISION, TRANSAMERICA
3 FINANCIAL CORPORATION, ON BEHALF OF THE NATIONAL
4 CONSUMER FINANCE ASSOCIATION

5 CHAIRMAN ATWATER: Mr. Mueller, would you like to
6 proceed with your ten minutes of testimony, please?

7 MR. MUELLER: Thank you very much, Mr. Atwater.

8 Mr. Chairman and members of the commission, my
9 name is Stephen Mueller, and I am with Transamerica Financial
10 Corporation and also the Chairman of the National Consumer
11 Finance Association's Task Force on EFTS.

12 I do wish to express my appreciation to the
13 commission for the invitation to appear here today and to
14 offer our views and comments on the consumer issues in the
15 development of electronic fund transfer systems.

16 The National Consumer Finance Association was
17 organized in 1916 and is the national trade association of
18 companies engaged in the consumer credit business. There are
19 some 26,000 offices within the industry, and NCFCA represents
20 nearly 850 member companies which finance consumers from over
21 16,000 offices in the United States and Puerto Rico.

22 This financing is done by direct cash installment
23 loans to families or individuals, the purchase of installment
24 sales paper, and the provision of revolving lines of credit
25 by finance companies or industrial banking companies. It

1 should be noted that consumer finance companies are innovators
2 in the field of consumer credit services and were the first
3 institutions to offer various types of direct cash and
4 installment loans.

5 As the second largest holder of consumer credit,
6 finance companies made available \$32.6 billion of consumer
7 credit in 1975. Consumers, in repayment for financing, made
8 some 400 million transfers of funds to finance companies in
9 1975, and this number would be significantly larger if
10 revolving credit operations are taken into account, but they
11 were not.

12 The segmentation among financial institutions is
13 eroding as a result of market forces and regulatory and legis-
14 lative trends. EFTS technology is an additional force, and
15 it will further the similarity of services of the financial
16 institutions. The technological advance as a result of EFTS
17 should be transparent to the underlying institutional
18 structure of the financial system so that the basic competitive
19 forces continue to operate. This is the only way in which
20 consumers can be assured of a range of choice and the benefits
21 of competition.

22 I didn't have any way of knowing Ms. Greenwald
23 would be my supporter. I didn't expect it from the banking
24 society, but she mentioned this a couple of times in her
25 testimony this morning, and I'm very thankful to her for that.

1 Actually, my remarks today will be directed, really,
2 toward the consumer benefit problem and the problems that I
3 see in the consumer finance industry of maximizing the choices
4 and convenience and the potential savings for the consumer in
5 the evolving EFT technology.

6 If all depository and nondepository institutions
7 are permitted access to an overall EFT network, then com-
8 petitive relationships among these institutions would continue
9 to exist and revolve around differentiated services. If,
10 however, nondepository financial institutions are excluded from
11 major EFT networks, those institutions will be placed in an
12 untenable competitive disadvantage vis-a-vis depository
13 financial institutions, and their consumer customers would be
14 disadvantaged. As EFT is merely another kind of payment
15 system, it should not be limited to select groups but shared
16 as all types of payment systems are currently shared.

17 EFT will tie in much more closely the retailers,
18 banks and nondepository institutions. Because of this, any
19 system which confers an unfair price advantage on the com-
20 monly known depository financial institutions regarding
21 access to or use of EFT systems will adversely affect non-
22 depository institutions and their customers.

23 Basic to this lack of consideration of non-
24 depository institutions is the assumption that our exchange
25 mechanism in an EFT mode must retain the same institutional

1 deposit arrangements presently in existence. But there is no
2 reason why a financial institution which is lending to a
3 customer must carry out this funds transfer through an
4 intermediary lending institution. Moreover, an intermediary
5 lending institution would not be required for the payments on
6 the loan to be made in an EFT mode.

7 It can be said, in fact, that for no other reason
8 than historical and technological circumstance in our present
9 payments system that it is based on an institutional frame-
10 work of commercial banks and a check medium of exchange.
11 Changing circumstances, such as evidenced by the emergence
12 of electronic funds transfer technology, may well call for a
13 restructuring of the payments system without dependence on
14 traditional arrangements. In the absence of such changes,
15 the economic benefits to consumers from the new technology
16 will be minimized by the insistence on traditional methods.

17 The development of EFTS is bringing about an
18 evolution in the payments system in which the commercial
19 banking system is no longer the exclusive vendor of the means
20 of money transfer. A growing number of institutions and
21 industries outside of banking are already offering money or
22 near-money deposit arrangements and providing money transfer
23 services.

24 The major contenders for money transfer powers are
25 the nonbank depository institutions -- savings and loan

1 associations, mutual savings banks and credit unions, as well
2 as the nondepository consumer finance companies, credit card
3 companies and retailers. While at present only currency and
4 commercial bank demand deposits provide the base for these
5 funds transfers, third party payments services are being
6 extended to the nonbank financial institutions by technology
7 and legislation. The result is a significant increase in
8 the pool of funds available for transfer, because we will
9 have added to the pool the deposits of thrift institutions.

10 In its most fundamental aspects, EFT would make a
11 "deposit" nothing more than a computerized financial record.
12 In other words, there would be no difference between a
13 "deposit" as a claim against funds left in the keeping of a
14 bank and a life insurance "premium" paid as a "deposit" toward
15 an "insured savings plan" or as a claim against a line of
16 credit. If, however, in an advancing system of EFT, the
17 concept of "deposit" is restricted to cover only the tradi-
18 tional demand, time or savings deposits, the result will be
19 that all nondepository financial institutions will be excluded
20 from the system.

21 Regardless of the definition of the term "deposit,"
22 finance companies must have funds transfer capabilities.
23 Without this capability, those consumers whose only source of
24 borrowed funds is the consumer finance industry would be
25 excluded from the benefits of convenience and cost savings

1 derived from an EFT system, and, further, millions of these
2 consumers will be limited in their choice of a payment device.

3 If the thrift institutions can have immediately
4 transferable funds, then why cannot the nondepository financial
5 institutions, such as consumer finance companies, retailers,
6 credit card companies and insurance companies, enjoy the
7 same privilege?

8 Money balances and credits or debits to them need
9 not be confined to depository institutions. The competitive
10 forces being released by the advancing technology of EFT
11 development should allow for the extension of this capacity
12 to nondepository institutions. The result could be a money
13 payment system supported strictly by fees and completely
14 disassociated from the extension of bank credit -- in short,
15 a pure transfer of funds service. Would not such a service
16 be to the ultimate benefit of the consumer?

17 The overwhelming majority of NCFE member companies
18 are nondepository financial organizations engaged largely in
19 the extension of consumer installment credit of the direct
20 cash loan and/or sales finance types. Each extension of
21 credit requires not only the initial or originating financial
22 transaction but also a recurring sequence of financial
23 transactions as loans are repaid over their term to maturity.
24 As a result, the number of transactions and the attendant
25 data processing required can be voluminous and costly.

1 In order to keep my testimony down, I would just
2 say, in conclusion, I feel it is important that more emphasis
3 be placed on allowing for choice by all consumers.

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

National Commission on Electronic Fund Transfers
Users Committee Public Hearings
"Consumers Issues in EFT"
October 26 and 27, 1976
Washington, D.C.

The documents which follow are submitted for the record
of this hearing by:

Stephen E. Mueller, representing
National Consumer Finance Association

160b

NATIONAL CONSUMER FINANCE ASSOCIATION

1000 SIXTEENTH STREET, N.W., WASHINGTON, D.C. 20036—202 638-1340

STATEMENT ON BEHALF OF

THE NATIONAL CONSUMER FINANCE ASSOCIATION

BY

STEPHEN E. MUELLER

BEFORE THE

NATIONAL COMMISSION ON ELECTRONIC FUND TRANSFERS

ON

CONSUMER ISSUES

IN THE

DEVELOPMENT OF EFTS

OCTOBER 26, 1976

MR. CHAIRMAN AND MEMBERS OF THE COMMISSION, MY NAME IS STEPHEN E. MUELLER. I AM VICE PRESIDENT, SYSTEM DEVELOPMENT DIVISION OF TRANSAMERICA FINANCIAL CORPORATION, AND CHAIRMAN OF THE NATIONAL CONSUMER FINANCE ASSOCIATION'S TASK FORCE ON EFTS.

I WISH TO EXPRESS MY APPRECIATION TO THE COMMISSION FOR THE INVITATION TO APPEAR HERE TODAY TO OFFER OUR VIEWS AND COMMENTS ON CONSUMER ISSUES IN THE DEVELOPMENT OF ELECTRONIC FUND TRANSFER SYSTEMS (EFTS).

THE NATIONAL CONSUMER FINANCE ASSOCIATION, (HEREINAFTER REFERRED TO AS NCFA), ORGANIZED IN 1916, IS THE NATIONAL TRADE ASSOCIATION OF COMPANIES ENGAGED IN THE CONSUMER CREDIT BUSINESS. THERE ARE SOME 26,000 OFFICES WITHIN THE INDUSTRY AND NCFA REPRESENTS NEARLY 850 MEMBER COMPANIES WHICH FINANCE CONSUMERS FROM OVER 16,000 OFFICES IN THE UNITED STATES AND PUERTO RICO. THIS FINANCING IS DONE BY DIRECT CASH INSTALLMENT LOANS TO FAMILIES OR INDIVIDUALS, THE PURCHASE OF INSTALLMENT SALES PAPER, AND THE PROVISION OF REVOLVING LINES OF CREDIT BY FINANCE COMPANIES OR INDUSTRIAL BANKING COMPANIES. IT SHOULD BE NOTED THAT CONSUMER FINANCE COMPANIES ARE INNOVATORS IN THE FIELD OF CONSUMER CREDIT SERVICES, AND WERE THE FIRST INSTITUTIONS TO OFFER VARIOUS TYPES OF DIRECT CASH AND INSTALLMENT LOANS.

AS THE SECOND LARGEST HOLDER OF CONSUMER CREDIT (NEXT TO COMMERCIAL BANKS), FINANCE COMPANIES MADE AVAILABLE \$32.6 BILLION OF CONSUMER CREDIT IN 1975. CONSUMERS IN REPAYMENT FOR FINANCING MADE SOME 400 MILLION TRANSFERS OF FUNDS TO FINANCE COMPANIES IN 1975 (TABLE 1), AND THIS NUMBER WOULD BE SIGNIFICANTLY LARGER IF REVOLVING CREDIT OPERATIONS ARE TAKEN INTO ACCOUNT.

THE SEGMENTATION AMONG FINANCIAL INSTITUTIONS IS ERODING AS A RESULT OF MARKET FORCES AND REGULATORY AND LEGISLATIVE TRENDS. EFTS TECHNOLOGY IS AN ADDITIONAL

- 2 -

FORCE AND IT WILL FURTHER THE SIMILARITY OF SERVICES OF THE FINANCIAL INSTITUTIONS. THE TECHNOLOGICAL ADVANCE AS A RESULT OF EFTS SHOULD BE TRANSPARENT TO THE UNDERLYING INSTITUTIONAL STRUCTURE OF THE FINANCIAL SYSTEM SO THAT THE BASIC COMPETITIVE FORCES CONTINUE TO OPERATE. THIS IS THE ONLY WAY IN WHICH CONSUMERS CAN BE ASSURED OF A RANGE OF CHOICE AND THE BENEFITS OF COMPETITION.

MY REMARKS WILL BE DIRECTED TOWARD A PARTICULAR ASPECT OF THE PROBLEM, THAT IS, ASSURANCE THAT ALL CONSUMERS, WHETHER DEPOSITORS IN FINANCIAL INSTITUTIONS OR NOT, MAY HAVE THE POTENTIAL FOR BENEFITING FROM AN INCREASE IN TIME AND LOCATION CONVENIENCE RESULTING FROM AN ELECTRONIC FUNDS SYSTEM. TO ASSURE THE MAXIMIZATION OF CHOICES, CONVENIENCE AND POTENTIAL COST BENEFITS, OF COURSE, REQUIRES ACCESS TO THE SYSTEM BY ALL INSTITUTIONS PROVIDING FINANCIAL SERVICES TO CONSUMERS.

IF ALL DEPOSITORY AND NON-DEPOSITORY INSTITUTIONS ARE PERMITTED ACCESS TO AN OVERALL EFT NETWORK, THEN COMPETITIVE RELATIONSHIPS AMONG THESE INSTITUTIONS WOULD CONTINUE TO EXIST AND REVOLVE AROUND DIFFERENTIATED SERVICES. IF, HOWEVER, NON-DEPOSITORY FINANCIAL INSTITUTIONS ARE EXCLUDED FROM MAJOR EFT NETWORKS, THOSE INSTITUTIONS WILL BE PLACED AT UNTENABLE COMPETITIVE DISADVANTAGE VIS-A-VIS DEPOSITORY FINANCIAL INSTITUTIONS, AND THEIR CONSUMER CUSTOMERS WOULD ALSO BE DISADVANTAGED. AS EFT IS MERELY ANOTHER KIND OF PAYMENT SYSTEM, IT SHOULD NOT BE LIMITED TO SELECT GROUPS, BUT SHARED AS THE OTHER TYPES OF PAYMENT SYSTEMS ARE SHARED.

EFT WILL TIE IN MUCH MORE CLOSELY THE RETAILERS, BANKS AND NON-DEPOSITORY INSTITUTIONS. BECAUSE OF THIS, ANY SYSTEM WHICH CONFERS AN UNFAIR PRICE ADVANTAGE ON THE COMMONLY KNOWN DEPOSITORY FINANCIAL INSTITUTIONS REGARDING ACCESS TO OR USE OF EFT SYSTEMS WILL ADVERSELY AFFECT NON-DEPOSITORY INSTITUTIONS AND THEIR CUSTOMERS FROM A COMPETITIVE STANDPOINT.

BASIC TO THIS LACK OF CONSIDERATION OF NON-DEPOSITORY INSTITUTIONS IS THE ASSUMPTION, THAT OUR EXCHANGE MECHANISM IN AN EFT MODE MUST RETAIN THE SAME INSTITUTIONAL DEPOSIT ARRANGEMENTS PRESENTLY IN EXISTENCE. BUT THERE IS NO REASON WHY A FINANCIAL INSTITUTION WHICH IS LENDING TO A CONSUMER (OR A BUSINESS) MUST CARRY OUT THIS FUNDS TRANSFER THROUGH AN INTERMEDIARY LENDING INSTITUTION. MOREOVER, AN INTERMEDIARY LENDING INSTITUTION WOULD NOT BE REQUIRED FOR THE PAYMENTS ON THE LOAN TO BE MADE IN EFT MODE.

IT CAN BE SAID, IN FACT, THAT FOR NO REASON OTHER THAN HISTORICAL AND TECHNOLOGICAL CIRCUMSTANCE IS OUR PRESENT PAYMENTS SYSTEM ONE FOR THE MOST PART BASED ON AN INSTITUTIONAL FRAMEWORK OF COMMERCIAL BANKS AND A CHECK MEDIUM OF EXCHANGE. CHANGING CIRCUMSTANCES, SUCH AS EVIDENCED BY THE EMERGENCE OF ELECTRONIC FUNDS TRANSFER TECHNOLOGY, MAY WELL CALL FOR A RESTRUCTURING OF THE PAYMENTS SYSTEM WITHOUT DEPENDENCE ON TRADITIONAL ARRANGEMENTS. IN THE ABSENCE OF SUCH CHANGES, THE ECONOMIC BENEFITS TO CONSUMERS FROM THE NEW TECHNOLOGY WILL BE MINIMIZED BY THE INSISTENCE ON TRADITIONAL METHODS.

THE DEVELOPMENT OF EFTS IS BRINGING ABOUT AN EVOLUTION IN THE PAYMENTS SYSTEM IN WHICH THE COMMERCIAL BANKING SYSTEM IS NO LONGER THE EXCLUSIVE VENDOR OF THE MEANS OF MONEY TRANSFER. A GROWING NUMBER OF INSTITUTIONS AND INDUSTRIES OUTSIDE OF BANKING ARE ALREADY OFFERING MONEY OR NEAR-MONEY DEPOSIT ARRANGEMENTS AND PROVIDING MONEY TRANSFER SERVICES.

THE MAJOR CONTENDERS FOR MONEY TRANSFER POWERS ARE THE NON-BANK DEPOSITORY INSTITUTIONS - SAVINGS AND LOAN ASSOCIATIONS, MUTUAL SAVINGS BANKS AND CREDIT UNIONS AS WELL AS THE NON-DEPOSITORY CONSUMER FINANCE COMPANIES, CREDIT CARD COMPANIES AND RETAILERS. WHILE AT PRESENT, ONLY CURRENCY AND COMMERCIAL BANK DEMAND DEPOSITS PROVIDE THE BASE FOR ALL FUNDS TRANSFER, THIRD PARTY PAYMENTS SERVICES ARE BEING EXTENDED TO THE NONBANK FINANCIAL INSTITUTIONS BY TECHNOLOGY AND LEGISLATION. THE RESULT IS A SIGNIFICANT INCREASE IN THE POOL OF FUNDS

- 4 -

AVAILABLE FOR TRANSFER BECAUSE WE WILL HAVE ADDED TO THE POOL THE DEPOSITS OF THRIFT INSTITUTIONS.

IN ITS MOST FUNDAMENTAL ASPECTS EFT WOULD MAKE A "DEPOSIT" NOTHING MORE THAN A COMPUTERIZED FINANCIAL RECORD. IN OTHER WORDS, THERE WOULD BE NO DIFFERENCE BETWEEN A "DEPOSIT" AS A CLAIM AGAINST FUNDS LEFT IN THE KEEPING OF A BANK, AND A LIFE INSURANCE "PREMIUM" PAID AS A "DEPOSIT" TOWARDS AN "INSURED SAVINGS PLAN", OR A CLAIM AGAINST A LINE OF CREDIT. IF, HOWEVER, IN AN ADVANCING SYSTEM OF EFT THE CONCEPT OF "DEPOSIT" IS RESTRICTED TO COVER ONLY THE TRADITIONAL DEMAND, TIME OR SAVINGS DEPOSITS, THE RESULT WILL BE THAT ALL NON-DEPOSITORY FINANCIAL INSTITUTIONS WILL BE EXCLUDED FROM THE SYSTEM.

REGARDLESS OF THE DEFINITION OF THE TERM DEPOSIT, FINANCE COMPANIES MUST HAVE FUNDS TRANSFER CAPABILITIES. WITHOUT THIS CAPABILITY THOSE CONSUMERS WHOSE ONLY SOURCE OF BORROWED FUNDS IS THE CONSUMER FINANCE INDUSTRY WOULD BE EXCLUDED FROM THE BENEFITS OF CONVENIENCE AND COST SAVINGS DERIVED FROM AN EFT SYSTEM, AND FURTHER, MILLIONS OF OTHER CONSUMERS WILL BE LIMITED IN THEIR CHOICE OF A PAYMENT DEVICE."

IF THE THRIFT INSTITUTIONS CAN HAVE IMMEDIATELY TRANSFERABLE FUNDS, THEN WHY CANNOT THE NON-DEPOSITORY FINANCIAL INSTITUTIONS, SUCH AS CONSUMER FINANCE COMPANIES, RETAILERS, CREDIT CARD COMPANIES AND INSURANCE COMPANIES, ENJOY THE SAME PRIVILEGE? MONEY BALANCES AND CREDITS OR DEBITS TO THEM NEED NOT BE CONFINED TO DEPOSITORY INSTITUTIONS. THE COMPETITIVE FORCES BEING RELEASED BY THE ADVANCING TECHNOLOGY OF EFT DEVELOPMENT SHOULD ALLOW FOR THE EXTENSION OF THIS CAPACITY TO NON-DEPOSITORY INSTITUTIONS. THE RESULT COULD BE A MONEY PAYMENT SYSTEM SUPPORTED BY FEES AND COMPLETELY DISASSOCIATED FROM THE EXTENSION OF BANK CREDIT - IN SHORT, A PURE TRANSFER OF FUNDS SERVICE. WOULD NOT SUCH A SYSTEM BE TO THE ULTIMATE BENEFIT OF THE CONSUMER?

THE OVERWHELMING MAJORITY OF NCUA MEMBER COMPANIES ARE NON-DEPOSITORY

- 5 -

FINANCIAL ORGANIZATIONS ENGAGED LARGELY IN THE EXTENSION OF CONSUMER INSTALLMENT CREDIT OF THE DIRECT CASH LOAN AND/OR SALES FINANCE TYPES. EACH EXTENSION OF CREDIT REQUIRES NOT ONLY THE INITIAL OR ORIGINATING FINANCIAL TRANSACTION BUT ALSO A RECURRING SEQUENCE OF FINANCIAL TRANSACTIONS AS LOANS ARE REPAYED OVER THEIR TERM TO MATURITY. AS A RESULT THE NUMBER OF TRANSACTIONS AND THE ATTENDANT DATA PROCESSING REQUIRED CAN BE VOLUMINOUS AND COSTLY.

THE INTEREST OF THE CONSUMER FINANCE INDUSTRY IN EFTS CENTERS ON THE FACT THAT CONSUMERS MADE NEARLY 400 MILLION TRANSFERS OF FUNDS TO FINANCE COMPANIES IN 1975. THESE CONSISTED OF INSTALLMENT PAYMENTS ON PERSONAL LOANS, AUTOMOBILE LOANS, MOBILE HOME LOANS AND OTHER CONSUMER PURCHASES.

PERSONAL LOANS

FINANCE COMPANIES ARE THE LARGEST SINGLE HOLDER OF PERSONAL LOANS REPAYABLE IN INSTALLMENTS. AT THE END OF 1975 FINANCE COMPANIES HELD \$17.7 BILLION IN PERSONAL LOANS AND COMMERCIAL BANKS HELD \$14.0 BILLION.

ACCORDING TO THE LATEST AVAILABLE INFORMATION FROM SURVEYS BY THE NATIONAL CONSUMER FINANCE ASSOCIATION THE AVERAGE SIZE PERSONAL LOAN MADE IN 1975 WAS \$1,354 AND 12.8 MILLION LOANS WERE MADE. APPROXIMATELY 41% OF THESE LOANS WERE MADE TO BORROWERS WHOSE INCOME WAS LESS THAN \$9,000. ABOUT 22% WERE MADE TO THOSE WITH INCOME OF \$9,000 TO \$11,999 AND 37% TO THOSE WHOSE INCOME WAS \$12,000 AND OVER.

EACH LOAN OUTSTANDING IS SUBJECT TO A PAYMENT EACH MONTH. AN ESTIMATED AVERAGE OF 14.6 MILLION LOANS WERE OUTSTANDING IN 1975, SO THE NUMBER OF FUNDS TRANSFERS FROM CONSUMERS TO FINANCE COMPANIES FOR THE MONTHLY REPAYMENT OF PERSONAL LOANS WOULD APPROXIMATE 175 MILLION DURING THE COURSE OF A YEAR. BY FAR THE MAJORITY OF THESE PAYMENTS WERE MADE BY CHECKS PAYABLE ON BANKS IN THE LOCALITY OF THE CONSUMER.

AUTOMOBILE FINANCING

APPROXIMATELY 2.5 MILLION TRANSFERS OF FUNDS WERE MADE BY FINANCE COMPANIES TO AUTOMOBILE DEALERS FOR FINANCING INDIVIDUAL CONSUMER PURCHASES NOT INCLUDING LEASES, OR FLEET OR COMMERCIAL VEHICLES FOR LARGE AND SMALL BUSINESSES.

TO ESTIMATE THE NUMBER OF FUND TRANSFERS FROM CONSUMERS TO FINANCE COMPANIES TO REPAY AUTOMOBILE INSTALLMENT CONTRACTS, THE LATEST DATA FROM NCFA SUGGEST THAT FINANCE COMPANY CONTRACTS OUTSTANDING IN 1975 AVERAGED \$2,702, AND THE NUMBER OF CONTRACTS AVERAGED 4.1 MILLION. ASSUMING A CONSUMER PAYMENT EACH MONTH, THE NUMBER OF TRANSFERS OF FUNDS FROM CONSUMERS TO FINANCE COMPANIES IN REPAYMENT OF AUTO FINANCING WOULD BE 48.6 MILLION IN 1975.

MOBILE HOME

MOBILE HOME FINANCING IN 1975 BY FINANCE COMPANIES TOTALED ABOUT \$0.8 BILLION. AT AN ESTIMATED \$7,938 PER ACCOUNT, OVER 100,000 MOBILE HOMES WERE FINANCED. WITH \$3.5 BILLION IN OUTSTANDINGS AT YEAR-END 1975 AND AN ESTIMATED \$6,701 PER CONTRACT SOME 500,000 PAYMENTS PER MONTH WOULD RESULT IN APPROXIMATELY 6.0 MILLION FUND TRANSFERS FROM CONSUMERS IN 1975.

OTHER CONSUMER FINANCING

THE CONSUMER FINANCE COMPANIES ALSO FINANCE PURCHASES AT RETAIL STORES. AMONG THE ITEMS INCLUDED IN THIS TYPE OF FINANCING ARE: APPLIANCES, TELEVISION AND STEREO SETS, RADIOS, FURNITURE, MUSICAL INSTRUMENTS, SEWING MACHINES AND ACCESSORIES, AND OTHER HOUSEHOLD DURABLES. TENS OF THOUSANDS OF DEALERS THROUGHOUT THE COUNTRY HAVE THEIR CUSTOMERS SERVED BY THIS TYPE OF FINANCING BY FINANCE COMPANIES.

IN RECENT YEARS, A NUMBER OF FINANCE COMPANIES HAVE OFFERED REVOLVING CHARGE ACCOUNT CREDIT, WHEREIN ALL FUNCTIONS OF A CREDIT DEPARTMENT ARE PROVIDED FOR A RETAILER INCLUDING CREDIT INVESTIGATION, ISSUANCE OF CUSTOMER CREDIT CARDS IN THE NAME OF THE RETAILER, BILLING AND COLLECTION. SERVICES FREQUENTLY PROVIDED ARE

THE FINANCING OF PURCHASES OF PERSONAL GOODS AND SUPPLIES, AUTOMOBILE RENTALS AND APPLIANCE SALES AND SERVICE. THESE ACCOUNTS OF FINANCE COMPANIES PROBABLY ACCOUNT FOR WELL OVER 10,000,000 TRANSACTIONS PER YEAR. ESTIMATES SHOWN IN TABLE 1 PROBABLY DO NOT COMPLETELY REFLECT THESE TYPES OF FUND TRANSFERS BETWEEN FINANCE COMPANIES AND CONSUMERS.

CHOICES OPEN TO ALL CONSUMERS

IN CONCLUSION, IT IS IMPORTANT THAT MORE EMPHASIS THAN IN THE PAST BE PLACED ON ALLOWING FOR CHOICE BY ALL CONSUMERS AS TO THEIR FORM OF PAYMENT SO AS TO AFFORD THEM THE OPPORTUNITIES FOR GREATER CONVENIENCE AND COST BENEFITS. A RECOMMENDATION WHICH WOULD DENY A CONSUMER ENTRY TO AN EFT SYSTEM SOLELY BECAUSE HE WAS NOT A SAVER OR DEPOSITOR IN A CHARTERED FINANCIAL INSTITUTION IS DETRIMENTAL TO HIS INTERESTS. TO ACHIEVE THIS EQUALITY OF PARTICIPATION BY CONSUMERS REQUIRES EQUAL ACCESS BY ALL INSTITUTIONS TO AN OVERALL ELECTRONIC FUNDS TRANSFER SYSTEM. IT IS IMPERATIVE THAT AT LEAST THE CURRENT LEVELS OF COMPETITION SHOULD BE MAINTAINED TO INSURE THE RANGE OF CHOICES AVAILABLE TO THE CONSUMERS AS TO PAYMENT MECHANISM AND CREDIT SUPPLIERS.

TABLE 1

Estimated Number of Consumer Credit Transfers
Finance Companies, 1975

	Personal Loans	Automobile Credit		Mobile Homes	All Other	Total
		New Cars	Used Cars			
1. Installment Credit Amount (In millions of dollars)*						
a. Outstanding end 1974	16,961	10,618		3,524	5,105	36,208
b. Extensions 1975	17,333	9,598		771	4,880	32,582
c. Liquidations 1975	16,616	8,777		844	5,862	32,099
d. Outstanding end 1975	17,681	11,439		3,451	4,124	36,695
2. Contracts or Loans Made in 1975**						
a. Average Size	\$1,354	\$4,959	\$2,651	\$7,938	\$471	--
b. Number (In Millions)	12.8	1.4	1.1	.01	10.4	25.8
3. Repayments on Loans or Contracts 1975**						
a. Average Size Outstanding Year-end 1974	\$1,125	\$2,573		\$6,701	\$388	--
b. Average Size Outstanding Year-end 1975	\$1,245	\$2,831		\$7,337	\$278	--
c. Number Outstanding Year-end 1974 (millions)	15.1	4.1		0.5	13.2	32.9
d. Number Outstanding Year-end 1975 (millions)	14.2	4.0		0.5	14.8	33.5
e. Number of Repayments During 1975 (12 times the mean of number outstanding year-end 1974 and year-end 1975 in millions)	175.2	48.6		6.0	168.0	397.8

*Estimates based on revised data released by the Federal Reserve in August 1976.

**Estimates based on Federal Reserve and National Consumer Finance Association data.

1605

1 CHAIRMAN ATWATER: Thank you very much, Mr. Mueller.
2 Questions by the commissioners?

3 CHAIRMAN WIDNALL: Mr. Mueller, you said you were
4 skipping over part of your testimony.

5 Do you want to include that in the record?

6 MR. MUELLER: Yes.

7 CHAIRMAN WIDNALL: So ordered.

8 MR. MITCHELL: These numbers in your testimony which
9 have to do with structure --
10 do they include the liability structure of the industry?

11 MR. MUELLER: No, they do not, sir.

12 MR. MITCHELL: Well, what is the amount of liquidity
13 balance that could be drawn on a bank
14 deposit or savings account in a thrift?

15 MR. MUELLER: I don't quite understand the question.
16 What is the amount of credit extendable to the
17 consumers?

18 MR. MITCHELL: No. I am talking about the liability
19 side of your balance sheet, of the industry's balance sheet.

20 What are those liabilities, and what proportion
21 of them are instant liquidity that you could withdraw on a
22 moment's notice?

23 MR. MUELLER: I don't have those figures available
24 at this time.

25 MR. MITCHELL: Well, how large is it? Or are all

1 of your liabilities certificates of one sort or another
2 from date of maturity?

3 MR. MUELLER: No, sir. Many of them are bank
4 credit lines which do not have dates of maturity. But many
5 of them are long-term dates which do have dates of maturity,
6 and others are short-term commercial paper.

7 MR. MITCHELL: If you
8 say that finance companies should have money transfer powers,
9 that means they have accounts that can be drawn on at any
10 time by anybody with the proper authorization, and those are
11 instant liquidity accounts. I'm just raising the question,
12 do you have such accounts?

13 MR. MUELLER: Yes, sir, we do.

14 MR. MITCHELL: How large are they?

15 MR. MUELLER: I would say, on average, that

16
17 at least 70 percent of the assets are liquid assets.

18 CHAIRMAN ATWATER: I wonder if, perhaps, Governor
19 Mitchell, we might ask for that in a formal way.

20 If you could supply that to the commission as a
21 part of your testimony that you have just given --

22 MR. MUELLER: I would be glad to.

23

24

25

1 MR. MITCHELL: It is more or less a leading
2 question to ask whether or not the consumer finance industry
3 is equipped to offer money transfer services.

4 MR. MUELLER: Well, I believe they are equipped,
5 sir. I cannot speak for the entire industry. I can speak
6 for my own company. But we have maturities on average that
7 mature over about a 15- to 16-month period. But the actual
8 cash transfer, the turnover is 100 percent in eight to nine
9 months, and if that is not liquid, I don't know what is.

10 MR. MITCHELL: It is a fact that, when
11 someone draws on an account, you have to be able to make that
12 payment immediately, and I don't think you have that type of
13 liability, do you?

14 MR. MUELLER: Well, the consumer finance industry
15 does not now have a large extension of open credit lines,
16 mainly because most of the states restrict open credit lending
17 for the consumer finance industry. But we are willing to
18 support open credit lines with liquid assets.

19 MR. MITCHELL: Are you suggesting a role
20 going through the commercial banking system or a role inde-
21 pendent of the commercial banking system?

22 MR. MUELLER: I'm suggesting a role independent of
23 the commercial banking system.

24 MR. MITCHELL: Then I think the character of your
25 liabilities determines whether or not you can still operate,

1 and they must be liquid liabilities.

2 MR. MUELLER: I would agree, sir.

3 CHAIRMAN ATWATER: Ms. Koplow.

4 MS. KOPLOW: I think part of what I wanted to ask
5 was asked by Governor Mitchell. But I think, if I understood
6 you correctly, you wanted to have the power to make loans
7 and accept deposits, and have the power of
8 demand deposit accounts.

9 This is what you are asking here for?

10 MR. MUELLER: No, ma'am. We're not asking for
11 deposit accounts at all. We are asking that the industry
12 that we are in be allowed access for EFT for only the areas
13 they are currently involved, and that is in the extension of
14 credit to the consuming public. We do not ask for depository-
15 taking capabilities.

16 That would have to be handled on an individual
17 company basis. And if they wanted to deal through a com-
18 mercial bank or through a savings and loan for that type of
19 institutional depository account, then, that is independent
20 and has nothing to do with the request by the industry to
21 service their credit accounts through EFT.

22 MS. KOPLOW: In order to do that, then your
23 customer must have a savings account, whether there is a
24 demand deposit, or a demand deposit in a commercial bank,
25 to effect this transaction. Is that correct?

1 MR. MUELLER: No, he would not necessarily have
2 to have a savings or deposit account, because, in my request
3 for the access to the EFT systems, or so that he can access
4 his credit line with the consumer finance companies to receive
5 the cash at some location.

6 MS. KOPLON: And how does he pay it back?

7 MR. MUELLER: Through the normal routine of monthly
8 payments. And, again, he may use an EFT system by using his
9 bank to pre-authorize or to authorize individually payment
10 out of his checking or savings account to the finance company.
11 That could be a third party transaction. But the acquisition
12 of credit from the finance company would be on a direct basis.

13

14

15

16

17

18

19

20

21

22

23

24

25

1 MS. KOPLOW: I think I see what you are trying to do.
2 I am not quite sure that I see it all clearly, but I will have
3 a subsequent question for you, probably in the mail.

4 CHAIRMAN ATWATER: Mr. Thorndike.

5 MR. THORNDIKE: Just to explore this
6 a little further, would this, for example, envisage that the
7 person could make a payment to his finance company from the
8 terminal at the supermarket where he goes with his paycheck to
9 buy his groceries?

10 MR. MUELLER: Yes, it does.

11 MR. THORNDIKE: That does not necessarily involve
12 the commercial banking operation?

13 MR. MUELLER: That is correct, sir.

14 Yes, it would. It would allow him at the same
15 instance to perhaps purchase automobile tires if he does not
16 have a major credit card from an oil company. He could access
17 through the system his credit line with the finance company and
18 get immediate payment from the finance company on his plan of
19 credit to the vendor or to the retailer.

20 MR. THORNDIKE: Are any arrangements of this sort
21 now in existence and in operation on an experimental or trial
22 mode?

23 MR. MUELLER: They are not, sir.

24 We do have the -- UCCC states do allow revolving
25 lines of credit, and there are institutions that do have

1 revolving lines of credit in those states. But at this time,
2 all those transactions are being made by paper through checks
3 or drafts.

4 CHAIRMAN ATWATER: Mr. Worley.

5 MR. WORLEY: Just to follow that discussion a little
6 further so I understand it, if a customer were to buy a
7 TV set in one of our stores under an EFT environment and wished
8 to finance it through one of your firms,

9 there would be some communication
10 between, perhaps, our POS terminal and your institution. But

11 how would the retailer receive
12 credit for that transaction? How would he get paid by your
13 company? Wouldn't the settlement have to be at some commercial
14 bank? That is where we would want it.

15 MR. MUELLER: Yes. The settlement between a retailer
16 and the consumer finance company would be through a bank.

17 MR. WORLEY: So this would necessitate the consumer
18 finance company having access to funds located in a commercial
19 bank where they could transfer those funds from their account
20 into the retailer's account. I think Governor Mitchell's
21 point, that there would have to be settlement made
22 within the framework of the commercial banks, is a
23 valid comment.

24 MR. MITCHELL: That you permit your your
25 customer to draw on your account at a commercial bank?

1 MR. MUELLER: That's right.

2 CHAIRMAN ATWATER: Mr. Mueller,

3 one of the issues you are proposing here is that
4 you are concerned about essentially unfair competition in this
5 case of the finance companies to the credit cards, be they
6 private or national credit card systems.

7 MR. MUELLER: Yes, sir, we are. Also, in the banks,
8 the consumer finance industry, and in part of the text loans to a
9 great deal of consumers who are in the lower-income ranges, and
10 in order to continue service to those particular customers, we
11 feel that the industry has a viable credit place in our
12 economic society. And if they are eliminated from EFT
13 technology, those customers will lose, because we can't afford
14 to continue to operate without EFT activities.

15 CHAIRMAN ATWATER: If I may ask one more question
16 before Mr. Tangney's question: What prevents you from doing
17 that today?

18 MR. MUELLER: What prevents us from doing it today?
19 Nothing really prevents us from doing it today, but all of the
20 current state legislation and all of the consideration for
21 federal legislation has been with depository institutions, and
22 almost all of the state legislation has eliminated or
23 restricted its EFT activities to deposit-taking institutions.

24 CHAIRMAN ATWATER: I see.

25 Mr. Tangney?

1 MR. TANGNEY: You mentioned in your testimony -- and
2 I'm going back to Governor Mitchell's question -- a debit or
3 credit balance.

4 Now, what would be a debit balance?

5 MR. MUELLER: A debit balance would be his line of
6 credit with us. He owes us, let's say, \$500, and in his case
7 wants to go out and buy an additional TV and finance it on his
8 account. He can increase that balance -- his balance with us
9 from a \$500 loan to, say, a \$1000 loan.

10 MR. TANGNEY: Well, what is a credit balance then?

11 MR. MUELLER: We don't have credit balances with us.

12 MR. TANGNEY: I thought you mentioned you wanted
13 both debit and credit balances.

14 MR. MUELLER: No, we don't want them.

15 In other words, the system is going to be handling
16 both. All we want is to be included in the debit balances.

17 MR. TANGNEY: Thank you.

18 CHAIRMAN ATWATER: Are there any other questions by
19 the Commission?

20 MR. WALTER ANDERSON: Could you outline the fee
21 structure you propose?

22 MR. MUELLER: The fee structure I propose would
23 probably be per transaction. There are already some established
24 per-transaction fee structures in existence, particularly for
25 the payment of utility bills, mortgages, et cetera. They are

1 being offered for 10 cents per transaction, which is better
2 than paying 13 cents on a stamp.

3 CHAIRMAN ATWATER: One of the issues you touched on
4 in your testimony I would like to ask just one more question
5 about.

6 We have been concerned, too, about how EFT affects
7 lower-income consumers. I think I heard a piece of your
8 testimony suggesting that the use of the EFT by the finance
9 companies would have something to do with that problem.

10 Is that a fair statement, and would you elaborate
11 just a bit on it?

12 MR. MUELLER: Yes, I would.

13 The consumer finance industry is in some of the
14 figures that I did pass out because there were figures, but the
15 41 percent of the loans that were made by consumer finance
16 companies since '75 were made to people whose income was less
17 than \$9000 per year. An additional 22 percent was between
18 \$9000 and \$12,000, and 37 percent was over \$12,000 per year.

19 And it is this population that is serviced, really,
20 by the consumer finance companies and, in my estimation, is
21 the one who will benefit most by the economies of EFT.

22 One of the reasons that a great number of our
23 current customers do not maintain bank or savings accounts is
24 because they do not have a great surplus of cash. They don't
25 have enough to start a checking or savings account. But

1 if through EFT they are allowed to have their paychecks
2 deposited automatically to an account, and if that account turns
3 out to be a no-fee check or savings account, perhaps even an
4 interest-bearing account, then these customers will be allowed
5 the advantages of EFT. Yet if their credit supplier is denied
6 the advantage of working with EFT, then they would have to go
7 through some other avenue.

8 CHAIRMAN ATWATER: Thank you very much.

9 Mr. Benton has a question.

10 MR. BENTON: I would just like to follow up that
11 point for one more moment.

12 Is it not also the case that some scenarios are
13 building on what we have heard this morning, that EFT will
14 substantially expand information? One of the positive aspects
15 of that is that a number of people who today are
16 denied credit by the banks may not be denied credit tomorrow
17 because of more accurate information regarding their credit-
18 worthiness, although they don't make it through traditional

19 scoring techniques and things of that sort. Is it not
20 possible that one of the side effects of EFTS could be a
21 substantial skimming off the top of some of your better
22 customers and, therefore, a further declination of your profit
23 picture, thus having an adverse affect on your whole industry?

24 MR. MUELLER: It certainly could, sir.

25 CHAIRMAN ATWATER: Are there any other questions or
observations?

(No response.)

CHAIRMAN ATWATER: Thank you very much for your
testimony, Mr. Mueller.

MR. MUELLER: Thank you.

1
2
3
4
5
6 CHAIRMAN WIDNALL: The next witness is Ana Aldama
7 speaking on behalf of the National Consumer Information Center
8 of Washington, D.C.

9 Would you come to the table.

10 (Witness sworn.)

11 CHAIRMAN ATWATER: We would ask you, if you would,
12 Ms. Aldama, to proceed with your testimony, and we will have
13 questions for you afterwards.

14 TESTIMONY OF ANA ALDAMA, PROGRAM PLANNER,
15 NATIONAL CONSUMER INFORMATION CENTER,
16 WASHINGTON, D.C.

17 MS. ALDAMA: Thank you, Mr. Chairman and members of
18 the committee.

19 My name is Ana Aldama. I am the Program Planner
20 at the National Consumer Information Center here in Washington,
21 D.C. It is a pleasure to be here to testify on behalf of the
22 lower and fixed-income consumers across the country.

23 First, I would like to give you a brief background
24 on the National Consumer Information Center and what we are
25 all about.

1 The National Consumer Information Center is a non-
2 profit organization which seeks to protect and advance the
3 interest of low-, moderate- and fixed-income consumers. NCIC
4 was founded in 1968 by a group of Howard University law students.
5 It was formed to help poor people in their plight against
6 poverty and lack of information and education on consumer
7 issues. Thus, one of our main objectives is to educate the
8 low-income consumer and disseminate information on consumer
9 issues that affect each of us but are sadly neglected in low,
10 moderate and fixed areas.

11 We would like to address the issues of consumer
12 choice, security and privacy, and the impact of electronic
13 fund transfer systems on those particular areas in relation to
14 the low-income consumer or user.

15 Electronic fund transfer systems have been implemented
16 on a broad scale, yet they are not apparent to a great majority
17 of consumers. The average consumer is just begining to become
18 aware of the spread of EFTS outside as well as inside the
19 financial service institutions.

20 The consumer's reaction is still uncertain.
21 Consumers have not been searching for new approaches in making
22 payments because the present checking and cash systems seem to
23 be satisfactory. Consumers have not been given an opportunity
24 to make a choice on the relatively new EFTS because the system
25 is already being introduced and implemented to a certain

1 degree.

2 Low-income consumer groups are found among certain
3 sectors of the population including minority groups, such as
4 blacks, Spanish-Americans, Indians, Orientals, and senior
5 citizens. Many of these consumers are not aware of the elec-
6 tronic fund transfer systems and as a consequence have little
7 or no idea how they will be affected by the widespread
8 implementation of the system. Many low-income consumers
9 primarily use cash as a method of making payments. Thus, a
10 widespread electronic fund system may deprive them of means of
11 making financial transactions.

12 Low-income consumers, in more instances than none,
13 do not have bank accounts. Low-income consumers have difficulty
14 obtaining credit, credit cards or charge accounts, which are
15 easily accessible to middle-income consumers. The most common
16 system of monetary transaction low-income consumers know and
17 are able to use is that of cash transactions. Among the
18 low-income population there are the unemployed, who quite
19 naturally, are excluded from those monetary transactions which
20 are everyday procedures for the average middle-income and/or
21 working individuals.

22 For the low-income consumer and the fixed-income
23 consumer, such as the senior citizens who have checking accounts,
24 the loss of float which the present checking system allows
25 would present a major problem. According to surveys performed

1 for different agencies throughout the country, approximately 45
2 percent of the checks written during one month were written on
3 accounts that had insufficient funds at the time the checks
4 were written. Funds were later made available before the checks
5 were cleared. The prospect of an electronic system that would
6 enable immediate direct debiting of the consumer's account at
7 the point of sale would be a strong source of apprehension for
8 the majority of the low- and fixed-income population as it would
9 mean loss of this float. Undoubtedly, the entire low-income
10 population, who make transactions through the present checking
11 system, would find its financial situation in a turmoil. Thus,
12 a plan may have to be developed to compensate for this loss of
13 float.

14 Security would pose other problems. For the few
15 low-income individuals who may have access to EFTS cards, what
16 would the liability provisions be if the card was lost or
17 stolen? With EFTS cards, if an unauthorized individual used
18 another customer's card in the system, in a single trans-
19 action an individual's life savings could be lost. This would
20 cause a serious problem for the average consumer. For the
21 low-income consumer, it would be a tragedy.

22 The privacy issue is raised. If the EFTS is fully
23 implemented, personal data would be collected on each person
24 who uses the system. This information can be compiled on a
25 ready-to-use form giving an entire spending history of the

1 person, thus allowing complete control over a person's private
2 life. Some individuals among low-income consumers have a
3 bad credit record. According to a recent Supreme Court decision
4 in Syracuse, New York, secrecy records in a given bank become
5 property of the bank so they can do as they wish with those
6 records. Is the electronic fund transfer system going to open
7 Pandora's box, which will affect credit and employment availa-
8 bility for the low-income consumer/user?

9 If EFTS were to be implemented on a full-scale basis,
10 including banking, insurance companies, food chains, transporta-
11 tion systems, retail stores, et cetera, what choice would the
12 low-income consumers have? None. Then the question is: How
13 is this individual going to handle his monetary transactions?
14 What will the alternatives be, or are there any alternatives?

15 Some possible answers to these questions could be
16 determined by carefully studying the low- and fixed-income
17 consumer/user and the serious implications that EFTS would pose
18 upon them. Also, consideration should be given to providing
19 an educational program for low-, moderate- and fixed-income
20 consumers concerning issues relative to EFTS which would
21 affect them.

22 In conclusion, NCIC is gratified that this
23 committee has directed its attention to this area of great
24 concern for the low- and fixed-income consumers. We are
25 hopeful that our remarks today will be of assistance to you in

1 your consideration of this important issue.

2 Thank you.

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

National Commission on Electronic Fund Transfers
Users Committee Public Hearings
"Consumers Issues in EFT"
October 26 and 27, 1976
Washington, D.C.

The documents which follow are submitted for the record
of this hearing by:

Ana Aldama of
National Consumer Information Center

NATIONAL CONSUMER INFORMATION CENTER

3005 GEORGIA AVENUE, N.W.

WASHINGTON, D.C. 20001

(202) 723-8090

STATEMENT

OF

ANA ALDAMA

PROGRAM PLANNER

NATIONAL CONSUMER INFORMATION CENTER

Before the Users Committee
of the

National Commission on Electronic Fund Transfers

October 26, 1976



EXECUTIVE OFFICERS EXECUTIVE STAFF

JOSEPH A. SMITH
Executive Director

FRANK A. PORTER
Deputy Director for
National Programs

MARIETTA MOORE
Deputy Director,
For Congressional Relations

JOHN P. SYMONS, JR.
Deputy Director for Business
Affairs

JOANN KRAMER
Deputy Director for
Public Relations

FRANCIS MOORE, JR.
Office Manager

BOARD OF DIRECTORS

HON. JAMES A. WASHINGTON, JR.
Chairman
HON. LINDY BORGES
President

DR. JAMES E. COOK
JOSEPH B. DUNN, JR.
HON. CLARENCE Y. J. HENSON
MAZADA J. MARSHALL

HERBERT O. REID
DOVEY ROUNDTREE
JEROME SHUMAN
RUTH R. WEBSTER

MR. CHAIRMAN and members of the Committee:

My name is Ana Aldama, I am the Program Planner at the National Consumer Information Center (NCIC) here in Washington, D.C. It is a pleasure to be here to testify on behalf of the low-, moderate- and fixed-income consumers across the country.

First, I would like to give you a brief background on the National Consumer Information Center and what we are all about.

The National Consumer Information Center is a non-profit organization which seeks to protect and advance the interest of low-, moderate- and fixed-income consumers. NCIC was founded in 1968 by a group of Howard University law students. It was formed to help poor people in their plight against poverty and lack of information and education on consumer issues. Thus, one of our main objectives is to educate the low-income consumer and disseminate information on consumer issues that affect each of us, but are sadly neglected in low, moderate and fixed areas.

We would like to address the issues of consumer choice, security and privacy, and the impact of Electronic Fund Transfer Systems (EFTS) on those particular areas in relation to the low-income consumer/user.

Electronic Fund Transfer Systems have been implemented on a broad scale, yet, they are not apparent to a great majority of consumers. The average consumer is just beginning to become aware of the spread of EFTS outside as well as inside the financial service institutions.

The consumer's reaction is still uncertain. Consumers have not been searching for new approaches in making payments because the present checking and cash systems seem to be satisfactory. Consumers have not been given an opportunity to make a choice on the relatively new EFTS because the system is already being introduced and implemented to a certain degree.

Low-income consumer groups are found among certain sectors of the population including minority groups, such as Blacks, Spanish Americans, Indians, Orientals, and senior citizens. Many of these consumers are not aware of the Electronic Fund Transfer Systems and as a consequence, have little or no idea how they will be affected by the widespread implementation of the system. Many low-income consumers primarily use cash as a method of making payments. Thus, a widespread electronic fund system may deprive them of means of making financial transactions.

Low-income consumers, in more instances than none, do not have bank accounts. Low-income consumers have difficulty obtaining credit, credit cards or charge accounts, which are easily accessible to middle-income consumers. The most common system of monetary transaction low-income consumers know and are able to use is that of "cash" transactions. Among the low-income population, there are the unemployed, who quite naturally, are excluded from those monetary transactions which are everyday procedures for the average middle-income and/or working individuals.

For the low-income consumer and the fixed-income consumer, such as the senior citizen who have checking accounts, the loss of "float" which the present checking system allows, would present a major problem. According to surveys performed for different agencies throughout the country, approximately 45% of the checks written during one month were written on accounts that had insufficient funds at the time the checks were written (funds were later made available before the checks were cleared). The prospect of an electronic system that would enable immediate direct debiting of the consumer's account at the point of sale would be a strong source of apprehension for the majority of the low- and fixed-income population as it would mean loss of this "float". Undoubtedly, the entire low-income population, who make transactions through the present checking system, would find its financial situation in a turmoil. Thus, a plan may have to be developed to compensate for this loss of float.

Security would pose other problems. For the few low-income individuals who may have access to EFTS cards, what would the liability provisions be if the card was lost or stolen? With EFTS cards, if an unauthorized individual used another customer's card in the system, with a single transaction an individual's life savings could be lost. This would cause a serious problem for the average consumer. For the low-income consumer, it would be a tragedy.

The privacy issue is raised. If the EFTS is fully implemented, personal data would be collected on each person who uses the system. This information can be compiled on a ready-to-use form giving an entire spending history of the person; thus, allowing complete control over a person's private life. Some individuals among low-income consumers have a "bad credit" record. According to a recent Supreme Court decision in Syracuse, New York, secrecy records in a given bank become property of the bank so they can do as they wish with those records. Is the Electronic Fund Transfers System going to open Pandora's box, which will affect credit and employment availability for the low-income consumer/user?

If EFTS were to be implemented on a full scale basis, including banking, insurance companies, food chains, transportation systems, retail stores, etc., what choice would the low-income consumers have? NONE. Then, the question is how is this individual going to handle his monetary transactions? What will the alternatives be or are there any alternatives?

Some possible answers to these questions could be determined by carefully studying the low- and fixed-income consumer/user and the serious implications that EFTS would pose upon them. Also, considerations should be given to providing an educational program for low-, moderate- and fixed-income consumers concerning issues relative to EFTS which would affect them.

In conclusion, NCIC is gratified that this Committee has directed its attention to this area of great concern for the low- and fixed-income consumers. We are hopeful that our remarks today will be of assistance to you in your consideration of this important issue.

Thank you.

1 CHAIRMAN ATWATER: Mrs. Koplow?

2 MS. KOPLow: Ms. Aldama, I think the committee
3 is very concerned about the problems that you have raised,
4 but I don't think that anything in what we are doing would
5 take the choice away from the individual to use his current
6 payment system, whatever it is.

7 The advantage of EFT, as we see it, is that the
8 consumer would have a choice, either/or, whichever was most
9 convenient for him, but I don't think we intended to in any
10 way eliminate the choice he has at the present time.

11 MS. ALDAMA: Yes, I understand that, except they
12 really don't have a choice. Because of their monetary
13 situation, it would be very difficult for them to go into a
14 card system where they hardly can pay with cash. This is
15 the choice I'm probably referring to more than anything.

16 MS. KOPLow: You spoke about float and you spoke
17 about the security of the card, the liabilities, and

18 if you were here today you heard some suggestions
19 made to compensate for the float and compensate for loss
20 of cards and that sort of thing. The committee
21 has that very much in mind, to recommend whatever it can to
22 take care of those problems.

23 MS. ALDAMA: Yes, I was very happy to hear that
24 earlier.

25 CHAIRMAN ATWATER: Governor Mitchell?

1 MR. MITCHELL: I think that you are raising an
2 issue of considerable importance, and that is how to deal
3 with the payments problems of lower income groups, because
4 they do not have accounts in commercial banks. They don't
5 even have accounts in savings and loan associations, which
6 is one step lower, I believe.

7 (Laughter.)
8

9 What I think we are talking about is a technique
10 of payment, of making payments, that augurs at least a
11 possibility of greatly improving the convenience and
12 certainty of money payments for low-income groups. If
13 financial institutions will accept direct deposits to the
14 credit of individuals in those groups, this is a far cheaper
15 alternative and better alternative to receiving a check,
16 which you might have to take to a credit union or to some
17 merchant who is charging a substantial fee to cash that check.

18 Not only that, but if people can be taught to
19 write checks, then they can disperse the funds out of that
20 account more efficiently, and with greater safety, than they
21 could by carrying around cash for a week or two.

22 MS. ALDAMA: Yes, I think we need a great deal
23 of consumer education in every area of these
24 monetary transactions. But, before that, the EFTS systems
25 have been arranged and implemented in such a way that they are

1 untenable for a person who gets a check of \$9000 a year or
2 \$8000 or \$7000 -- the individual who has \$3000 or maybe not
3 even that. They work as domestics and they don't even get a
4 check for what they do, so only cash can they use. I am
5 aware of many more problems of the real low income person,
6 having been in the field for the past 2½ months. And they
7 are really backwards. They are very behind the times.

8 And so, how could we include the low-income
9 individual consumer?

10 MR. MITCHELL: I think EFT offers a better
11 opportunity to do that than the other system.

12 MS. ALDAMA: I agree. I think so, too, but it
13 would take years of education, I believe, and that is what
14 I am concerned about. How can they be included?

15 CHAIRMAN ATWATER: Mr. Plumly.

16 MR. PLUMLY: Ms. Aldama, is an EFTS system today
17 in place? Social Security, Federal Reserve and merchants
18 cooperatively permit -- as a matter of fact, encourage --
19 Social Security supplemental security income people, the adult
20 aged, disabled and blind to receive direct deposit payments
21 today. It is just in its beginning stages, but there are
22 already over 200,000 of these people
23
24
25

1 who have opted to have their monthly payments go to the
2 financial organization of their choice.

3 Now, this does, of course, involve knowing how
4 to use a checking account, or some means of getting
5 the payments out. But it certainly beats them spending
6 anywhere from \$1.00 to \$3.00 cashing their check at a
7 check-cashing service, particularly in the major
8 metropolitan areas, and then taking that money
9 to buy postal money orders, when if they had a checking
10 account, and knew how to use one, and were a little
11 selective, they could get free checking services along with
12 it.

13 CHAIRMAN ATWATER: Mr. Wegner, I believe, has a
14 question as well.

15 MR. WEGNER: I want to say first of all I am
16 delighted that you're here representing your organization.
17 I think the Consumer Information Center is an excellent
18 idea. I think it is the kind of a service and organization
19 that is needed throughout the country. I think that is the
20 first entry point to a good relationship between the
21 commercial community and those who are perhaps moving into
22 a serious relationship with financial institutions for the
23 first time. Hopefully, that first meeting is a good one,
24 and you can help make it so.

25 There is a question here, which has posed a

1 problem in my mind -- the question of the bad credit
2 record.

3 Now, a lot of good people, a lot of people with
4 a lot of money, develop bad credit records. They come
5 and go, unfortunately. Sometimes it is an accident.
6 Sometimes it's a circumstance that occurs once
7 and doesn't occur again. What from the point of view of the
8 people you're dealing with constitutes a fair and
9 equitable way to handle the need of an institution to know
10 what the pattern is of a person's ability to repay, for
11 example, loans that they have had in the past, realizing
12 that the cost of the loan, based on the information available
13 to me, the cost of processing the new application, is
14 somewhere around \$40 or \$50 apiece?

15 Now, if we are dealing with a number of small
16 loans, as a percent of operating cost it's very, very high,
17 and one of the opportunities in EFT is to reduce this cost,
18 which will then become a saving to the consumer.

19 but then of
20 course you get into the other area of -----
21 some transgressions into privacy, or unduly penalizing a
22 person who five years ago could not repay a loan, and this
23 sort of thing.

24 How do you see this balanced? What is the best
25 thing for this commission to do with regard to this problem?

1 MS. ALDAMA: Well, I believe that really
2 developing the educational system on credit or credit
3 availability, and I think that if banks or savings and
4 loans or credit unions would have a consumer information
5 and education part or department or division, that would
6 help, not only to the low-income, middle-income, but even some
7 of the higher income people don't even know anything about
8 EFTS, so of course the educational system would be sort of
9 developing an educational system.

10 That wouldn't cost anything. It would be part
11 of the service. I can see this in all consumer education.
12 That is what my center is all about, but I think this is
13 very necessary for the low-income people, especially, because
14 they would not be as much at fault when they have to pay
15 bills if they knew more about how the credit system works.

16 CHAIRMAN ATWATER: Mr. Rogers.

17 MR. ROGERS: My question has just been answered.

18 CHAIRMAN ATWATER: Mr. Green.

19 MR. GREEN: Thank you. I will withstand the
20 temptation of answering George too directly, only to say
21 that where some people might think the thrift industry is a
22 step below, I would hope that some also think we are the
23 champion of the consumer, and I would like to put that
24 before us as being a true definition of our industry.

25 You know, you spoke of this problem of float,

1 and I think this is a very important thing, too, but I
2 submit to you that whether we like it
3 or not, there has got to be a payments mechanism for people
4 to pay for the goods and services that they have purchased.
5 Poor people and rich people all have to go through some
6 payments mechanism, and I think the payments mechanism that
7 would be in the best interest of low-income families and
8 the best interests of consumers on the whole, will be those
9 types of payments mechanisms that will allow those funds to
10 stay on interest-bearing accounts up until the time that
11 they use them.

12 And I think here that we're talking about two
13 types of systems, the NOW Account, where it stays in an
14 interest-bearing account until you use it, or an EFT account,
15 where at the point of sale that person can activate their
16 account from an institution that has savings account
17 services, so that they can keep that money drawing interest.

18 Do you concur with this?

19 MS. ALDAMA: Yes, I do. I agree with you 100
20 percent, and I realize that float is not a right, it is
21 a privilege, but senior citizens, especially would
22
23 suffer a great deal, because it is a part of everyday life
24 for them now. I agree education will bring a new system,
25 and we will just have to adapt to the new system.

1 But at the present time, gradually, how are
2 they going to take it? That is my concern, but I know
3 exactly what you mean, and I agree.

4 MR. GREEN: You agree with me that we are
5 champions of the consumer? Thank you very much.

6 (Laughter.)

7 CHAIRMAN ATWATER: Let's not be accused of
8 prejudice. I will not go on to the next speaker, but simply
9 to comment that out of the many useful things that you have
10 presented to this commission, I think one that you gave
11 earlier, which is that you felt, in effect, there was not
12 only a need for an educational program which might be
13 carried on in a number of ways, but you felt that there
14 was a need for a study of electronic fund
15 transfer systems as they apply to low-income people. I
16 think that is something we will certainly record in your
17 testimony as worth some kind of examination.

18 MR. WEGNER: May I make one further comment?

19 May I ask the witness, for the record, if you have
20 information in greater detail about what the thinking of
21 the National Consumer Information Center is with regard to
22 how consumer information could be handled nationally,
23 statewide, and otherwise.

24 Could we have that submitted, also, for inclusion
25 in the record?

1 MS. ALDAMA: I will be very happy to submit
2 that.

3 CHAIRMAN ATWATER: Any information on either
4 the specifications or research we would be very happy to have.

5 Are there other questions by the commission?

6 (No response.)

7 CHAIRMAN ATWATER: Thank you very much for your
8 testimony.

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 CHAIRMAN WIDNALL: The next witness is Robert
2 Haydock, Bingham, Dana & Gould attorneys, chairman of the
3 3-4-8 subcommittee of the editorial board of the Uniform
4 Commercial Code.

5 (Witness sworn.)
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

1 STATEMENT OF ROBERT HAYDOCK, JR., COMMISSIONER
2 ON UNIFORM STATE LAWS FOR MASSACHUSETTS, MEMBER
3 OF PERMANENT EDITORIAL BOARD FOR UNIFORM
4 COMMERCIAL CODE

5 CHAIRMAN ATWATER: Welcome, Mr. Haydock. We ask
6 for your testimony, and we do have questions.

7 MR. HAYDOCK: Thank you, Mr. Chairman, and
8 members of the commission.

9 Professor Westin spoke this morning about a
10 board or a committee that might exist to monitor
11 developments in privacy law. I am a member of a somewhat
12 similar board, the Permanent Editorial Board for the Uniform
13 Commercial Code. This Board has been in effect for quite
14 some time, and its function is to keep an eye on the Code
15 and the developments in that area, and to the extent that it
16 seems necessary, to present amendments, new laws, new
17 sections, and so on.

18 The Board has been particularly concerned about
19 the effect of electronic data processing on certain specific
20 articles, two of which have been mentioned this morning.
21 And as a result, they have set up the 3-4-8 committee, which,
22 as you can guess, is based on the number of the articles that
23 are involved.

24 Article 3 of the Uniform Commercial Code, which,
25 by the way, has been adopted now in 49 states and the

Permanent Editorial Board established the 348 Committee (sometimes called the EDP Committee) to advise it on the issue of whether the Board should undertake to prepare substantial amendments or supplements to Articles 3, 4 or 8 of the Code to take into account the impact of electronic data processing on transactions governed by those Articles and to process or prepare amendments or supplements thereto where recommended. In addition to myself the present members of the Committee are:

Carl W. Funk, Esq.
John H. Higgs, Esq.
Paul E. Homrighausen, Esq.
McChesney H. Jeffries, Esq.
Professor Norman Penney
Hamilton F. Potter, Jr., Esq.
Blair Shick, Esq.
Professor Hal S. Scott
Professor Herbert Wechsler

The 348 Committee issued its first report to the Permanent Editorial Board on June 12, 1975 (the 1975 Report). It recommended that Amendments to Article 8 which had been prepared by a committee of the American Bar Association be reviewed by the 348 Committee and submitted to the Permanent Editorial Board. The Amendments would expand Article 8 to cover the transfer of either certificated or uncertificated securities and would, with necessary changes

in general corporation law, to permit corporations to eliminate stock certificates. This review has in fact occurred and resulted in a revised draft of the Amendments being presented by the Permanent Editorial Board to the Conference of Commissioners on Uniform State Laws at a meeting of the Conference in Atlanta last summer. It is contemplated that a further revised draft will be presented to The American Law Institute in May of 1977 with the hope that a second and final reading of the Amendments will occur and be approved at the meeting of the Conference in the coming summer.

The 1975 Report also made comments and recommendations with respect to Articles 3 and 4. They are as follows:

The issues with respect to Articles 3 and 4 resemble those with respect to Article 8 but are more complex and harder to resolve. Perhaps the most fundamental difference is that EDP will probably have a much greater impact on the banking system than it will on our system of evidencing and transferring investments. A certificateless or largely certificateless society could seemingly exist without EDP, while EDP is central or more central to the checkless or less-check society. While the technology of the ACH (automated clearing house) is well advanced, the technology of generating a transfer of funds by electronic means at

the point of sale ("POS") is still in the experimental stage. Moreover, many marketing problems, such as exactly how such services will be offered and the form they will take, have not been resolved. On top of this there are bank branching questions, antitrust questions, questions relating to a possible reorganization of our financial institutions, strong consumer issues and the familiar federal/state issue.

Reacting perhaps to a fear of the unknown, Congress last year established a National Commission on Electronic Fund Transfers, to be made up of representatives of twelve federal agencies having authority over some aspect of banking, fund transfers or consumer rights, two representatives of state banking authorities, seven representatives of the various elements of the banking industry and five public members, charged with reviewing all the problems raised by EFTS (electronic fund transfer systems) and recommending appropriate legislative and administrative action. At the time of this writing the President has not yet appointed the Commission, reportedly because he has been unable to find a satisfactory Chairman. There has been a strong move to legislate a moratorium in the use of POS pending the report of the Commission. While this move is expected to fail

at the federal level and at most state levels, such a moratorium has been enacted in the state of Utah.

Article 4 of the UCC deals primarily with debit transfers evidenced by instruments. Many of its provisions, such as those relating to endorsement of an item, are completely inapplicable to electronic fund transfers and applicability of other provisions is not clear. There is a serious question, for example, as to whether any of the provisions of Article 4 apply to credit transfers at all except perhaps by analogy.

The question of the applicability of Article 4 to EFTS has not prevented the development of the automated clearing house or experimentation in the POS area. Section 4-103 of Article 4 provides that the Article may be varied by agreement, by Federal Reserve regulations and operating letters, by clearing house rules and the like. Relying on these provisions ACH and EFTS have moved forward without worrying about Article 4. In fact, a legal committee of NACHA (the National Automated Clearing House Association) has recently recommended that no effort be made at this time to draft legislation covering ACH operations. Since the last meeting of the 348 Committee it

has been learned that a Federal Reserve committee is presently working on a draft operating letter which will deal with automated clearing houses and, furthermore, is contemplating preparing regulations which will cover point of sale transactions.

The foregoing discussion highlights the federal/state issue and the timing problem. To the arguments against state action discussed above in connection with Article 8 are added the broad rule-making authority of the Federal Reserve Board and the fact that any legislation will have to face head-on the consumer rights problem. Draftsmen of a revised Article 4 may not be able to avoid truth in lending, fair credit reporting, breach of warranty and stop payment issues. Federal legislation has moved into the consumer field, not so much because there is a strong need for uniformity, but because of a lack of concerted state action on the subject, which results in part from the great difficulty of developing a consensus among the more important commercial states as to how consumer problems should be handled. Thus, in addition to the undesirable transition period during which some states would have adopted amendments to Articles

3 and 4 and other states would not have done so, there is a risk of non-uniform amendments being adopted in many of the states.

The strongest argument for state action still remains, however: namely, the existence of a highly technical and well-developed uniform body of state law on the subject, the adaptation of which to checkless transactions and credit transactions by state action would be cleaner, simpler and perhaps quicker than either uprooting existing state law by a comprehensive federal statute or adopting federal "amendments" to state law.

At its first meeting, the 348 Committee concentrated on the federal/state issue and, with the support of all the consultants, tentatively opted for a state law approach. This conclusion was reaffirmed at the second meeting, which was attended by representatives of three federal agencies concerned, none of whom, however, expressed a strong opinion on the issue. The Committee recognized that an amended Article 4 would not even attempt to solve all of the consumer issues, but further recognized that certain of them could not be avoided. It also understood that any legislative scheme at the state level would have to deal primarily with fundamentals

in a manner which would dovetail with the actions and authority of federal agencies.

While the precise steps necessary to achieve these objectives are by no means clear, the Committee is of the view that the failure to undertake a program at this time will leave a vacuum which will certainly be largely filled at the federal level and may invite non-uniform state legislation which would slow the development of a comprehensive EFTS program.

One member of the Committee suggested that any undertaking to prepare amendments to Article 4 would take three years from its beginning to final production of a statute approved by the American Law Institute and the National Conference. A four-year span might be more realistic. Enactment, even with an energetic enacting program, could take another two or three years. This suggests that if the Uniform Commercial Code is to continue to be the source of the fundamental structure of fund transfers, work must start now.

The drafting process itself will tend to sharpen the issues and should move forward at about the speed with which answers to technological and marketing problems of EFTS are found. A drafting committee in being should participate in their solution.

Recommendation

That the 348 Committee be authorized to undertake the preparation of amendments to Articles 3 and 4, that it be authorized to employ a Reporter to assist it and that the Chairman of the Permanent Editorial Board be authorized to add additional members to the Committee to broaden its representation.

Subsequent to the issuance of the 1975 Report, the Committee has engaged Professor Hal S. Scott of the Harvard Law School, formerly a Professor of Law at the University of California, as its Reporter. He is in the process of surveying EFTS developments around the country and will be meeting with the Committee in the near future to reconsider its time table and to discuss the preparation of a report on his findings. At that time the Committee will consider a number of the issues specifically referred to in the Commission's notice of hearing. In particular, they will include the following:

1. The types of payment or collection transactions that should be covered by the UCC;
2. Whether rules covering different types of transactions should be integrated in a single Article;
3. The extent to which consumer problems should be dealt with;
4. Matters which should be left to federal law;
5. The extent to which flexibility should be built into the rules in the manner of Section 4-103 of existing Article 4 or in some other manner;

6. The extent to which Article 4 should be broadened to cover organizations other than banks which will be involved in the fund transfer process.

The draftsmen of the Uniform Commercial Code made a deliberate decision to avoid consumer issues as much as possible and adopted the approach, exemplified by Sections 9-201 and 9-203 of the Code, that its provisions would be subject to provisions of other laws protecting consumer interests. This was done at the time when there was a great divergence among the states on the need for consumer protection. Its wisdom has been demonstrated by the lack of acceptance of the Uniform Consumer Credit Code which, so far, has been enacted by only nine states. Since consumer interests were of necessity tied into the mechanics of the transactions governed by the UCC, however, it was impossible to avoid consumer issues entirely. Article 9, for example, has a whole set of different rules governing security interests in consumer goods. Article 4, in dealing with the rights and obligations of a depositor, of necessity, involves consumer rights.

Uniformity in the consumer area has been obtained primarily through federal intervention. Models are now in place, however, which may make it easier to achieve consensus among the states on the consumer aspects of EFTS.

In any event, it is clear that any legislation relating to fund transfers cannot avoid consumer issues for purely mechanical reasons. If, for example, chargebacks are to be allowed in connection with point of sale transactions they should be covered in the basic statute since they are really an integral part of the payment process. It is too early for me to say whether all desirable consumer safeguards (including protection of privacy) should be part of such a statute or whether they should be dealt with in other legislation.

Our original time schedule would have permitted us to make many of these decisions subsequent to the final report of the Commission. Owing to substantial state legislative activity in the area of EFTS, however, we are being pressed to move more rapidly than originally planned and, of course, it is now clear that the final report of the Commission will be forthcoming later than originally expected. It would therefore seem very desirable that we continue to try to coordinate informally our activities with those of the Commission so that we may be aware on a tentative basis of the directions which its final report might take. Professor Scott has been in touch with the Commission's staff. If more formal liaison should be established, we would be pleased to develop the same.

1 District of Columbia, deals with commercial
2 paper and negotiable instruments. Article 4 deals with the
3 mechanics of the paper collection process and the rights
4 and liabilities and obligations of banks and their
5 depositors. Article 8, which is of no great interest to this
6 Commission, deals with the transfer of investment securities.

7 The 3-4-8 committee has been appointed. It has
8 been in effect for approximately two years now, and I'm glad
9 to see that you will have two other members of the
10 committee testifying here later, Norman Penny and Paul
11 Homrighausen, both of whom know a great deal more about
12 articles 3 and 4 than I do.

13 One of the reasons for that is that I'm working on
14 article 8 at the moment. We have a statute which has gone
15 through the first meeting of the Commissioners on Uniform
16 State Laws, and will come before the American Law Institute
17 this May, and I hope very much will be approved next summer,
18 which will permit the elimination, where desirable, of
19 stock certificates.

20 Now, we have not been sitting on our hands
21 while we have been working on article 8. We have been
22 thinking a great deal about Articles 3 and 4. We have had
23 at least two meetings, at which various bank regulatory
24 people have been in attendance, and people who have written
25 extensively on the subject in the past and know a
great deal about the

1 fund transfer business have joined us, and we have faced
2 a number of problems, and we have made a very simple
3 recommendation to our board, which has been accepted by the
4 board, which is that articles 3 and 4 should be amended.

5 While it's very simple to say that, and we
6 haven't yet told anybody precisely how it should be
7 amended, we have been authorized by the board to hire a
8 reporter, who is in the room here, sitting at that table.
9 He is Professor Hal Scott, who has done a lot of his
10 academic work in this field, and we have commissioned him
11 to spend his time this summer, which he did, going around the
12 country talking to various experts in this field to gather
13 information.

14 We hope very shortly to have another meeting
15 of the committee to consider where we are going to go from
16 here. Part of our recommendation included a time schedule,
17 and that time schedule is one of the things that we are
18 going to have to consider more carefully at our next meeting.

19 We are more fortunate than you are. We don't
20 have to have a report ready by some specific date. We
21 can play along and see what developments are. We are very
22 concerned as to whether there have been
23 sufficient developments in the field of electronic fund
24 transfers at this time for us to come up with sensible rules.

25 Until we see the structures, it may not be

1 possible to really determine what those rules should be.
2 The process, however, takes a long time. The article 8
3 amendments, I think, by the time they get through the various
4 state legislatures, will have been around for six years,
5 and we tossed out the six-year number in our report.

6 I think we have already started, so perhaps we
7 have only five years to go. This would allow about four years
8 to prepare the amendments, and then would give us two years
9 to see that they are adopted.

10 This may be optimistic on the adoption side; it
11 may be unnecessarily long on the drafting side. I think one
12 of the witnesses this morning said a decade was going to be
13 required until we really knew where EFTS was going to be. I
14 think Ms. Koplow suggested it was closer to five years, and
15 I think she is perhaps right. I don't know. That is my
16 own guess.

17 It was clear to me in a discussion with Senator
18 Derezinski out in the corridor after he testified this morning
19 that he wants to see a statute long before four years from
20 now, and there is pressure in state legislatures around the
21 country to get some sort of a model at this time.

22 Our feeling on this delay was that, although we
23 agree with the senator that the present Article 4, which
24 deals with paper transaction, is not really
25

1 applicable to electronic fund transfers, and it is
2 difficult to apply it to credit transactions; that is,
3 where somebody is sending money from his bank account to
4 somebody else's bank account, it is a collections article.

5 Nevertheless, it contains a number of rather
6 basic rules which can be applied, and in some cases have
7 been applied, to electronic fund transfers.

8 In the ACH field, the automated clearing-house
9 field, they have very often defined — in some situations
10 they have defined an electronic fund or magnetic record
11 on a tape as an item, thereby turning on the machinery of
12 Article 4, which basically deals with items.

13 This approach doesn't always work.

14
15
16
17
18
19
20
21
22
23
24
25

1 However, the section 4-103 of Article 4 does
2 provide that the rules of the article are subject to modification
3 by agreement. That is, you can make an agreement with the
4 depositors and the banks involved. The article can also be
5 modified by Federal Reserve regulations and operating letters,
6 and it is subject to clearinghouse rules.

7 Now, those permit broad variations from Article 4
8 and enable you, really, to take it and use it as a semi-
9 structure, at least for the present, and thus permit the
10 development of these various, new electronic fund transfer
11 systems. We feel that it would be a mistake to try to freeze
12 the systems at this time.

13 But, again, we are under this great pressure to
14 come forward with something soon, fairly soon. And I am not
15 going to predict what will happen. We will, obviously, meet
16 from time to time, keep our eye on the situation. We are in
17 that position where we will monitor it and, hopefully, come
18 forward at the right time with the right statute.

19 Now, I would just like to summarize briefly six
20 of the problems that we have dealt with and that we have not
21 yet solved, and we are going to work with them.

22 First of all, what are the types of payment or
23 collection transaction that should be covered by the code?
24 Should credit cards be under the Uniform Commercial Code?
25

1 Debit cards; perhaps pre-authorized payment systems; ACH
2 systems; these are areas that we have not yet made a final
3 decision on.

4 Should the rules covering the different types of
5 transactions be integrated in a single article?
6

7 Is there something in common about them? That is something
8 we are going to have to decide on. At the moment, they seem
9 to operate quite differently under different rules, but we
10 may find a commonality running through them which will make
11 it possible or desirable to put everything in a single
12 article. The Senator this morning suggested that we ought
13 to have a supplementary article, a new Article 10 or some-
14 thing like that, to the code. We have not, obviously, made
15 that decision yet.

16 The extent to which consumer problems should be
17 dealt with. Originally, when the code was enacted, the views
18 on the way consumer issues should be handled varied so much
19 from state to state that it would have been impossible to
20 get the consensus necessary to get agreement among the 49 states
21 that have adopted the Uniform Commercial Code. And, as a result, the
22 Code tried to push aside the consumer issues to the extent
23 that they could be, making it very clear that any consumer
24 law overrode any provision in the Code.

25 This is particularly true in Article 9. Many

1 people have thought that that was a bad decision. It seems to
2 me fairly clear now that when we start dealing with this
3 Article 4 and the relationships between banks and their
4 depositors, we are going to get into consumer problems without
5 any doubt, certainly to the extent that they deal with the
6 mechanics of the process.

7 Whether we should go further than that and deal
8 with matters that do not relate to the precise mechanics of
9 the process, whether we should deal with some of the privacy
10 issues that were raised today, we are not clear on that
11 subject.

12 Another very important problem, one which must
13 concern this Commission, is whether these matters should be left to
14 federal law. What should be the balance between federal law and
15 state law on the subject? Our committee has recommended that, with
16 Article 4 and the many cases and rules that have developed
17 from it, we should use that as a base and build on that. But
18 how high we build is going to depend, to a considerable
19 extent, on what you recommend and whether what you recommend
20 is carried out in the Congress.

21 We will, obviously, want to build some flexibility
22 into our new articles. And I think it almost goes without
23 saying that we will have something that is quite similar to
24 Section 4-103 in the new code, and we may even make it more
25 flexible than it is at present.

1 Finally, the question arises: To what extent should
2 Article 4 be broadened to cover organizations other than banks?

3 That's a tough one, and

4
5 I think we are going to have to go a
6 little further than banks when we start discussing rights and
7 liabilities here. There are outside organizations now that are
8 going to be involved directly in the funds transfer process.

9 I think that is a summary of our problems. If you
10 can help us, we will appreciate it.

11 I will say again, we are very interested in the
12 consumer problems. We have Blair Shick who is the former
13 Deputy Director of the Consumer Law Center in Boston on our
14 committee. We are going to try to establish a better liaison
15 with national consumer groups so that they will know what we
16 are thinking which, I think, is very important. And we would
17 like to continue our liaison with you so that you will know
18 what we are thinking. And we would like very much to get some
19 feeling of where you are going.

20 CHAIRMAN ATWATER: Thank you. That, I think, you
21 can be assured of.

22 Are there questions now by the Commissioners, please?

23 MR. GOLDFARB: Mr. Haydock, you indicated that one
24 of the questions you have is the extent to which the UCC
25 should cover consumer problems. And one of the

1 concern is that you may not be able to get consensus among the
2 states as to whether those provisions should be part of the UCC.
3 That appears to have been a problem for some years, getting
4 consensus among the states as to consumer credit protection
5 matters.

6 Wouldn't that be an argument for allowing the
7 Federal Government to involve itself in most of the consumer
8 questions?

9 MR. HAYDOCK: Well, clearly, in the consumer field
10 the Federal Government came in and in a sense created
11 uniformity.

12 My own feeling on that at the moment is ambivalent.
13 I do think that a model has now been created, and I would be
14 willing to wager that the thinking at the state level is a lot
15 more uniform today than it was 15 years ago when the UCC -- or
16 20 years ago, when the UCC was being originally drafted.

17 MR. GOLDFARB: So what would you conclude from that?

18 MR. HAYDOCK: Well, I would conclude that if we do
19 decide to go whole hog in this consumer field, we would have a
20 good chance of success. That is my present feeling. I'm not
21 sure that we will. And I suggest, again, that we will be very
22 influenced by what the Commission has to say on this.

23 We are sorry that there were delays in your going
24 forward. Our time schedule was somewhat worked out in
25 relation to yours. But we have developed, between Professor

1 Scott and your staff, some good liaison, and we are going to
2 keep in touch with you.

3 CHAIRMAN ATWATER: Ms. Koplow.

4 MS. KOPLOW: Mr. Haydock, were you here at this
5 morning's session?

6 MR. HAYDOCK: I was here for most of it but not all.

7 MS. KOPLOW: Mr. Marson from
8 California spoke, and I questioned him about how long it would
9 take to develop a body of law that would govern all of the
10 phases of EFTS. He said that it would not take long, and that
11 such a body of law was ready in the State of California.

12 Are you aware of the laws in California?

13 MR. HAYDOCK: Well, I'm certainly aware, from what
14 I heard him testify this morning. But he was talking
15 primarily about privacy there, I think. I don't think he was
16 talking about EFTS, in general. But I could be wrong on that.

17 MS. KOPLOW:

18 My question was phrased outside of what he testified on,
19 and he said that California was ready with a body of law that
20 would take care of all of the phases of electronic funds
21 transfer problems.

22 MR. HAYDOCK: Well, I will certainly look at the
23 California law. I am not aware of it at the moment.

24 CHAIRMAN ATWATER: Governor Mitchell.

25 MR. MITCHELL: I would like to get you to focus

1 on the concept that EFT is not going to reach a settled state,
rather it is going to continuously evolve. We don't know how long
3 that evolution might take.

4 Now, in that kind of an environment -- an
5 environment which neither this Commission nor the Congress
6 could stop from occurring -- is
7 it better to rely on agreements among financial institutions
8 and clearing house associations to accommodate developments and
9 avoid enabling them into law?

10 MR. HAYDOCK: Well, I think there is a lot in what
11 you say. I think there is a very good point here. I think
12 that for us to try to develop a new statute which would be as
13 specific as Article 4 is in the paper collection process might
14 be a mistake. That's why I say that one of the things we've
15 got to think about is making the new law more flexible, even
16 more flexible than 4 is right now.

17 I think that is a good point. I'm not prepared to
18 make a decision on that myself at this point. I'm just aware
19 of the problem.

20 MR. MITCHELL: How effective are interbank agree-
21 ments, for example, in dealing with the problems?

22 MR. HAYDOCK: I think they are very effective. But
23 persons that are involved in EFTS transactions besides banks are
24 some of the outside computer companies and the depositors
25 themselves, the individuals themselves, and the extent to

1 which we can get a really valid and effective agreement with a
2 depositor is not perfectly clear. And so in the end, I think a
3 statutory framework would be better. Your point is one of the
4 reasons we felt for the time being that 4-103 would allow EFTS
5 to develop naturally without any interference from us. But I
6 do have the optimism or perhaps ignorance at the moment, that
7 we can find certain general principles that will fit the
8 situation and adapt Article 4 so that it will be more effective
9 and at the
10 same time, not tie down the development. Two years from
11 now I may turn out to be wrong.

12 MR. MITCHELL: But I think, on the side of consumer
13 interests, you've laid aside the part that's most important for
14 you not to: the financial institutions can reflect
15 protect their own interests, but the
16 consumer, the user of the system, is out in left field with
17 nobody to take care of his interests.

18 MR. HAYDOCK: Well, I agree with that.

19 CHAIRMAN ATWATER: I was going to ask something
20 similar to that question. In connection with so-called
21 consumer problems, your item No. 3, you mentioned the
22 mechanics, and I would just be a little curious, if you would
23 expand upon what those mechanics would be in terms of the
24 consumer issues.

25 MR. HAYDOCK: Well, I guess the example I gave in

1 my testimony is the most specific one, and that is, if it is
2 decided that we are going to have a charge-back arrangement in
connection with a credit card, in which a man has five days, let's say,
4 to charge it back, that is a matter of interest to the
5 consumer. But it is also a part of the mechanics of the whole
6 process. And, therefore, clearly, we are going to have to
7 cover that in our article.

8 CHAIRMAN ATWATER: Thank you.

9 Are there other questions by the Commission?

10 (No response.)

11 CHAIRMAN ATWATER: Thank you very much, Mr. Haydock.
12 Your testimony has been very helpful.

National Commission on Electronic Fund Transfers
Users Committee Public Hearings
"Consumers Issues in EFT"
October 26 and 27, 1976
Washington, D.C.

The documents which follow are submitted for the record
of this hearing by:

Robert Haydock, Jr, Commissioner on
Uniform State Laws for Massachusetts

TESTIMONY OF ROBERT HAYDOCK, JR.
BEFORE THE NATIONAL COMMISSION ON
ELECTRONIC FUND TRANSFERS

October 26, 1976

I am a Commissioner on Uniform State Laws for Massachusetts, a member of the Permanent Editorial Board for the Uniform Commercial Code (UCC) and Chairman of a subcommittee of the Permanent Editorial Board known as the 348 Committee.

The UCC, which has been enacted by forty-nine states and the District of Columbia, codifies various aspects of commercial law. Article 3 of the Code governs transactions involving commercial paper including drafts, checks, certificates of deposit and promissory notes. Article 4 governs bank deposits and collections and Article 8 covers investment securities, including stocks, bonds and other instruments commonly traded on securities markets.

The UCC was a joint project of The American Law Institute and the National Conference of Commissioners on Uniform State Laws. These two organizations established the Permanent Editorial Board to monitor the application of the Code and to recommend such amendments to it as changes in business practice might seem to require. The

section, issues which essentially deal with contractual relationships, to be dealt with at the state level.

Obviously uniformity is as desirable here as it is in other areas of commercial law. The National Conference of Commissioners on Uniform State Laws is the appropriate body to work out the details of the necessary legislation.

The existing Code would have to be stretched considerably in order to accommodate the problems raised by this new technology. Articles 3 and 4 deal with the fact that people desiring to make payments (or promises to pay) are looking at, writing upon, losing, stealing, signing, forging, carrying about, revising, failing to complete, doing business in strange places with, and otherwise handling paper.

The underlying assumption of many of the provisions of Articles 3 and 4 is that the paper document is readable by humans without the aid of machines. To bring the magnetic tape of EFT systems under the Code's definition of a "writing" (Sec. 1-201(46)), not only requires the skill of a contortionist but runs directly counter to the philosophy of the Code which was "to avoid making practical issues between practical men turn upon the location of an intangible something...and to substitute for such abstractions proof of words and actions of a tangible character."¹ (Sec. 2-101, Comment).

An excellent article detailing many of these problems is included in Volume 35, Number 1 of the Maryland Law Review (1975). I commend it to your attention.

1. Stephen M. Ege, "Electronic Funds Transfer: A Survey of Problems and Prospects in 1975," 35 Maryland Law Review 3 (1975).

CONTINUED

4 OF 6

Rather than try to patch Articles 3 and 4 of the current Code, we should recommend to the National Conference of Commissioners on Uniform State Laws the creation of another Article which can deal clearly and exclusively with the new technology of EFT.

III. Security

The security of EFT systems for consumers covers a broad range of potential problems: unauthorized disclosure of information (discussed under Privacy), errors in accounts, theft in the most traditional sense at terminals, and computer theft, both of individual accounts and penetration of the entire system.

I will not reiterate here my comments on the unauthorized disclosure of information, except to emphasize the importance of the issue.

Obviously errors will occur with EFTS, just as they now occur with the traditional paper system. Anyone who has ever had experience with computerized billing shudders at the prospect of what may happen with EFT unless safeguards are built in. The oft-repeated excuse that "Something happened with the computer" does little to instill confidence in electronic fund transfer systems.

What is critical here is that consumers have adequate means of ascertaining when an error has been made in their accounts and of obtaining redress. As I have mentioned earlier, legislation mandating periodic statements, in a legible and understandable form, would meet this need. This could most easily be handled through the Uniform Commercial Code. The imposition of penalties for undue delay in correcting errors in consumer accounts would

be one means of encouraging financial institutions to act promptly when errors are reported by consumers.

An aspect of security that is rarely touched upon is the security of the consumer who withdraws cash at an automatic teller machine in an "out of the way" location. State criminal law covers the crime involved. The question is how to prevent it from occurring. One possibility is to regulate locations of ATMs, lighting, hours of operation and other security provisions. In any event, this should be handled at the state level in order to provide for responsiveness to local situations and adequate enforcement.

The two areas most often thought of in connection with EFTS and security are unauthorized penetration of the consumer's individual account and large-scale penetration of the entire system. I am not a computer expert and can offer no solutions to the technical problems involved in making computer systems more secure. I can highlight some of the problems and suggest ways in which the legal system should respond.

Penetration of an individual account is most likely to occur through a lost card or improper customer identification. The cardholder's liability for a lost card should be clearly defined. One approach would be to assess liability against the cardholder only if the card had been requested or applied for (i.e., no unsolicited cards) and if the card issuer had given adequate notice of the cardholder's potential liability and provided him with an addressed notification to be used in case of loss. Liability could be limited to \$50 prior to notification of the loss.

The problem of wholesale penetration of the system is an enormous one. Computer crime is burgeoning. An article on computer crime notes:

... /H/ardly any /computer thefts/ were discovered through normal security precautions or accounting controls and that nearly all of them were uncovered by happenstance. Some experts estimate that the ratio of undiscovered to discovered crimes may be on the order of 100 to 1.²

Statutory and regulatory law are required both for preventive measures and to assure that criminal law keeps step with technology.

One matter to be considered is the point-of-sale devices in retail stores. These are on non-bank premises and are operated by non-bank personnel. Will they be covered by federal and state banking statutes?

This demonstrates the difficulty in approaching the problem in traditional ways. EFT is a unique system, requiring us to re-think many of the categories we are accustomed to using. We need to develop legislation that will consider problems and solutions comprehensively. We should not be bound by boxes of the past.

There is room for both federal and state action here. Problems of contractual relationships and criminal law should remain the province of the states. Finding a solution to computer fraud, which is often interstate in nature, requires a cooperative effort by federal and state legislatures.

2. Porter, "Computer Raped by Telephone," N.Y. Times, September 8, 1974 (Magazine), at 34.

2019

IV. Consumer Choice

As EFT becomes a reality, it is essential that consumers, merchants and businesses retain the freedom, as both a legal and practical matter, to hold accounts in whatever institutions they wish. Moreover those who wish to avoid use of EFT altogether should be free to do so, as long as they are willing to pay the costs.

One problem in ascertaining the costs is that EFT will blend into one system a number of banking services (credit, third party transfers, savings, cash) which are not purchased separately by, and provided separately to, the consumer. If there is no means provided for individual pricing of these services, then some consumers will pay for more services than they want or use, while others will use more than they pay for.

In order to keep options open for all consumers, including businesses, we must assure that savings and loans, credit unions, and other thrift institutions, as well as banks, can participate fully in any EFT system. One means of accomplishing this is to require sharing by all institutions. Establishment of an off-premises ATM or a POS terminal could be made contingent upon an agreement that it would be made available for use by any financial institution on a nondiscriminatory basis upon request of the financial institution and payment of reasonable fees.

Failure to require sharing is likely to lead to domination by one particular financial institution or by one kind of financial institution. Such domination will lead, in the long run, to

fewer choices for the consumer, including, conceivably, the inability to pay cash for some goods and services.

Competition can only be preserved through legislation. Leaving the question to be settled by the marketplace will result in no protection for the consumer.

Competition within the state should be handled by the state. The McFadden Act implicitly recognized this when it left the question of branch banking to the states.

Courts have been wrestling with the concept of what constitutes a branch for years. The question has arisen over devices ranging from deposit boxes to armored cars to automatic teller machines. I believe ATMs and point-of-sale terminals differ so greatly from the traditional concept of a branch that our present legal mechanism is totally inadequate to deal with it.

In spite of this inapplicability of current law, the problem of maintaining competition remains. It is probably of greater significance now than when the McFadden Act was passed because of a greater tendency toward monopoly today, particularly in light of the new, more rapid and widespread technology involved in EFT.

The potential for large financial institutions to obtain significant economic advantages is a matter of federal concern because of the interstate aspects. The federal government should take a strong role here in antitrust legislation and enforcement. There is still a role for state government in this area. Local competition may best be analyzed and preserved by state agencies.

One possible approach might be that taken in the recently enacted amendments to the antitrust act, which provides for enforcement powers for state attorneys general.

SUMMARY

I have focused on a number of problems presented by EFT. Despite this, I remain firmly convinced that computerized financial transactions are not only inevitable, but hold great promise for consumers in terms of more rapid and more universally accepted transfer of funds, as well as increased personal convenience. I, myself, have held a debit card ever since such a system was instituted in my home town, and have been very happy with the service.

As with any technology, EFT is neutral in itself. It is in the application that the potential for significant benefits and significant injury lies. My purpose in pointing out the problems in the areas of privacy, commercial law, and security, is not to decry the advent of EFT, but to call for state and federal action that will assure that electronic fund transfer systems work to serve people.

CHAIRMAN WIDNALL: The next witness is Mr. Norman Penney.

202

(Witness sworn.)

CHAIRMAN ATWATER: Mr. Penney, we will appreciate your
ten minutes of testimony. Please be prepared to respond to
questions.

TESTIMONY OF PROFESSOR NORMAN PENNEY,

NATIONAL COMMISSION ON ELECTRONIC FUND TRANSFERS.

MR. PENNEY: Thank you, Mr. Chairman.

Am I correct in understanding that the members of
the Commission staff have received copies of my prepared state-
ment so that I am not required to read the statement?

CHAIRMAN ATWATER: Yes, we have.

MR. PENNEY: If I may, therefore, I would like to
simply focus on a few matters and then
devote the balance of such time as the Commission wishes to
cross examine me on what I have said or what I have taken a
wild swing at.

I addressed my response to the initial Notice of the
Hearings in which a number of specific questions were posed,
and I dealt with a fair number of those. On
some of them, obviously, I was making simply a statement that
was in the nature of a judgment call on which, I am sure, my
opinion is no better or worse than anyone else's.

I have tried in what I am going to say now, to
focus on a few matters on which I know something. I will not deal
with the generalized questions having to do with privacy or

1 security and matters of that kind, out rather with questions about
2 the relevance of the present rules, the rights
3 that are foreclosed or diminished, and particularly, of course,
4 all of this having to do with the rights of consumers in an EFT
5 environment.

6 One of the first questions that you posed, and one
7 with which a number of people have dealt is, does Article 4 of
8 the Uniform Commercial Code apply to EFTS transactions?

9 My answer to that is mixed. EFTS, as you all know,
10 is a mixed bag of subsystems, and I think the general consensus
11 of those who responded to this question is that the answer is
12 probably yes, or affirmative, to coverage of what might be
13 characterized as pre-authorized debits; and probably yes to
14 transactions conducted through ATMs or automated teller
15 machines.

16 The answer, however, is probably "no" to pre-authorized
17 credit transactions and probably no, therefore, to much of what
18 is involved in POS-type installations.

19 ACH is something else. There are many elements, of
20 course, in ACH and POS that are, in effect, pre-authorized debit
21 transactions. However, as to those, as I have said, probably
22 Article 4 can be made to apply, and without too much
23 stretching.

24 The next question you asked had to do with rights
25 foreclosed or diminished. What is

1 it that the consumer is likely to lose or which of his rights
2 are threatened by EFTS systems?

3 Probably the one that is mentioned the most is the
4 right to stop payment. As you know, the Code gives that right
5 to a consumer, and as a matter of fact, it is provided for in
6 even an oral form. The ability to make an oral stop, which is
7 a consumer issue, was indeed one of the few areas that the
8 bankers, at least in New York and some other states, fought very
9 vigorously at the time the Code was proposed for adoption in
10 New York and some other states.

11 Another right, so-called, of the customer that is an
12 issue is the right to the return of checks with a bank state-
13 ment. Obviously, in the systems that are being discussed,
14 there will not be any check, as such. That being the case, the
15 kind of statement that the customer gets raises problems about
16 the evidentiary value of whatever it is he does get, either
17 with his statement or from the terminals that he uses. This
18 question also affects the customer's record-keeping capability
19 and his ability to verify the transactions that he conducts
20 with his bank. And this is in turn tied to the question of a
21 customer's ability to insist that only those items that are
22 properly payable are debited to his account.

23 As the rules of the check game now stand, as most
24 of you know, a customer is only liable for those
25 debits to his account which are properly payable; or putting it

1 in reverse, the bank may only debit his account for properly
2 payable items. If the items are not properly payable, the bank
3 is paying out its own money, and the customer can insist that his
4 account be recredited.

5 The kind of information that the customer now gets
6 with the bank statements and the checks enable the customer to
7 police that right, and that right, in a sense, is jeopardized by
8 the reduction of the information that he gets.

9 Somewhat related to this is the point that banks, in
10 their bank statements, often utilize legends which attempt to
11 establish by contract the conclusiveness of bank statements
12 after the passage of a certain period of time. In most juris-
13 dictions where this matter has been discussed, that attempt by
14 the banks has been characterized as in violation of 4-103. That
15 provision seeks to limit banks' ability to contract out of
16 liability. But in New York, as some of you know, there are
17 several lower court decisions upholding the effects of such
18 legends in the banks' behalf.

19

20

21

22

23

24

25

1 I am concerned that if we move toward the
2 system which eliminates some of the information that a
3 customer gets, and at the same time we have a trend -- and
4 this now appears to be the case in New York -- permitting
5 banks to establish the conclusiveness of the statements they
6 furnish, this will
7 be a real threat to the consumer's relationship with his
8 bank.

9 You have also asked the question about whether
10 I believe that the legislation in this field should be left
11 to the states, or whether the federal government should
12 undertake to regulate it.

13 I think I said in my statement that I believe
14 that many, if not most, of the rules here are better left to the
15 UCC, and the amendment process that has been just described
by Mr. Haydock. Nevertheless, there are a few things on which I think
16 it is proper, and possibly important and necessary, that the
17 federal government step in.

18 For example, I am one of those who would support
19 efforts now, as soon as possible, to put debit cards in
20 several respects on the same basis as credit cards.

21 I would urge, for example, that card issuers,
22 that is, debit card issuers, suffer the same rules or
23 limitations on the sending of unsolicited cards.

24 I would urge that they have the same benefits of the
25

1 \$50 limit on liability, and as a matter of fact, as I think
2 you know, there are a number of states that have now provided
3 this kind of limited liability with respect to debit cards.

4 The question of cards that are to be used in
5 POS terminals is a little more complicated because they have
6 a variety of capabilities.

7 If they, of course, have the credit card
8 capability, they are already subject to the federal regulations
9 now in effect. But assuming they don't, that is, assuming
10 such POS cards do not have the credit card capability, there
11 then arises the question of whether these cards should have
12 rules apply to them that are again somewhat similar to those
13 operative in Truth-in-Lending. In particular, I have in mind the
14 rules in regard to third party defenses, which is somewhat
15 related to the charge back or stop payment phenomenon, and
16 fair credit billing rules.

17 As a general proposition, I think I'm persuaded
18 now that these cards probably ought to have the same kinds of
19 rules attached to them as are attached to credit cards with
20 respect to fair credit billing, and that some system needs to
21 be worked out to give the customer some of the benefits of the
22 stop payment or third party defense that are available to
23 credit card customers.

24 I'm not quite settled in my own mind as to what the
25 proper approach on this ought to be, but one thought that

1 occurred to me recently -- and it is not novel to me because
2 it is again related to the present rules on credit cards --
3 is that if a card in a POS environment is used in a way that
4 is really a substitute for cash which might, for example,
5 be for a transaction, a local transaction of less than \$50,
6 it ought not to be reversible.

7 On the other hand, if it is for a large transaction,
8 that is a transaction in excess of \$50, maybe that is the
9 cutting line at which somebody would normally use a check
10 and they, therefore, at that level ought to enjoy the same
11 benefits to stop, reverse, assert third party defenses or
12 whatever.

13 I think that's all I have to say at the moment.

14 I made a number of other comments in my submitted
15 statement, but I would like to stop.

16 CHAIRMAN ATWATER: Thank you very much.

17 Mr. Worley?

18 MR. WORLEY: Yes.

19 I'm wondering if you could express an opinion
20 with respect to a retail transaction at a point of sale as
21 to what kind of written evidence, if any, a customer
22 ought to have to support a transaction that they have
23 accomplished through a POS terminal.

24 MR. PENNEY: Well, I said in my prepared statement
25 that I tend at the moment to sympathize with the Comptroller's

1 proposed guideline that would require such terminals to
2 produce a piece of paper on which certain critical information
3 would be furnished to the customer.

4 How far that ought to go, I don't know.

5 It seems to me in most such POS sales transactions
6 you've already got or you can get a sales slip if you want
7 the details of the transaction.

8 MR. WORLEY: How long would you suggest that the
9 sales slip be retained by the retailer as evidence of a proper
10 charge against a customer's bank account through the use of
11 a debit card transaction?

12 MR. PENNEY: Well, I am really out of my
13 my area, in answering that.

14 I suppose he has got the problem, again, that all
15 people engaged in any aspect of this have, of later contesting
16 or responding to a claim and I suppose, therefore, the
17 statute of limitations period ought to have some bearing.

18 MR. WORLEY: You don't really mean that, I hope.

19 (Laughter.)

20 MR. WORLEY: The whole idea of EFT is to reduce
21 the flow of paper, not magnify it.

22 MR. PENNEY: I don't want it to flow. I thought
23 you asked me if I wanted you to keep it.

24 MR. WORLEY: Don't you think an EFT debit card
25 transaction might be similar to a credit card transaction in

1 which the credit card industry clearly has that
2 same problem at present?

3 MR. PENNEY: Well, I'm speaking in ignorance of
4 what the practices are in the use of credit card pieces of
5 paper and how long they are required to retain such records.

6 Just for openers, I suppose a similar kind of rule
7 or similar kind of approach might be well utilized for this
8 paper.

9 MR. WORLEY: Well, you spoke of substituting the
10 warranty of these products for the signature on the check.

11 MR. PENNEY: I was talking about the
12 check at that juncture. I had in mind there the problem
13 particularly of the pre-authorized debit which is now an
14 established business, as you know, with respect to insurance
15 premiums and the like.

16 And the problem is, I think, as I stated it,
17 that the code rules, if they are taken literally, just don't
18 seem to give the same degree of protection because of the
19 absence of customers' signatures.

20 MR. WORLEY: I'm really interested in the problem
21 of how to substitute proof of a transaction or proof of
22 payment based on the receipt of a bank statement with some
23 form of descriptive billing.

24 In terms of the
25 UCC, is it your idea that that would substitute for a check

1 in substantiating expenditures, for example?

2 MR. PENNEY: There are different levels of the
3 problem I think we're all trying to address with respect to
4 this furnishing of information, whether it be in the form of
5 paper or whatever.

6 One problem is the problem of fighting with your
7 bank if they've made a mistake, and at the moment you've got
8 a piece of paper, among other things, to fight them with.
9 And I am trying to furnish them something else.

10 Certainly, that seems to me much more needful
11 in a free-standing ATM, standing out in the middle of a
12 metropolitan area with nobody around, when the machine does
13 not give you the money you think you asked for.

14 If you haven't got some kind of record of it,
15 it seems to me you're in deep trouble unless the president of
16 the bank happens to be standing behind you, which I think
17 happened in one case that I know of.

18 CHAIRMAN ATWATER: Mr. Tangney?

19 MR. TANGNEY: You mentioned that Article 4 gives the
20 consumer two things, in your opinion. Article 4 gives the
21 consumer protection which relates to debit transactions, but
22 not to credit.

23 Could you expand on that a little bit?

24 MR. PENNEY: I don't think I quite said it that way,
25 Mr. Tangney.

1 I tried to say, maybe not very artfully, that I
2 thought that Article 4 generally is applicable to
3 pre-authorized debit transactions because most of what goes
4 on in those transactions is sufficiently analogous to check
5 flows, so as to fall within the general schematic approach
6 of Article 4.

7 On the other hand, pre-authorized credits don't
8 fall as easily under 4, because if you look at the definitions
9 and so forth in Article 4 it is talking about the movement of
10 debits as opposed to credits.

11 MR. TANGNEY: But credits are movement of funds
12 into the consumers account; debits are moving funds out.

13 MR. PENNEY: That's right, as are checks.

14 MR. TANGNEY: So the debit is the key.

15 If the consumer is protected under Article 4 for
16 debits, that is the protection he needs, is it not?

17 MR. PENNEY: Well, the consumer, believe it or not,
18 is at some degree of exposure even with respect to money
19 coming into his account. It is kind of hard for people to
20 figure out how that can be, but I can give you two or three
21 situations where it might occur.

22 Let's assume you've got an account which is one of
23 two or three in a bank, and you set up the machinery to have
24 paychecks or whatever credited to your account. If for some
25 reason you decide that you don't want to have the money come

1 into that account and in fact it comes in, two or three
2 things quickly might happen. If there is no following out of
3 your instructions there may be adverse tax consequences.
4 Another thing is you may be subjected to garnishment or some
5 other process.

6 A third thing is that account may in fact be
7 an account which you share jointly with some other person,
8 and when the money comes in the other guy takes it, and that
9 is why you want to stop it.

10 MR. TANGNEY: But don't we have the same problems
11 today in our computerized networks when the magnetic ink
12 is misread and it goes into the wrong account?

13 MR. PENNEY: Sure.

14 MR. TANGNEY: My point is that the differences --

15 MR. PENNEY: But that's an error.

16 I'm talking about the failure of the bank to implement
17 instructions and how a person is exposed by the failure on
18 the credit side.

19 MR. TANGNEY: That's a failure, also.

20 My other point is

21 it has always been
22 my experience as a banker that we have to prove to the
23 customer that we took the money out at his instruction, and
24 when we have no instructions the
25 customer cannot come to us and prove that he did not. It is

1 up to us to prove that he did take that money out.

2 So your concern on a credit card or ATM, it is up
3 to us to prove that he did it, not him to prove that he did
4 not.

5 MR. PENNEY: Except that if you go ahead and take
6 the money out of his account and you have been operating,
7 let us say, on the strength of what is much more frequently
8 discussed, a lost or stolen debit card (and
9 the customer may be completely innocent of the fact that some
10 other person has stolen the card) and you go ahead happily
11 honoring all of these debits. Meanwhile, the customer has no
12 knowledge of this and later on, of course, there comes a
13 reckoning, and the question is whether the customer can now
14 have his account restored.

15 And I think most people agree the answer to that,
16 unless the customer has been negligent in the handling of
17 that card, is yes.

18 MR. TANGNEY: But in the same way today, if someone
19 takes a check and forges a signature, he'll take the
20 money out until the day of reckoning, and when the day of
21 reckoning comes the consumer is reimbursed.

22 MR. PENNEY: Sure, but the problem with these
23 debit cards is they are floating around, they are much easier
24 to use improperly, they lend themselves, in a way, to improper
25 use unless they are properly controlled, unless you have the

1 proper safeguards, the PIN numbers, the whole business.

2 CHAIRMAN ATWATER: Are there other questions?

3 Yes, Mr. Anderson.

4 MR. KENNETH ANDERSON: Is it your feeling that
5 the problems that the consumer faces as a result of the way
6 the law is written today are sufficiently important that those
7 problems ought to be resolved by changes in the law before EFT
8 goes much further, much faster?

9 MR. PENNEY: In respect to what the establishment of
10 a sort of bill of rights of the consumer in the EFTS environ-
11 ment and privacy, which I know very little about, requires some
12 staking out before the systems become too heavily developed.
13 Because at that point you get very substantial economic hardware
14 and software, these vested interests make it much more difficult
15 to make changes.

16 So I am sort of sympathetic with the argument, and
17 I think you are seeking to elucidate from me that we ought to
18 stake out that ground now insofar as we can perceive in advance
19 what the problem areas are, but always in a way, of course, that
20 won't unduly inhibit the development of the systems.

21 We don't want to completely hobble it in a way that
22 won't allow for technological innovation.
23
24
25

1 CHAIRMAN ATWATER: Governor Mitchell.

2 MR. MITCHELL: Just a question of fact.

3 Suppose I went to Giant Food Store and wrote a
4 check for \$40 to buy groceries. In the normal course of
5 events, Giant Food Stores are on their toes, and that check
6 would be taken to their commercial bank and presented for
7 collection the next day.

8 My question is, how much time do I have for my stop
9 payment order?

10 MR. PENNEY: You can register your stop payment at
11 any time before the check is fully processed for payment
12 at your bank.

13 MR. MITCHELL: Does that grant the right to return
14 items?

15 MR. PENNEY: The answer to your question is determined
16 by Section 4-303 of the Code. That is, when a stop payment
17 comes too late, you put together 4-303 and 4-403, and the
18 answer to your question comes right up. You have the right
19 to stop payment on that check until any one of the various
20 steps that are spelled out in 4-303 are accomplished.

21 MR. MITCHELL: It is midnight the next night.

22 MR. PENNEY: That is a very debatable question,
23 as Professor Leary will tell you if he is around.

24 You speak with an accent that suggests you are from
25

1 out of town.

2 MR. MITCHELL: No, no. I live right here.

3 You are the most elusive witness we have had
4 today.

5 (Laughter.)

6 MR. PENNEY: I thought I gave you a direct, straight
7 answer. The law is elusive. If you have clearing house
8 rules in Washington that provide for return of items by
9 midnight the day after tomorrow night, that is the cut time.

10 MR. MITCHELL: There are not such rules, I don't
11 believe.

12 CHAIRMAN ATWATER: May I ask a general question?

13 Here we are at the end of our list of
14 questions, but supposing there were written a bill of rights for
15 the consumer.

16

17

18 Let's assume, for the moment, we are able to
19 agree on a few of those issues.

20 What impact would that have on the
21 UCC? What would be the mechanics, the method, the timing of
22 the incorporation of those positions into the Uniform
23 Commercial Code?

24 MR. PENNEY: Well, I have to speak with a bit,
25 of vested interest as a member of this committee

1 that Mr. Haydock and I both serve on.

2 I think that there are some rules, for example,
3 those with respect to stops that are better left to the UCC.

4 I think, as I said earlier, the limitation of
5 liability on exposure to cardholders ought to be dealt with
6 very quickly, because those cards are proliferating at a
7 very rapid rate, and it seems to me the analogy is so perfect
8 that why somebody -- the FTC or somebody -- doesn't promulgate
9 such a rule tomorrow, I don't know.

10 It seems to me that's the appropriate thing to
11 do insofar as the other types of rights that are at issue here.
12 Most of them, I would say, or certainly a good number of them,
13 that are not related to privacy

14 are better left to the UCC revision effort,
15 and I think it will come rather swiftly.

16 However, as I said in my statement, if the technology
17 and the business develops much more swiftly than our clinking,
18 clanking machinery can cope with, then it may come that a
19 federal intervention of some kind is necessary in specific
20 areas.

21 CHAIRMAN ATWATER: Ms. Koplow?

22 MS. KOPLow: Mr. Penney, isn't there now in the
23 operation of the electronic fund transfer system, those that
24 operate on a contractual agreement between the consumer

25 and the bank?

1 MR. PENNEY: Well, there are about as many as there
2 are different banks and are customers.

3 I made an effort this summer when I was putting
4 on this little program to contact as many banks as I could
5 quickly and get customer contracts from them, and it was
6 really quite interesting how many different efforts there
7 were, how varying they were. Some of them were quite
8 overreaching, I should say.

9 MS. KOPLow: That might be, but until such time
10 as legislation or regulation is passed to control or unify
11 the kind of fears that we might have, isn't that a good enough
12 substitute to let industry progress?

13 MR. PENNEY: I am all for allowing private
14 agreement between banks, and banks and clearing houses and
15 the like, control for a substantial period.

16 MS. KOPLow: I'm not talking about the wholesaler.
17 I'm talking about the consumer.

18 MR. PENNEY: That's exactly what I'm addressing
19 and I feel much more nervous about that.

20 I think generally speaking -- and Mr. Tangney
21 thinks I'm an anti-bank lobbyist, the way I'm speaking. I've
22 had banks as clients, I've worked in banks. I'm sympathetic
23 to banks. I know a lot about banks and their problems. To
24 know them is to love them, and also, I think, to know in some
25 instances where they go wrong. And I think some banks have

1 overreached.

2 I think by and large the industry is now quite
3 consumer-aware, and they are, generally speaking, pretty good
4 about not seeking to overreach with customers in their private
5 contracts.

6 But there are some instances where they try, and I
7 am trying to suggest one or two, such as exposure on debit
8 cards for openers, and I would not leave that to them.

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 MS. KOPLOW: Then are you saying in fact that
2 until these issues can be resolved there oughtn't to be any
3 EFT exchange between the consumer and the bank?

4 MR. PENNEY: No.

5 MS. KOPLOW: And how are they perceived? I see you
6 are saying no. How do they proceed prior to the time that
7 regulations or laws were passed to govern it?

8 MR. PENNEY: Well, what's happening now, as I'm
9 sure you are aware, is that many states are beginning to inter-
10 vene because of consumer interest in the phenomenon. Wisconsin
11 and a number of states in the midwest have already enacted
12 legislation controlling some of the things I discussed.

13 I'm a little concerned because if there is a pro-
14 liferation of these different state statutes that vary sub-
15 stantially one from another, we are going to have a terrible
16 problem, it seems to me, when it comes to uniform codification.

17 MS. KOPLOW: But isn't that exactly what is going
18 to happen, because it may take the Uniform Commercial Code five
19 years, four years, to perfect the kind of model legislation
20 that they think every state should have.

21 Are you suggesting that prior to action by the Uniform
22 Commercial Code Committee that the federal government act?

23 MR. PENNEY: In the areas that I have particularly
24
25

1 addressed, the answer I have given is yes.

2 MS. KOPLow: Then if that happens, you won't need
3 the Uniform Commercial Code.

4 MR. PENNEY: No.

5 The Uniform Commercial Code deals with many other
6 matters than simply the exposure to risk on debit cards and
7 unsolicited cards.

8 MS. KOPLow: Well, who is going to decide? Are
9 you suggesting that we decide which ones the federal
10 government handles and which ones we leave for the development
11 of the states on the Uniform Commercial Code?

12 MR. PENNEY: I think what you need to do is to
13 make an assessment of the kinds of problems like the ones I
14 have attempted to suggest to you that seem to warrant federal
15 intervention soon and get behind it in whatever reports you
16 issue.

17 I have given you the one I would say that you
18 ought to recommend be treated by some sort of federal statutory
19 regulation soon.

20 It seems to me there are other matters that you can
21 identify as consumer-related, but might better be left to
22 uniform codification and you ought to leave it alone.

23 CHAIRMAN ATWATER: Are there other questions by
24 the Commission?

25 MR. MITCHELL: Yes. May I ask one other question?

1 CHAIRMAN ATWATER: Governor Mitchell.


2 MR. MITCHELL: If you were setting forth precisely
3 what should be on a commercial bank statement that did not
4 involve the return of checks or the use of checks, what are
5 the items of information that are essential to protect
6 consumer interests and the like?

7 MR. PENNEY: Well, the analog, of course, today
8 is the credit card bank, the bank credit card statement,
9 which includes the date of the transaction, the name of the
10 payee and the amount.

11 I have had my own problems with card issuers in
12 respect to contested transactions, and for that reason, I am
13 sorry to confess I'm sort of a proponent of "country club"
14 billing, so-called, but I don't think it really works for some
15 of the applications of this kind of system.

16 So in substitution for that, I guess what I would
17 like, if it were technologically feasible, would be we would
18 have a little bit more information, for example, on not only
19 the name of the payee, possibly, the city or something about
20 the location, where it was used, and -- this is very much more
21 doubtful -- some effort to characterize the type of purchase,
22 whatever it was, that was bought.

23 Now, we are talking about an awful lot of
24 characters now and an awful lot of code, and I may be
25 completely out of it in terms of the ability of any system to



1 properly respond to that, but if I had my druthers, that is
2 what I would like to see.

3 MR. MITCHELL: The endorsement doesn't
4 matter to you, then?

5 MR. PENNEY: There isn't any such thing as an
6 endorsement on an electronic blip.

7 MR. MITCHELL: But there is on a check.

8 MR. PENNEY: That's right.

9 MR. MITCHELL: And you are not disturbed by
10 that not appearing?

11 MR. PENNEY: Well, no, because it is a different
12 matter. I don't think you need to worry about that in
13 electronic transactions.

14 CHAIRMAN ATWATER: Are there other questions?

15 (No response.)

16 CHAIRMAN ATWATER: Professor Penney, we thank you
17 very much for your testimony.

18 It's been extremely helpful.

19

20

21

22

23

24

25

National Commission on Electronic Fund Transfers
Users Committee Public Hearings
"Consumers Issues in EFT"
October 26 and 27, 1976
Washington, D.C.

The documents which follow are submitted for the record
of this hearing by:

Norman Penney, Professor, of
Cornell University School of Law

October 26, 1976

Statement of Professor Norman Penney
to the
National Commission on Electronic Fund Transfers

Gentlemen:

I am grateful for the opportunity to appear before you, and wish to respond to some of the questions which you have put forward in your notice of hearings dated September 30, 1976. Obviously the questions asked are much more numerous than can be responded to in a 15 minute presentation. I am happy about that, because although I find that I am interested in most of the questions asked and have opinions on many of them, there are only a few on which I may have something to offer as a so-called specialist.

PRIVACY

Let me make a brief comment on the first area of your inquiry, namely privacy. I do not pretend to be an expert in this field but have read some of the literature on the subject and have attended a couple CLE programs at which the problem was discussed. May I simply summarize my viewpoint by saying that although I think the concerns about privacy may be somewhat overstressed in detail, I am persuaded that the risks, over the long range, are much greater than most industry representative will acknowledge. In particular, if I had to associate myself with either the viewpoint of Mr. Deutsch or Mr. Armer as expressed at the Bank Marketing Association meeting in Toronto and as reported in the American Banker article of September 14, 1976,

Page 2

on the issue of privacy or "government prying", I would choose the side of Mr. Armer and the angels.

CONSUMER CONVENIENCE

Under the heading of Consumer Convenience begun on page 5 of the notice, again I do not purport to be either an economist or a marketing expert. My own unscientific sample of consumers, students and others with whom I discussed this matter, however, persuades me that as a general proposition, most consumers do not want EFTS services. For the most part, I think they would rather leave matters as they are; and in this respect I believe the reports that we read in the media are essentially accurate. Some, but only a few recognize possible advantages. These would include:

- (1) Saving time in check writing and bank reconciliation;
- (2) Convenient one-stop banking locations where they can perform a number of critical but routine banking functions more swiftly than at present;
- (3) Reasonable assurance that certain critical bills will be regularly paid on prearranged credit transfer arrangements;
- (4) 24 hour cash availability in critical location with new ATM facilities;
- (5) More places where business can be done without cash through the utilization of POS terminals;
- (6) Direct deposit of payroll, social security, annuity and other regular remittances.

While many customers will be happy to take advantage of some of these services, the notion of moving into an arrangement in which a major share of the household budget is handled by EFT systems strikes a negative chord in the great majority of American consumers at least at the present time. He or she is much more interested in managing his own affairs, in keeping control over his own packetbook, in having detailed records of his accounts, in having the right to stop payment on his checks if he later decides to stop checks and in having the availability of the float, than in the "benefits" of EFTS.

I believe that the pressures for moving to EFTS come mainly from the corporate sector particularly the banks, as stated by Mr. Armer and many others. Bankers are properly concerned with the "paper crunch" and the cost escalations that are associated with the paper medium. I believe, therefore, that if we are to go to EFTS, we should do so gradually and in a way that leaves the consumer/bank customer with a choice. The choice should include the ability, for the foreseeable future, to continue to use checks and other media of payment. To ensure this may require some regulation to prevent loading checking accounts charges in a way that would force customers into the new medium. I am concerned that a dual system may present financial institutions with an enormous expense which will prompt them to push their customers into the new services. I would hate to see bank customers pressured into these new arrangements in a way that removes a number of their present rights or benefits,

Page 4

and, at the same time saves them little or no money. A not very good analogy is the bank credit card. The cards were initially promoted with unsolicited mass mailings to attain critical usage volumes. Customers were initially offered a "free period" for payment of department stores and other bills, but recently there is a plan to make a minimum charge, eliminating the free element.

RIGHTS, DUTIES AND RESPONSIBILITIES OF CONSUMERS IN TRANSACTIONS

The main comments I have to offer are under the heading Rights, Duties and Responsibilities of Consumers in Transactions and the questions put forward under that heading beginning on page 6 of the notice of hearing.

Relevance of Present Rules

The first question asked at the top of page 7 of your notice is "to what extent are present rules governing commercial transactions relevant to an EFT environment? Will EFT distort the application of any present rules or create unfair burdens?" I have submitted to the commission as an appendix to this statement a short article which I recently submitted to the University of Pittsburgh Law Review having to do with the impact of EFTS on the rules of Articles 3 & 4 of the Uniform Commercial Code. Summarizing from that article, I think it is fair to say that the present rules of Article 4 probably do apply to preauthorized debit transfer systems and to transactions conducted through automated teller machines. However,

insofar as EFTS systems include preauthorized credit transfers and point of sale transactions with virtually instantaneous debits and credits, present rules of Article 4 are either inapplicable or inappropriate in many instances. The main areas that need to be dealt with are: the right of the customer to stop payment, the duties of the customer in respect to a returned bank statement, finality of payment, and the warranties of the various participants, particularly a warranty of authority to substitute for the warranty of the genuineness of the drawer's signature on a check.

Consumer Rights Foreclosed or Diminished

I have already mentioned the right to stop payment. This is a valuable right but one whose merits can be debated. One could question whether this right should be available-unfettered-and at the whim or caprice of the customer as it is at present with checks. But in addition to the right to stop payment, a customer also has the right to insist that any debits from his account be otherwise properly payable (under UCC, § 4-401) and a customer's bank cannot exculpate itself from negligence in performing its banking functions in respect to those payments under UCC § 4-103. A customer also has a right to the return of his cancelled checks and these checks perform a useful auditing and evidentiary function.

How and Who to Regulate

As you know, I am a member of the 348 Committee of the ALI Permanent Editorial Board which was formed to consider the

amendment of Articles 3 & 4 and that committee was unanimous in the view that most of the rules I am talking about today ought to be contained in a revised Article 4 of the Uniform Commercial Code. I am content to leave some of the rule making to bank -to-bank contracts and Regulation J. However, I do think that most of the rules that impact directly upon the consumer ought to be the subject of state legislation (preferably uniform), unless the state becomes so much a captive of the banking industry or so dilatory in enactment of model proposals that federal action seems necessary.

Debit Card Model

Insofar as the legal model for the debit card is concerned, I believe that the combination of the check model and the credit card model is most appropriate. I would strongly urge that credit card rules on unsolicited cards and \$50 limitation of customers liability be applied to debit cards.

Assignment of Liability

As to the question, how should liability be assigned among the participants in the transaction, I believe the liability should be assigned in a way that most closely comports with the present allocation of these risks in respect to checks.

Change in Consumer's Ability to Detect and Correct Error

Since financial institutions are the proponents of these systems, the burden should be upon them to demonstrate a compelling reason for the shift of any substantial present or new risk to the consumer. The question of how does EFT change the

consumer's ability to detect and correct errors seems to me to relate primarily to the bank statement. The customer under most EFT systems receives a statement mostly closely analogous to the statement received by a bank credit card customer. There is not very much information about individual transactions--only the date, the name of the payee and the amount. Also, I think it is pretty well recognized that a customer is less likely to keep detailed records of payments made through remote terminals than he is with the present checks stubs that are provided in checkbooks. It is for that reason that I generally tend to favor the proposal in the Comptrollers Guidelines which requires that POS and ATM terminals produce hard copy output for the customers records.

I am skipping over the other questions on the bottom of page 7, because I am not really sure what the commissioners are after, and I do not have much to offer on these questions.

Consumer Rights Jeopardized by EFT Breakdown

The question of jeopardy to the consumer's rights produced by EFT systems breakdown depends firstly on the extent to which customers become substantially dependent upon such systems. It also depends upon what actions their creditors are likely to take if, as a result of a breakdown there is a failure of payment, or failure of timely or sufficient payment. My suggested response to this as well as other similar questions is to try to require that there be a complete disclosure to the customer of the risks, that the operating financial institutions con-

tinue to bear some of the risk of consequential harm, and that the customer continue to have available to him other modes or media of payment that he may utilize if he should conclude that the risks of this particular type of system are too great for some sensitive transactions.

Preservation of Claims Against Merchants

If a consumer wants to preserve his claim against merchants in third party credit granting environment, there is no way to do that where the merchant receives payment instantaneously through a POS terminal, unless you build in the kinds of provisions now in the Uniform Commercial Code and Truth in Lending.

Float

I would not legislate the consumer advantage obtained through deferred payment, namely float, and I would give the initial benefit of that economic gain to the bank. I would hope, however, (and if I had my druthers I would require) that some of this profit be passed along to the customers of the banks by way of reduced charges for the service. On the question of whether the acceptance of EFT would be impaired by the fact that it does not involve a float, I think the answer is "yes", although I do not believe that most customers would articulate this as a reason since they are only generally aware of the phenomenon.

Audit Trail Standards

I don't have enough expertise to know what standards ought to be imposed for audit trails, but I think that bank regulators ought to impose some standards.

Consumer's Management of Their Financial Affairs

I don't think that EFT will decrease the ability of consumer to manage their financial affairs. In fact, it might even increase that ability. I believe that this is a mixed question with a mixed answer and the main thing that needs to be furnished to the consumer is sensible and usable information. This would include:

- (1) Full disclosures of how the system works;
- (2) Hard copy records of transactions from terminals, and
- (3) As much information as possible in monthly statements, etc.

Satisfying Governmentally Mandated Recordkeeping Requirements

On whether the type and nature of records generated in an EFT environment will satisfy governmentally mandated recordkeeping requirements, I am not in a position to answer. However, if there is some short fall in this respect, either the government requirements need to be relaxed or this commission should see to it that the records provided are sufficient, particularly where the principal requirers are other agencies of the federal government, like the IRS.

Signature Substitutes

I don't know what you mean by the question on legally cognizable substitutions for signatures; I suppose any kind of a identifier that is sufficiently unique and individualized ought to suffice. This would include: pin numbers, thumb prints, and possibly some other identifiers as well.

Mandatory Documentation

On your question as to whether it can reasonably be mandated that unmanned terminals devices produce documentation which is prima facie proof of the transaction? I would say "yes", that it can be reasonably mandated that such terminals produce the documentation. However, what is to be prima facie proof seems to me to be a local question of evidence and, I am not sure what the Commission can do about that except to insure that the documentation is sufficient for most federal purposes as indicated in the response to your earlier question.

What Kind of Legislation

As to your final question on page 9. "Assuming the need for legislation in any of the above areas, should such legislation take the form of amendments to existing state or federal legislation or is a separate body of legislation desirable?" I think the answer is probably mixed. Most of what you dealt with under the heading of Rights and Duties of the Consumer can be covered by amendments to the Uniform Commercial Code at the state level. Some things, however, probably could be handled by federal regulations, (such as giving debit card customers the same protections as credit card customers).

I think amending the Code is preferable because there is already a fairly elaborate and effective body of law dealing with a closely related and analogous medium of payment that can be adapted. Also, unless there is a compelling reason, I prefer state over federal legislation, particularly in the commercial law area.

I have nothing to offer on the subject of security, but in respect to Consumer Choice, I would urge steps to retain that choice by legislation in the first instance. The logic of that position requires me to answer your last question by saying that the cost of the continued ability of an employee to demand a check ought not to be borne by the employee, but rather by the employer and/or the paying bank.

Thank you.

224m

QUESTIONS NEEDING ANSWERS--EFFECTS OF
EFTS ON THE U.C.C

Norman Penney*

The purpose of this brief paper is to summarize the problems that need to be addressed if Articles 3 and 4 of the Uniform Commercial Code (but principally Article 4) are to be adapted to regulate Electronic Fund Transfer Systems (EFTS). These questions have been raised previously by a number of commentators and by studies which have been carried out preliminary to the implementation of EFTS projects. The questions take on new urgency because of the accelerating developments in the EFTS field, the appointment of the National Commission on Electronic Fund Transfers, and the work of the Electronic Data Processing Committee of the Permanent Editorial Board for the U.C.C. In 1974, Congress established a National Commission on Electronic Fund Transfers to be made up of representatives of twelve federal agencies having authority over some aspect of banking, fund transfers, or consumer rights; two representatives of state banking authorities; seven representatives of the various elements of the banking industry, and five public members, charged with reviewing all the problems raised by EFTS and recommending appropriate legislative and administrative action.¹ The Commission has only recently been appointed and while the program of the Commission is not yet known, it seems likely that its work will focus particularly on the antitrust, branch banking, and industry structure implications of the new systems.

* ⑤ 1976

The "EDP (Electronic Data Processing) Committee," generally referred to as the "348 Committee", was established by the Permanent Editorial Board to help it determine whether, at this time, the Board should undertake to prepare substantial amendments, or supplements, to Articles 3, 4, or 8 of the Uniform Commercial Code to take into account the impact of EDP on transactions governed by those articles.² In a report submitted in June of 1975, the committee recommended, among other things that the 348 Committee be authorized to undertake the preparation of amendments to Articles 3 and 4, that it be authorized to employ a Reporter to assist it, and that the Chairman of the Permanent Editorial Board be authorized to add additional members to the Committee to broaden its representation.³ As of this writing, a Reporter has not been appointed; however, it seems likely that one will be appointed in 1976, and that work on the revision will commence at that time.

Some Preliminary Questions

In coming to its recommendation, the 348 Committee had to consider a number of preliminary questions. These included: 1. Are the developments in EFTS sufficiently stabilized to warrant codification or regulation at this time? 2. Should this codification or regulation be accomplished by Federal regulation, Federal statute, Uniform State statute, private agreement, or some mix of these and other methods? 3. If the Uniform State statute approach is to be pursued, would it be better to develop a new special statute or amend Article 4 of the U.C.C.?

Despite the many arguments for Federal legislation or regulation, the argument for state action was persuasive to the committee: "namely the existence of a highly technical and well developed uniform body of state law on the subject, the adaption of which to checkless transactions and credit transactions by state action would be cleaner, simpler and perhaps quicker than either uprooting existing state law by a comprehensive federal statute or adopting federal 'amendments' to state law."⁴ The committee stated its view that a "failure to begin a drafting effort at this time would leave a vacuum which [would almost] certainly be filled at the federal level and [might] invite non-uniform state legislation which would [impede] the development of a comprehensive EFTS program."⁵

Current Experimental and Operational Electronic
Fund Transfer Systems

Any discussion of the legal issues raised by EFTS should be made against the backdrop of the particular system or systems which are employed. EFTS is a broad term which has been defined as "any development, project or test which has as its goal the replacement of a portion of the current paper based fund transfer system by means of electronic technology."⁶ In fact, the systems can be categorized or broken into some five or six different types or components.

The Bill-check: Pre-authorized Paperless Entry Debit Transfer

This system began with pre-authorized (by the customer) drafts

drawn by utility and insurance companies on the checking accounts of their customers. The companies were saving postage and extra handling and got the benefit of a larger number of prompt payments. The banks earned service charges and also picked up new depositors, since the paper debit systems normally required that the participating (creditor) companies each maintain an account in the same bank as the customer of the participating utilities and insurance companies to facilitate the transfers. The customer also saved "handling" and postage and got the assurance of having his most critical, recurring bills regularly met, thus avoiding the threat of interruptions of service and policy lapses. In more recent years this type of system has been made partly "paperless" by the substitution of magnetic tapes or punch cards for the paper drafts previously drawn by the companies. The tapes or cards actuate the debits to customer's accounts and the customer receives a report of the transaction rather than a cancelled paper draft.

Direct Payroll Deposit: Paperless Entry Credit Transfers

In this type of system, frequently used by municipalities, school systems, and other large employers, a bank contracts with such employers to make direct deposits to the accounts of their employees of the sums normally transferred by payroll checks. In its original form this system also often required the use of some checks, particularly if more than one employee-depository bank (or transferee) was involved, since the bank of the employer had to have some means for transmitting the payment to banks other than itself for employees maintaining their accounts elsewhere.

There are marketing and legal obstacles to having all the employees of an employer maintain an account in the employer's bank. Here, too, companies have recently begun supplying magnetic tapes to their banks for these purposes or data which enable the banks to prepare the payrolls, i.e., calculate the deductions, prepare the reports, and make the credits or transfers.

The Automated Clearing House (ACH)

This entity is super-imposed upon, or substitutes for, the normal clearing house and is now operative in Atlanta, Los Angeles, San Francisco, Philadelphia, and an increasing number of additional cities. As presently operated, it is simply an agency that receives punch cards or magnetic tapes from the participating banks which originate the debits or credits on behalf of their customers. The Automated Clearing House reorders and redistributes such information to the other banks in the system, making the normal clearing house settlement transactions between the participating banks in the process. It has been the introduction of the ACH that has enabled banks providing the pre-authorized debit and credit services to offer a much more efficient and large scale capability to companies and depositors. In EFTS jargon, the bank which initiates a payroll (credit) transfer on behalf of its employer-company-customer is spoken of as either the "originating bank" or the "transferor bank," and the bank of the depositor employee is spoken of as the "receiving bank" or "transferee bank." In the debit transfer system the bank

of the utility or other company initiating the request or instruction for a debit transfer (comparable to the draft in the predecessor paper phase) is again spoken of as the "originating bank" and the customer's bank, which might be viewed as the payor bank, is again spoken of as the "receiving bank."

Truncation Proposals

Proposals for truncation of the collection process, envisioning the continued use of checks for at least a part of the payment process, are mainly of two types. The first is the type in which the depository bank (the first bank to receive the check for deposit or cash and collection) would retain the check but would transmit the serial number of the check, the information on the payee line, and the amount of the check to the payor bank which would then debit the account of the customer-drawer. The customer-drawer would receive only the transmitted information in the monthly statement. The other, less radical, proposal contemplates the retention of the items by the payor bank, but the supplying of the critical information, as above, to the customer. This latter type of arrangement has been available to large scale checking customers for several years. In these systems and proposals, checks are usually able to be made available to the customers on specific demand.

Point of Sale (POS) and Automated Teller Systems

In its most radical forms, the POS systems would result in immediate debits from the customer's account actuated by instructions entered into the system at a point of sale terminal in the

merchant's store. If operated on a regional or national level, this would relegate the ACH and other regional clearing entities to the role of a switching facility rather than a clearing house performing a discrete function. Such a system would also be capable of carrying credit transfer instructions and furnishing a mechanism for instant loan transactions (on prearranged lines of credit) in much the same way as the bank credit card does today.

In its less radical form, as contemplated by the Atlanta Study, the POS system would instantly generate an advice of credit to the merchant seller, but there would be a second stage for the actual transfer function, following the procedures described in the bill-check or debit transfer system above. A magnetic tape or punch cards would move from the customer's bank to a clearing house (ACH) which would then reprocess the items.

Of all the components or systems, POS is the most variable and will undoubtedly continue in a state of flux, experimentation, and refinement for a number of years to come.

Automated tellers may be of the simple, cash dispensing variety in which a cash card can be used together with a code number to withdraw set, small amounts of cash such as \$25 or \$50 from the machine. Alternatively, this function could be combined with the capability of the machine to receive deposits or grant loans on prearranged lines of credit.

Some Legal Problems of Particular Systems

Bill-check Debit Transfers

Many of the legal questions pertinent here are also relevant to

paperless credit transfer systems, even though the latter do not contemplate "collection." The principal questions appear to be:

1. Is Article 4 appropriate? As indicated above, the "348 Committee" has concluded in the affirmative.
2. Is there an "item" under 4-104(1)(g)? While the Atlanta Study and Homrighausen, writing about the California system, suggest a possible affirmative conclusion,⁷ both Georgia and California have added electronic transfers to the definition of "item" or "instrument" within the meaning of the controlling statute or operating rules.⁸ The Federal Reserve Bank, in its promulgation of proposed revisions to regulation J in 1973, also dealt with the definition problem.⁹
3. What should be provided to accomplish the 4-207, warranty-of-authority function? The principal problem is raised by that section's heavy reliance on the signature of the customer. The California operating rules and the FRB proposed revisions to regulation J have devised new warranties to perform this function.
4. Are sections 4-109, 4-213, and 4-303 adequate to deal with finality in the EFTS context? While two of the steps listed in section 4-109--verification of signatures and affixing a "paid" stamp--would not be applicable to the "completion of the process of posting" in the EFTS context, the rest of that section as well as sections 4-213 and 4-303 appear to be literally applicable to the debit transfer system. The question is whether

the rules provided are appropriate to the paperless system or need some "tinkering."

5. How should the allocation of risks and liabilities be apportioned among the participants in the system in respect to such "breakdowns" as unauthorized issuances, material alteration, or failure to issue items? Much should depend on what kind of system is actually involved and what the functions of the various parties in the system are. Homrighausen has suggested that the receiving bank's possible liability to its depositor includes its responsibility are for: (a) failure to effect a debit or credit after an authorization is accepted, (b) effecting a debit too soon or a credit too late, (c) effecting a debit for more than the debt or a credit for less the amount owed to the depositor, (d) effecting multiple debits to a depositor's account with respect to a single periodic obligation, and (e) effecting a debit or credit without effective authorization.¹⁰

6. Are the standards of care imposed by sections 4-103, 4-202, and 1-201 (19) ("good faith") appropriate and sufficient for EFTS systems?¹¹ In the same vein, section 4-108, excusing delays and other "misfires" caused by acts of God, needs to be examined. How much of the risk of loss for "misfires" will section 4-103 permit the bank to put on the depositor? Should the automated character of the system require a higher degree of "strict liability" on the seller of the service?

7. How should the deferred posting and late return functions of sections 4-301 and 4-302 be provided for? Section 4-301(4) provides that an item is "returned" when it is either delivered

or sent. In what manner is a receiving (payor) bank to "send" or "deliver" an item it has received in electronic form? Would section 4-301(1) permit a return by simply sending a written notice?

8. What provisions need to be made to substitute for or implement the customer's right of stop payment? In the most radical of EFTS systems, POS, payment would be virtually instantaneous, thus making section 4-403 ineffective as a practical matter. However, in the systems now in use in California and Georgia, involving an ACH and a further processing step at the ACH level before the depositor's bank has an opportunity to "act finally," there may be some leeway for such a stop procedure. This concept is also intimately tied to the problem of finality mentioned above. If payments are to be "final" in the EFTS context in a much shorter time than in the current "paper world," it may be necessary to make some provision to permit customers to reverse charges to their accounts in a way similar to stop payment even after "final payment." This may be required in order to satisfy consumer advocates and to gain wider acceptance in marketing the system to the public. The current California system obligates a company in a debit transfer arrangement to furnish the customer with a 7-day notice of a debit entry that differs from the next previous entry relating to the same transactions. This system gives the customer an opportunity to stop the payment if the amount is incorrect or the item is otherwise questionable. In addition, the depositor has 15 days during which he may cause a recredit to his account on furnishing the receiving bank with a

written representation that the entry is in error.¹² What does this do to the "conditional payment" rules of section 3-802?

9. What must be done in respect to section 4-406 if Article 4 is to apply? As has been previously argued, the duty imposed upon the customer to examine statements and returned items and report unauthorized signatures is patently inappropriate since the character of the information furnished to customers will be different with EFTS.¹³ It appears necessary to recast section 4-406 to impose duties on the customer more reasonably related to the new system. Section 4-406 applies most frequently to the problem of a series of forged or altered checks by the same wrongdoer, although there is some duty imposed even in respect to a single item. That section also imposes time constraints upon claims of the customer against the payor bank for "improperly payable" checks. The shortest period is one year for forged indorsements, although this may apparently be further abridged under section 4-103. Is a shorter period, such as the 15 days after receipt or availability of a statement provided under the California operating rules, appropriate? Although some cases under section 4-103 have upheld bank statement legends with similar import,¹⁴ the short time and draconian sanction seem unduly onerous to this writer.

Direct Payroll Deposit (Paperless Credit Transfers)

Many of the questions relating to debit transfers, such as the appropriateness of Article 4, the meaning of the term, "item",

finality, the allocation of risks, stop payment, and the responsibility of the customer to discover and report errors, have some applicability to the paperless credit transfer or direct payroll deposit systems. As indicated above, Article 4 seems generally less appropriate in view of the intention, expressed in the title of the Article itself, to make it applicable to the collection process rather than a system for transferring credits. In addition to such questions common to both types of systems, there are a few questions more specific to credit transfer systems. These include:

1. What provision should be made for the revocation of credit entries¹⁵ and for the equivalent of the "return" contemplated in the normal debit transfer system?¹⁶
2. What should the responsibility of the receiving bank be for prompt crediting to the customer's account and should there be the equivalent of a wrongful dishonor claim for late credits or failure to credit?¹⁷
3. Will state statutes providing for the manner in which wages are to be paid require amendment? An affirmative conclusion on this last question has been drawn in Georgia and California.¹⁸

The Automated Clearing House

Fla.

The legal framework in which the Automated Clearing House is to operate depends heavily on the function to be performed by the clearing house. If it is to be merely a switching facility and a channel or link for communication, it might properly be given less responsibility than is the case in California or Georgia

where the clearing house reorders the tapes and the cards and performs a discrete function in further distributing the debit and credit transfer items. Insofar as the ACH does perform such discrete functions, similar questions to those raised above are involved, such as:

1. What warranties should the ACH give and to whom should they run?
2. What warranties and obligations should run to the ACH and by whom should they be given?
3. What duties and time limitations should be imposed upon the ACH?
4. What rights should the ACH have to enforce its claim for recovery, such as indemnity rights and rights to charge bank balances in its control?¹⁹

Truncation of Items

If the truncation system contemplates the retention of the check or item at the depository bank, how is the payor bank to satisfy its duty to examine its customers' items for "proper payability" under section 4-401 without some special statutory provision?

There is also a question of whether the customer of a bank has a "right" to receive possession of payment items and whether this "right" can be contracted away. If paper items are to be destroyed or retained at a point distant from the depositor, do rules need to be developed to provide the customer with evidence of "payment" of the underlying obligation equivalent to the can-

celled check?²⁰ Finally, how should the risks unique to the truncation systems be dealt with, i.e., inadvertent mistakes in transmitting information? It is, of course, recognized that many of these questions are the same as those posed with respect to the debit transfer and credit transfer systems above, but as mentioned above, truncation systems normally contemplate the continued use, at least in part, of checks.

Point of Sale and Automated Teller Systems

It would appear that most of the significant legal issues arising in these systems also arise in one of the other systems dealt with above, or are of a general character, applicable to all EFTS. It is to be noted, however, that there is a distinct difference between the type of POS system currently operating in California and Georgia, with intermediate processing at the ACH, and the futuristic, fully automated system in which remote instructions result in instantaneous debits or credits to customer's accounts. The rules to be provided for POS systems will have to take this distinction into account. There appear to be relatively fewer problems in devising special rules for automated tellers since most of the transactions will be "on us," i.e., involving only the bank and its immediate customers. There are, of course, some questions to be dealt with, such as: finality, what the "banking day" means in this context, and the apportionment of risks unique to this kind of mechanical and electronic device. At first blush, however, there would seem to be few matters

requiring amendment to the Code.

Conclusion

While the above listing is not exhaustive,²¹ it is hoped that it does include many of the questions that will have to be considered by the Reporter who is engaged to study and draft amendments to Article 4 of the Uniform Commercial Code. There has already been a significant amount of work done in responding to these questions and it is hoped that further responses and suggestions will appear in this Symposium, and elsewhere, in time to be considered by the Reporter and the others who are charged with the responsibility of dealing with these problems.

* A.B. 1950, Yale University; LL.B. 1953, Cornell University; Professor of Law, Cornell University. Professor Penney is a member of the Electronic Data Processing Committee of the Permanent Editorial Board for the U.C.C.

1. 12 USC §§ 2401-08 (Supp. 1974).
2. Electronic Data Processing Committee, Report to The Permanent Editorial Board for the U.C.C. 1 (1975).
3. Id. at 10.
4. Id. at 9.
5. Id.
6. P. Brooke, Electronic Fund Transfer Systems, Two Questions 2 (American Banker Reprint Svc.).
7. Atlanta Fed. Res. Bank, Legal Considerations 19 (6 Research on Improvements of the Payments Mechanism 1972) [hereinafter cited as Atlanta Study]; Homrighausen, One Large Step Toward Less Checks: The California Automated Clearing House System, 28 Bus. L. 1143, 1146-47 (1973).
8. Ga. Code Ann. § 109A-4-104(1)(g) (Supp. 1975); Homrighausen, supra note 7, at 1147-48. See also Fla. Laws, C. 75-73 §1 eff. June 6, 1975
9. 38 Fed. Reg. 32953 (1973). See also the more recent proposed rules in 41 Fed. Reg. 3097 (1976).
10. Homrighausen, supra note 7, at 1149.
11. Comment, 47 Notre Dame L. 1163, 1238 (1972).
12. Homrighausen, supra note 7, at 1151-53.
13. Penney, Bank Statements, Cancelled Checks and Article 4 in the Electronic Age, 65 Mich. L. Rev. 1341, 1358-59 (1967); Cf. Clarke, An Item is an Item is an Item, Article 4 of the U.S.C. and the Electronic Age, 25 Bus. L. 109, 115-16 (1969).
14. New York Credit Men's Adjustment Bureau, Inc., as Trustee v. Manufacturers Hanover Trust Company, 41 A.D. 2d 912(7) (Mem. 1st Dept., 1971).
15. Atlanta Study 59. Cornoi v. Mfrs. Haw. Tr. Co. 16 UCC Rep. 184 (1975) Homrighausen, supra note 7, at 1148-49.

224dd

Accordingly, Subchapter A, Chapter 11, Title 31 of the Code of Federal Regulations is, as of January 1, 1976, amended by the addition of a new Part, designated Part 210, to read as follows:

Sec.	Scope of regulations.
210.1	Definitions.
210.2	Federal Reserve Banks.
210.3	Recipients.
210.4	Program agencies.
210.5	The Government.
210.6	Financial organizations.
210.7	Timeliness of action.
210.8	Death or legal incapacity of recipients or death of beneficiaries.
210.9	Liability of, and acquittance to, the United States.

AUTHORITY: 5 U.S.C. 301, 12 U.S.C. 301; Title 31, U.S.C., and other provisions of law

§ 210.1 Scope of regulations.

This Part governs the making of recurring payments by the Government, by means other than by check, through Federal Reserve Banks and financial organizations to recipients maintaining accounts at such financial organizations.

§ 210.2 Definitions.

As used in this Part, unless the context otherwise requires:

(a) "Federal Reserve Bank" means any Head Office or Branch Office of any such Bank, acting as Fiscal Agent of the United States.

(b) "Financial organization" means any bank, savings bank, savings and loan association or similar institution, or Federal or State chartered credit union, which was affirmatively indicated to a Federal Reserve Bank its preparedness to receive credit payments under this Part.

(c) "Government" means the Government of the United States, the Department of the Treasury, a Federal disbursing office, and a program agency which has made arrangements with the Department of the Treasury to make payments under this Part, or any of them.

(d) "Credit payment" means an order for the payment of money issued by the Government under this Part to pay a recurring payment. A credit payment may be contained on (1) a letter, memorandum, telegram, computer print out or similar writing, or (2) any form of communication other than voice, which is registered upon magnetic tape, disc or any other medium designed to capture and contain in durable form conventional signals used for the electronic communication of messages.

(e) "Payment date" means the date specified for a credit payment. Such date is the date on which the funds specified in the credit payment are to be available for withdrawal from the recipient's account with the financial organization specified by such recipient, and on which such funds are to be made available to the financial organization by the Federal Reserve Bank with which the financial organization maintains or utilizes an account. If the payment date is not a business day for the financial organization receiving a credit payment, or for

the Federal Reserve Bank from which it received such payment, then the next succeeding business day for both shall be deemed to be the payment date.

(f) "Recipient" means a person entitled to receive recurring payments from the Government.

(g) "Beneficiary" means a person other than a recipient who is entitled to receive the benefit of all or part of a recurring payment from the Government.

(h) "Recurring payment" means any Federal Government benefit, annuity, or payment (or allotment therefrom), including any payment of salary, wages,

(i) "Program agency" means any agency which makes recurring payments, and includes any department, agency, independent establishment, board, office, commission or other establishment in the executive, legislative, or judicial branch of the Government, any wholly-owned or controlled Government corporation, and the municipal government of the District of Columbia.

(j) "Standard Authorization Form" means the authorization form prescribed by the Department of the Treasury for the recurring payment for execution by (1) a recipient, and (2) a financial organization maintaining an account for such recipient.

§ 210.3 Federal Reserve Banks.

(a) Each Federal Reserve Bank as Fiscal Agent of the United States shall receive credit payments from the Government and shall make available and pay such credit payments to financial organizations, and shall otherwise carry out the procedures and conduct the operations contemplated under this Part. Each Federal Reserve Bank may issue operating circulars (sometimes referred to as operating letters or bulletins) not inconsistent with this Part, governing the details of its credit payment handling operating and containing such provisions as are required and permitted by this Part.

(b) The Government by its action of issuing and sending any credit payment contained in the media specified in § 210.2(d) hereof shall be deemed to authorize the Federal Reserve Banks (1) to pay such credit payment to the debit of the general account of the United States Treasury on the payment date, and (2) to handle and act upon such credit payment.

(c) Upon receipt of a credit payment, a Federal Reserve Bank shall, if the credit payment is directed to a financial organization which maintains or utilizes an account on the books of another Federal Reserve Bank, forward such credit payment to such other Federal Reserve Bank. The Federal Reserve Bank on whose books the financial organization or its designated correspondent maintains an account shall deliver or make available such credit payment to such financial organization not later than the close of business for such financial organization on the business day prior to

the payment date on the medium as agreed to by such Federal Reserve Bank and financial organization.

(d) A financial organization by its action in maintaining or utilizing an account at a Federal Reserve Bank shall be deemed to authorize that Federal Reserve Bank to credit the amount of the credit payment to the account on its books of such financial organization or its designated correspondent maintaining an account with the Federal Reserve Bank.

(e) A Federal Reserve Bank receiving a credit payment from the Government shall make the amount of such credit payment available for withdrawal from the account on its books, referred to in § 210.3(d) above, at the opening of business on the payment date.

(f) Each Federal Reserve Bank shall be responsible only to the Department of the Treasury and shall not be liable to any other party for any loss resulting from such Federal Reserve Bank's actions under this Part.

§ 210.4 Recipients.

(a) In order for a recipient to receive a recurring payment by means of direct deposit of the amounts of credit payments under this Part, at a financial organization of the recipient's choosing and to an account the title of which includes the recipient's name, the recipient shall execute the applicable portion and deliver to such financial organization the Standard Authorization Form prescribed by the Department of the Treasury for such recurring payments. A recipient shall be responsible for any inaccuracy in the data entered by such recipient on such Standard Authorization Form.

(b) In executing a Standard Authorization Form, a recipient (1) designates the financial organization and the account on the books of such financial organization to which the amounts of the credit payments shall be credited, (2) is deemed to agree to the provisions of this Part, and (3) authorizes the program agency to terminate any previously executed Standard Authorization Form or any other inconsistent payment instructions applicable to the relevant recurring payment.

(c) A recipient shall execute a separate Standard Authorization Form for each type of recurring payment made hereunder. If a recipient wishes to direct a recurring payment to a different account or financial organization, the recipient shall execute a new Standard Authorization Form.

(d) A recipient may at any time authorize the program agency to terminate a Standard Authorization Form by notifying such program agency.

(e) The death or legal incapacity of recipient or the death of a beneficiary shall terminate a Standard Authorization Form issued with respect to a recurring payment.

(f) A recipient of a recurring payment may request only that a credit payment be in the full amount of such recurring

payment and be credited to one account on the books of a financial organization. Except as authorized by law or other regulations, the procedures set forth in this Part shall not be used for effectuating an assignment of a recurring payment.

(g) A recipient may be required by local law or by financial organization procedures to have the execution of a Standard Authorization Form notarized.

(h) A change in the title of an account on the books of a financial organization which (1) removes the name of the recipient, (2) removes or adds the name of a beneficiary, or (3) alters the interest of the beneficiary in the account shall terminate any Standard Authorization Form in which that account is designated, and shall require the execution of a new Standard Authorization Form before further credit payments may be credited to that account.

§ 210.5 Program agencies.

The program agency will maintain the data necessary for authorization of credit payments and shall make such data available for the issuance of such credit payments in sufficient time for the Government, in performing its disbursing function, to carry out its responsibilities under this Part. Such data shall be certified by the program agency's certifying officer in accordance with 31 U.S.C. 82c.

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

CHAIRMAN WIDNALL: I think we ought to decide to
take a five minute break at this point to stand up and stretch.

And then we have two sets of witnesses coming on
right after that.

(Recess.)

CHAIRMAN ATWATER: May I have your attention,

1 please.

2 We are going to reassemble.

3. This announcement is for the Commissioners.

4 There will be material for tomorrow's meeting in
5 Room 2129 which is right next door, so on your way
6 out to the cab or car, I would appreciate it if you would
7 pick up that material. It will save the staff some
8 manipulation to get it to you.

9 CHAIRMAN WIDNALL: The next witnesses are
10 Karen Hayes, Fritz Biermeier, and Thomas K. Zaucha, speaking
11 on behalf of the Joint EFT Committee of the National
12 Association of Food Chains and the Supermarket Institute.

13 (Witnesses sworn.)

14 TESTIMONY OF KAREN HAYES, FRITZ BIERMEIER, AND
15 THOMAS K. ZAUCHA, JOINT EFT COMMITTEE, NATIONAL
16 ASSOCIATION OF FOOD CHAINS AND SUPERMARKET
17 INSTITUTE.

18 MR. BIERMEIER: Good afternoon. My name is
19 Fritz Biermeier, and I'm Vice President of Supermarkets
20 General Corporation, Chairman of the Joint National Association
21 of Food Chains and Supermarket Institute's EFT Committee.

22 On my immediate left is Karen Hayes, Director of
23 Consumer Affairs for Stop & Shop Companies, and a member of
24 our Electronic Funds Transfer Committee, and also a member of
25 the National Association of Food Chains Consumer Affairs

1 Committee.

2 On my far left is Tom Zaucha, Director of Public
3 Affairs for the National Association of Food Chains.

4 For those of you who are not familiar with our
5 industry, the National Association of Food Chains is a
6 supermarket institute of two organizations which will shortly
7 merge into an organization called the Food Marketing Institute.

8 The combined membership of those two organizations
9 will represent better than one hundred billion dollars in
10 food retail sales in the United States.

11 The membership ranges from the largest retail
12 food chains in the country down to single store operators.

13 Just last spring, recognizing the need to address
14 issues in electronic funds transfer for the food industry,
15 the National Association of Food Chains and SMI created the
16 Joint Electronic Funds Transfer Committee.

17 The organization structure represents many
18 disciplines of the food industry, including chief financial
19 officers, chief executive officers and technical disciplines
20 within the organizations.

21 We immediately moved to surface issues in the
22 area of electronic funds transfer, attempt to establish
23 guidelines, educate our constituency, and finally to
24 communicate -- which is part of the reason why we are here
25 today -- our concern about the proliferation of retail

1 EFT networks, without the benefit of retail or consumer
2 input, has moved our committee to study some major issue areas.

3 These areas are economic issues, system
4 design issues, systems performance issues, security and
5 legal issues, communications issues, and social impact.

6 The focus of these major areas of examination
7 have uncovered two significant points to our committee.

8 The first of these is that each of the six areas
9 are characterized by questions which pertain
10 particularly to the consumer participation on an electronic
11 funds transfer system.

12 And the second

13 is that we did not find any compelling economic reasons for
14 retailers to install such systems. Hence, the work of our
15 committee has migrated towards the position that in order
16 for an electronic funds transfer to have a reasonable chance
17 of success, it must have lasting benefits to our consumers.

18 Having examined the Commission's list of issues,
19 we have chosen two areas that we felt would assist the
20 Commission towards better understanding of the consumer point
21 of view.

22 We have been encouraged with the staff work of
23 the Commission servicing issues particularly in the areas of
24 security, liability, privacy and consumer rights. However,
25 we felt the commission and the consumer would benefit most

from a concentration by our committee on the issues
1 of convenience and choice.

2 We have, therefore, prepared a document for
3 today's testimony to the Commission, and Karen
4 Hayes will present that document now. It represents input,
5 not only from our committee, but substantial input from the
6 Consumer Affairs Committee of the National Association of
7 Food Chains.

8 Karen?

9 MS. HAYES: Thank you.

10 Just to elaborate a little bit, I do represent
11 here over 70 consumer affairs specialists with various
12 chains across the country, and just to give you an idea, we
13 see our expertise as knowing and interpreting consumers' wants
14 and needs for our company. That is our function.

15 I am here representing about 70 of these
16 consumer affairs specialists with supermarket chains.

17 As Mr. Biermeier said, my purpose today is to
18 share with you some of our concerns related to the impact of
19 EFT on the consumer.

20 Our committee has spent considerable time discussing
21 this topic, and feels that our interests and those of the
22 consumer are virtually the same in this area. The reason for
23 this commonality of interest, and it is probably apparent,
24 is that the consumer is also our customer. We want to be sure
25 that if and when EFT services are offered in our supermarkets,

1 they do not adversely impact our customers.

2 Our business is extremely competitive. We
3 continually strive to build sales volume through providing
4 the best customer value and service. If EFT reduces our level
5 of service or raises our costs, then both customers and
6 retailers will be less well off.

7 We have identified a number of ways that EFT is
8 likely to affect the consumer and feel that by selecting
9 the issues of security, privacy, consumer rights and duties,
10 convenience and choice, as Mr. Biermeier mentioned before,
11 you have picked the most important ones for inclusion in
12 this hearing.

13 I plan to limit my brief remarks to a consideration
14 of only the last two, convenience and choice. The other
15 areas are, of course, important, but have already received
16 considerable attention from a number of consumer interest
17 groups.

18 For this reason, I am sure that they will be dealt
19 with thoroughly before this hearing. The subjects of
20 consumer convenience and choice, by contrast, have not, to
21 our knowledge, received the same level of attention.

22 These two areas are of particular concern to the
23 supermarket customer and for this reason we feel they deserve
24 a more thorough discussion.

25 Let's begin with a look at the issue of convenience.

1 The act of making financial services more available may appear
2 to be adding more convenience, and I believe that it does.

3 But how much does that convenience benefit the customer?

4 This may sound like a silly question, but we have
5 already heard customers asking, "Why should I change my way of
6 doing things just to permit the banks and supermarkets to
7 benefit?"

8 Our experience with the introduction of UPC
9 scanning has clearly indicated that the customer is able to
10 determine whether or not a new innovation provides consumer
11 benefits. If the customer does not award significant value
12 to EFT, then it is likely to be ignored.

13 Our limited research on this subject tends to
14 indicate that the consumer is fairly satisfied with the
15 current payment system. While the current system is far
16 from perfect, let's take a look at the convenience that it now
17 provides.

18 There are nearly 32,000 supermarkets in the U.S.
19 and each one of these stores is open at least six days a
20 week. In many areas, Sunday openings are also common.

21 Each week, the typical supermarket cashed checks
22 with a value equivalent to 85 percent of its sales.

23 These stores currently are able to handle several
24 payment systems. For example, a recent survey indicated that
25 more than 30 percent of the customers pay for their groceries

1 by check most of the time, while 50 percent never pay by
2 check.

3 The supermarket already tends to be a place where
4 shoppers do other financial chores. For instance, 17 percent
5 cash their paychecks and 5 percent pay utility bills while
6 they do their shopping.

7 But at the same time, customers are concerned
8 about service. Surveys have historically shown that the number
9 one complaint about supermarkets involves service at the
10 checkout. One recent study reported that the typical consumer
11 estimated that he or she waited fully 9 minutes in line at
12 the checkout lane. Naturally, this figure varies greatly
13 depending on the time of day and the day of the week, but the
14 point remains that it is the checkout operation, including
15 the tendering time, that is currently the most frustrating
16 aspect of the supermarket.

17 A major open question from the consumer is how will
18 EFT affect my waiting time in the store? Even if the customer
19 can handle more financial transactions through EFT at the
20 supermarket, the value of this convenience will be diminished
21 substantially if EFT causes delays or additional waiting
22 lines.

23 Beyond the effect of EFT on the current level of
24 service, customers are wondering what new effects EFT may have
25 on customer convenience, especially in comparison with current

1 payment systems.

2 For example, will EFT permit the customer to manage
3 the money in his or her checkbook in the same way it is done
4 presently? Our preliminary research showed that about 20
5 percent of those interviewed occasionally take advantage of
6 the float in their checkbooks. If EFT deprives these
7 customers of that option, we can expect some resistance.
8 Experience has shown that it is never easy to take something
9 away from an individual.

10 Will the mechanics of using EFT be simple and
11 understandable to the average shopper? As designers of the
12 system strive to meet requirements for security and privacy,
13 will it be possible to keep the system adequately simple so
14 as to not exclude less literate or technically competent
15 consumers?

16 Most important of all, who will educate the
17 customer about EFT and how will the customer inquire or
18 complain about the performance of the system? The customer
19 needs the opportunity to obtain adequate information about
20 the performance of the system and to register concerns and
21 complaints.

22 Without this feedback mechanism, the customer
23 will have no way to affect the EFT system.

24 Convenience of EFT ultimately will be determined
25 by the effect of the new system on customer's ability to

1 accomplish his or her own objectives. Today we find a
2 situation, at least in supermarkets, where the current
3 payment system appears to be relatively effective in meeting
4 the customer needs.

5 We are, therefore, concerned that EFT be designed
6 in a way to speed the financial transactions without
7 increasing the customers waiting time, increasing the
8 complexity of the process and eliminating the opportunity
9 for the customer to interact easily with his or her financial
10 institution.

11 In the last analysis, consumers want no more
12 hassle from EFT than they receive from the current system
13 and hopefully less.

14 Choice, like convenience, is an issue of significant
15 importance to our customers. Food retailing operates on
16 the premise that the consumer should be provided with adequate
17 information on which to make an informed choice among the
18 products and services that are offered in the marketplace.

19 This same principle, in our judgment, extends to
20 both the development and design of EFT.

21 What are some of the choices that customers have
22 today which must be kept in mind in developing an EFT system?

23 The choice of payment system. Today, the customer
24 can pay for his or her groceries with cash, check, and in some
25 instances, even a credit card.

1 It is in the consumer's best interest to have a
2 ready access to these other payment systems for a fairly
3 long period of time. While there are many positive aspects of
4 EFT, there is a need to maintain the customer's options while
5 this new payment system is evolving.

6 The choice of financial institution. The consumer
7 can today choose a financial institution independently of
8 the choice of a supermarket, and it is in the interest of the
9 consumers to maintain that separation.

10 Retailers don't want to influence their customer's
11 choice of financial institution any more than they want the
12 financial institutions to dictate the choice of supermarkets.
13 An EFT system should be universal in the sense that all
14 customers can gain access to the services, regardless of
15 where they bank.

16 Choice of store. Nearly 9 out of 10 consumers
17 regularly shop at more than one supermarket and the customer's
18 ability to choose the store at which he or she shops is of
19 utmost importance.

20 An EFT system that hinders this choice will
21 clearly penalize the customer.

22 Consumers recognize that high costs make it
23 impossible to provide unlimited choice, but they feel that they
24 are entitled to some choice or a clear and persuasive
25 explanation as to why a choice is not possible.

1 If the emerging EFT system will require or
2 cause a change in the set of choices currently facing the
3 customer, then there will be a real need to explain this
4 to the customers. To reduce the choices without adequate
5 justification could cause a serious pitfall.

6 In conclusion, it appears that there is a good
7 chance that the emerging EFT system could have as significant
8 an impact on the consumer's convenience and choice as it
9 will on the better publicized issues of privacy and security.

10 For this reason, we would encourage you to look
11 even more carefully into your future deliberations at these
12 two areas, as the decisions on these matters will regularly
13 affect millions of customers.

14 Since we also have a strong interest in these
15 areas, we would like to volunteer, if you desire, to keep
16 you apprised of what we learn on these issues from our
17 regular dialogue with customers.

18 It is clearly in the consumer's best interest to
19 keep you informed of what's happening in the stores.

20 Thank you.

21

22

23

24

25

1 CHAIRMAN ATWATER: Thank you.

2 MR. BIERMEIER: We strongly believe that the material
3 being presented here today represents just the tip of the ice-
4 berg. We certainly in the supermarket industry have comments to
5 be made in a number of different areas for other subcommittees
6 of the Commission and hope to do so in the future. But we
7 really believe that the Commission must continue to research and
8 assure that all unanswered questions in the consumer forefront
9 are resolved, because without the consumer, in the retail EFTF
10 environment, you have no system at all.

11 CHAIRMAN ATWATER: Mr. Green.

12 MR. GREEN: I certainly like what you say, Ms. Hayes,
13 and would agree with virtually all of your points. I just
14 wonder if you have talked with the people at the
15 Smith supermarket chain out in Glendale about how this is
16 speeding up or slowing down the processing of people who are
17 buying groceries and checking out at the checkout stands--I
18 am talking about the Glendale Federal operation.

19 MS. HAYES: I am not personally familiar with that
20 chain. I don't know if either Tom or Fritz is familiar with
21 that chain. I think it is too early to tell how consumers will
22 be reacting.

23 There are individual experiments going on, and we
24 will be keeping close contact with these individual experiences.
25 But I'm not familiar with that particular chain.

1 MR. GREEN: This particular operation has the
2 point-of-sale terminal right at the checkout stand, as
3 opposed to the convenience counter. So it is something that
4 your comments seem to address.

5 MR. BIERMEIER: Perceptions may be quite different
6 from the actual fact. And in particular, I have perceptions
7 in relationship to the Glendale format which, I believe,
8 engineering data would tend to justify. When you add to the
9 payment cycle the insert of a card, a handshake with telephone
10 line, an insert of a PIN number, creation of a document and
11 solicitation of customer signature, you are replacing only
12 something like 25 percent of the sales accomplished by signing
13 a check or exchanging of cash, that the electronic transfer
14 in Glendale will take more time to process.

15 MR. ZAUCHA: And just to emphasize the significance
16 of this question, that in a number of tests that have been
17 run, next to the price of food, the next major consumer com-
18 plaint is the time they spend in the checkout line. And that
19 has been one of the major impetuses with the Universal Product
20 Code and the scanning system. So our primary orientation at
21 the supermarket industry is to remove that significant consumer
22 complaint of waiting time as they are checking out. That is
23 an important tradeoff that I think we are going to take a
24 good look at: does an EFT transaction, in fact, slow down or
25

1 hasten up the integration with the UPC scanning system. And I,
2 do think that the testimony presented by the National Consumer
3 Information Council in saying that consumer's reaction is still
4 uncertain, pretty much reflects whether the added EFT service
5 is worth no increase in time or an increase in the amount of
6 time to check out your food.

7 CHAIRMAN ATWATER: Mr. Wegner.

8 MR. WEGNER: Thank you, Mr. Chairman.

9 Commissioner Green and I had an opportunity to
10 cross the country on a trip we
11 made to five different cities with part of the Commission staff
12 to look at various kinds of installations at work. I think
13 there is a truism at work here that bears on the business of
14 research. In consumer areas it is very difficult
15 and very risky to make estimates about what the consumer is
16 going to accept before the consumer has had a chance to play
17 around with the product.

18 I basically believe that an objective judgment can
19 be made. Several very large and important
20 institutions have told us this, that, "well, you can make judg-
21 ments that it looks good to you and you like it and
22 you're comfortable with it after playing around with it," and
23 chances are it will gain consumer acceptance. I don't
24 think it is basically that hard a problem. I think EFT has
25 an enormous amount to offer this country in terms of greater

1 security, in terms of the consumer benefits of time and place
2 choices in the field, in terms of speeding up the checkout line.
3 Also, despite what I understand in your program are union
4 problems about location and labor and so on, I think one of
5 the end products of EFT overtime will be an increase in the
6 number of jobs available. Of course, there will be disloca-
7 tions. This is the price of progress. I despair when I think
8 what this Commission would be facing were it to be considering
9 at this moment, instead of electronic funds transfer, the
10 question of introducing electricity into private homes. You
11 can imagine the arguments that would be made against the danger
12 to children and that sort of thing. Or, heaven forbid, if we
13 were to recommend legislation on whether or not the first air-
14 plane should lift off from a turf field somewhere. You know,
15 a case could be made that that should never be allowed to
16 happen.

16 And I think, in looking at the minutia of problems,
17 we tend to get myopic about the many benefits and the fine
18 tuning of acceptance and that sort of thing. This isn't much
19 of a question -- it has turned out to be a speech. Forgive
20 me. But I basically believe there are terrific consumer goods
21 in this thing, and I think you people have done an exceptional
22 job on a low-margin industry to bring benefits
23
24
25

1 to the consumer by the virtue of the fact that you exist,
2 first of all; and I hope you continue in your implementation and
3 experimentation with EFT because we stand to learn from it.

4 MR. ZAUCHA: Mr. Wegner, if I might just comment,
5 having testified in the same room in front of different
6 committees, we would sure like to have you come back and tell
7 some other people about the profit margin of our industry, and
8 I can assure you that we do share your enthusiasm about
9 technological change and improved productivity, not only for
10 the supermarket industry but for the financial institutions,
11 as well.

12 And we also, I think, share your caution in making
13 any prejudgments about what ultimately the consumers' reaction
14 will be about either EFT or UPC, for that matter. Both, I
15 think, developments are unique. They provide a new opportunity
16 for consumers. And we are reacting to UPC with that same
17 caution of how a consumer reacts. In the first month we had
18 better see how they react -- twelve months later -- our concern
19 is that in these early stages that we indeed look at our
20 installations from a test standpoint so that we can get as much
21 consumer input as feedback into our system before making any
22 long-term commitments.

23 MS. HAYES: I would just like to elaborate on that.

24 I think you pointed out consumers' need to see it
25 and work with it. I think part of my job and others like me is

1 to get the people who design the system and the people who use
2 the system in touch with consumers. They are out there. We
3 personally can get our hands on a thousand people to talk to
4 and to get initial feedback, and I think you have to get it in
5 all stages. But you have to get it right in the beginning, and
6 they have to be included in from the very beginning.

7 CHAIRMAN ATWATER: Ms. Koplow.

8 MS. KOPLOW: I have questions on your studies.

9 First of all, did your study reveal any psychological
10 effect on consumers such that they would have a tendency to spend
11 more using a debit card?

12 MS. HAYES: I think it can't. It's too early to
13 tell. They may have
14 some fears along that line, but I think it is too early to tell,
15 from what I can see.

16 MS. KOPLOW: The other question deals with the
17 matter of convenience. Has there been any reaction to
18 that sort of one-stop shopping -- you can deposit money,
19 you can make withdrawals, you can pay your bills as well as do
20 your marketing all at one time in one place. Has there been
21 any reaction to that kind of convenience?

22 MR. ZAUCHA: It's hard to get over the primary
23 psychological experience of going shopping for food -- the
24 consumer has integrated the cost benefit of these other trans-
25 actions -- whether or not -- I don't know whether we would

1 want to say anything on that at the moment.

2 MR. BIERMEIER: I think it's important to understand
3 the message we are trying to bring across to you today, and that
4 is, we believe the impetus of the food industry is for greater
5 productivity, the satisfaction of certain customer issues on
6 price and on making the shopping experience pleasant but
7 swift. If you were standing in a line at one of our super-
8 markets and the customer in front of you was paying three bills
9 and depositing something in an account, and trying to get some
10 cash out and pay for the groceries, you're not going to be very
11 happy if that takes ten minutes.

12 I can tell you that the trend in the supermarket
13 industry is now to have courtesy counters to cash checks,
14 because the new electronic equipment that we are installing in
15 our stores allow us to do negative and positive lookups of
16 check authorization at the checkout.

17 So what we're talking about is providing these
18 services, but in order to do that we are going to have to man
19 the stores with additional hours and people, and I think you
20 should recognize that when a service has a cost, that cost has
21 to be passed on to someone.

22 MR. ZAUCHA: Ms. Koplow, if I might just add one
23 other point to your first question, I do understand that there
24 has been one study completed by a consumer organization that
25 says that, no, not necessarily customers come into the

1 supermarket and buy more, but they come in and make their
2 financial transaction and take the money and go into the mall
3 next door and spend it. So that kind of concerns us, too.

4 CHAIRMAN ATWATER: We have time for one more
5 question.

6 Mr. Rogers?

7 We have time for two more questions.

8 MR. ROGERS: I guess I'm not really quite clear yet
9 on your specific recommendations as to what we ought to
10 be studying here and the priorities we ought to give it.
11 Maybe I could ask two questions which might clarify that for
12 me.

13 My first question is: Would it not still be within the
14 retailer's power in his decision as to what alternative modes
15 of payment he would offer to his customers, be it debit card,
16 credit card, cash, check or even barter?

17 And the second one, somewhat related to that, is it
18 not the supermarket's economic decision, as to getting into
19 these systems after they make their own study as to whether
20 or not it provides the convenience or whatever they are looking for
21 in terms of their bottom line profit?

22 MR. BIERMEIER: I think that is a normal course of
23 action that you would expect under a free enterprise system.

24 Unfortunately, in the early installations of
25 electronic funds transfer systems around the country, the

1 financial institutions, as we see it, see the opportunity to
2 gain a share of the market. Because of that, they don't
3 generally prepare and present all of the economic factors
4 involved in the installation of electronic funds transfer
5 systems in a particular store.

6 For example, is that particular terminal and the
7 cost inherent in it actually carrying its weight in terms of
8 additional deposits, et cetera.

9 I guess one of the things we are concerned about is
10 the overall value to society of adding in these types of
11 electronic funds transfer terminals; and being in a position in
12 1982 with customers substantially converted to such a system,
13 our numbers of customers that we normally would have had in a
14 cash or check environment, are now being confronted with the
15 fact that hidden in that total system has been an 80-cent
16 transaction cost that we are now being asked to pick up. And
17 what choice do we have if our customers are out of a card or
18 have another system and say, "I'm sorry, we cannot do electronic
19 funds transfer for you," or "You will have to pay 80 cents."
20 Then the customer says, "I don't care to pay 80 cents," and
21 someone opens down the street and says, "Well, we will absorb
22 that cost," and someone opens elsewhere and says, "If you
23 pay cash, we will sell cheap," and all of a sudden, the system
24 collapses. As a society we have put a lot of money into
25 it, and we've dislocated a lot of customers, and what is the

1 value of the system?

2 MR. ZAUCHA: Plus let me answer that same question in
3 a little different vein, that the hearings we have here are
4 on consumer issues and consumer concerns, and, indeed, I think
5 retailers, food retailers in particular, have some very hard
6 decisions to make based on those
7 consumer concerns. Our purpose in communicating to you is
8 that in your final judgments and resolutions, your
9 recommendations will also reflect the same consumer concerns
10 that we have talked about today.

11 CHAIRMAN ATWATER: Mr. Benton. No. Governor
12 Mitchell.

13 MR. MITCHELL: I have always thought of the food
14 industry as being one that was extremely conscious of its costs,
15 and yet when I tried to find out--indirectly, I must say--how much
16 it costs you to have cash as a method of settlement compared
17 to checks as a method of settlement, I have not been able to
18 gather any information at all.

19 Now, do you have such information, and could you
20 supply it to us?

21 MR. BIERMEIER: We have that portion of that cost
22 that we bear.

23 MR. MITCHELL: I would be very interested in that,
24 because I think it is germane in a consumer-oriented economy
25 for the consumer to know whether he is using a method of

1 settlement that costs ten times as much as any other method of
2 settlement. It might not make very much difference in his bill,
3 but it might make a great deal of difference to you which one
4 he opts for.

5 MR. BIERMEIER: There is no question that each of
6 the payments systems have inherent in them certain costs
7 of operation.

8 MR. MITCHELL: Well, I would think that our general
9 feeling is that the hidden costs of cash are much higher than
10 any other system.

11 MR. ZAUCHA: Governor, we will provide followup
12 information for the record and for the Commission. And I might
13 add that, in talking to Esther Peterson on the break, she wants
14 to know how many times you make it a habit to buy
15 groceries and then stop/payment on your
16 check.

17
18
19
20
21
22
23
24
25

1 CHAIRMAN ATWATER: Mr. Anderson.

2 MR. KENNETH ANDERSON: Just one question. As I
3 take it, you see vis a vis consumer convenience the importance
4 of that little black box in the store, the terminal, being
5 shared and susceptible to accomodating a variety of different
6 systems; is that correct?

7 MS. HAYES: Yes.

8 MR. BIERMEIER: We are really competing in the field
9 of distribution of food and would not like to be in a posi-
10 tion where we are competing as to which financial institu-
11 tion services we happen to offer.

12 CHAIRMAN ATWATER: Mr. Benton.

13 MR. BENTON: First, we would like to accept your
14 offer of providing us with some results from your consumer
15 research, as you said before. I just wanted to get that on
16 the record.

17 And I would like to ask a question, which goes back
18 a little bit to what Commissioner Anderson was just referencing.

19 Your industry has spent significant amounts of monies
20 building some of the most effective check control systems
21 that exist anywhere in the country. At the same time, not-
22 withstanding your desire to see EFTS universal, we all know
23 that for many months, if not years, to come it will not be
24 put in by a pioneering organization as is the case
25

1 all around the country today. Thirdly, I would further
2 assume that your industry has no intentions of ever
3 intentionally turning away customers because they do not have
4 access to those systems. Which leads me, therefore, to this
5 question, which deals with a little bit of social cost, and
6 that is, I am wondering how you deal with the fact that you
7 basically are going to end up with two different kinds of costs
8 of business as time goes on: one cost of doing business with
9 the customer who comes in with a card and who shares in the
10 benefits and price of your electronic systems, and
11 the second customer who is not banking at the same bank or
12 doesn't have access to that system and comes in with paper, and
13 that is reflected in your cost of paper control.

14 You have now doubled your check control systems
15 cost. The benefits are not there to cover that, from what I
16 have seen.

17 So the question is: How do you get out of it? Are
18 you ultimately going to end up in a situation where
19 you are going to be turning away high-risk, paper-based
20 customers? High-risk customers who come in with paper five
21 years from now after the penetration of electronics has
22 become significant?

23 MR. BIERMEIER: I guess our response to that is that
24 we are looking for a system, an electronic funds transfer
25 or any other type of payment system where the consumer feels

1 that the cost that they are incurring in entering in and trans-
2 acting in that system is commensurate with the services they
3 receive.

4 And when you talk about the fact that we will have
5 two different types of cost, one for a card-based system, one
6 for a paper-based system, if in fact the costs are open and
7 clear to the consumer and what is being incurred either in the
8 cost of food or in the cost of the transaction are clear and
9 they are willing to accept those costs, based on their under-
10 standing of the service they receive, we have a system that is
11 viable and workable.

12 CHAIRMAN ATWATER: We thank you very much for your
13 excellent testimony, and we appreciate your providing the
14 information now and later. Thank you.

15
16
17
18
19
20
21
22
23
24
25

National Commission on Electronic Fund Transfers
Users Committee Public Hearings
"Consumers Issues in EFT"
October 26 and 27, 1976
Washington, D.C.

The documents which follow are submitted for the record
of this hearing by:

National Association of Food Chains/
Supermarket Institute Joint Committee
on EFT

Testimony
before
National Commission on Electronic Fund Transfer
Presented by
Karen Hayes, Director of Consumer Affairs
The Stop & Shop Companies, Inc.
October 26, 1976

Good morning. My purpose today is to share with you our experiences and concerns related to the impact of E.F.T. on the consumer. Our committee has spent considerable time discussing this topic and feels that our interests and those of the consumer are virtually the same in this area. The reason for this commonality of interest, and it is probably apparent, is that the consumer is also our customer. We want to be sure that if and when E.F.T. services are offered in our supermarkets, they do not adversely impact our customers. Our business is extremely competitive. We continually strive to build sales volume through providing the best customer value and service. If E.F.T. reduces our level of service or raises our costs, then both customers and retailers will be less well off.

We have identified a number of ways that E.F.T. is likely to affect the consumer and feel that by selecting the issues of security, privacy, consumer rights and duties, convenience, and choice, you have picked the most important ones for inclusion in this hearing. I plan to limit my brief remarks to a consideration of only the last two areas, i.e. convenience and choice. The other areas are, of course, important but have already received considerable attention from a number of consumer interest groups. For this reason, I am sure that they will be dealt with thoroughly before this hearing. The subjects of consumer convenience and choice, by contrast, have not, to our knowledge, received the same level of attention. These two areas are of particular concern to the supermarket customer

and for this reason, we feel they deserve a more thorough discussion.

Let's begin with a look at the issue of convenience. The act of making financial services more available may appear to be adding more convenience, and I believe that it does. But how much does that convenience benefit the customer? This may sound like a silly question, but we have already heard customers asking, "Why should I change my way of doing things just to permit the banks and supermarkets to benefit?" Our experience with the introduction of scanning has clearly indicated that the customer is able to determine whether or not a new innovation provides consumer benefits. If the customer does not award significant value to E.F.T., then it is likely to be ignored or even worse....boycotted.

Our limited research on this subject tends to indicate that the consumer is fairly satisfied with the current payment system. While the current system is far from perfect, let's take a look at the convenience that it now provides. There are nearly 32,000 supermarkets in the U.S. and each one of these stores is open at least six days a week. In many areas, Sunday openings are also common.

- Each week the typical supermarket cashed checks with a value equivalent to more than 85 percent of its sales.
- These stores currently are able to handle several payment systems. For example, a recent survey indicated that more than 30 percent of the customers pay for their groceries by check most of the time, while 50 percent never pay by check.
- The supermarket already tends to be a place where shoppers do other financial chores, i.e. 17 percent cash their paychecks and 5 percent pay utility bills, etc. while at the grocery store.

But at the same time, customers are concerned about service. Surveys have historically shown that the number one complaint about supermarkets involves service at the checkout. One recent study reported that the typical customer estimated that he or she waited fully 9 minutes in line at the checkout lane. Naturally, this figure varies greatly depending on the time of day and the day of the week, but the point remains that it is the checkout operation, including the tendering time, that is currently the most frustrating aspect of the supermarket. A major open question from the customer is, how will E.F.T. affect my waiting time in the store? Even if the customer can handle more financial transactions through E.F.T. at the supermarket, the value of this convenience will be diminished substantially if E.F.T. causes delays or additional waiting lines.

Beyond the effect of E.F.T. on the current level of conveniences, customers are wondering what new affects E.F.T. may have on customer convenience. Will E.F.T. be convenient to use in comparison with current payment systems? For example:

- Will E.F.T. permit the customer to manage the money in his or her checkbook in the same way it is done presently?

Our preliminary research showed that about 20 percent of those interviewed occasionally "play the float" in their checkbooks. If E.F.T. deprives these customers of that option, we can expect some resistance. Experience has shown that it is never easy to take something away from an individual.

- Will the mechanics of using E.F.T. be simple and understandable to the average shopper? As designers of the system strive to meet the requirements for security and privacy, will it be possible to keep the system adequately simple so as to not exclude less literate or technically competent customers?

- Who will educate the customer about E.F.T. and how will the customer inquire or complain about the performance of the system? The customer needs the opportunity to obtain adequate information about the performance of the system and to register concerns and complaints. Without this feedback mechanism, the customer will have no way to affect the E.F.T. system.

Convenience of E.F.T. ultimately will be determined by the effect of the new system on customer's ability to accomplish his or her own objectives. Today we find a situation, at least in supermarkets, where the current payment system appears to be relatively effective in meeting the customer needs. We are, therefore, concerned that E.F.T. be designed in a way to speed the financial transactions without

- a) increasing the customer's waiting time,
- b) increasing the complexity of the process and,
- c) eliminating the opportunity for the customer to interact easily with his or her financial institution.

In the last analysis, customers want no more hassle from E.F.T. than they receive from the current system and hopefully less.

Choice, like convenience, is an issue of significant importance to our customers. Food retailing operates on the premise that the consumer should be provided with adequate information on which to make an informed choice among the products and services that are offered in the marketplace. This same principle, in our judgement, extends to both the development and design of E.F.T.

What are some of the choices that customers have today which must be kept in mind in developing an E.F.T. system?

- The choice of payment system. Today the customer can pay for his or her groceries with cash, check, and in some instances even a credit card.

It is in the consumer's best interest to have a ready

access to these other payment systems for a fairly long period of time. While there are many positive aspects of E.F.T., there is a need to maintain the customer's options while this new payment system is evolving.

- The choice of financial institution. The customer can today choose a financial institution independently of the choice of a supermarket and it is in the interest of the customers to maintain that separation.

Retailers don't want to influence their customer's choice of financial institution anymore than they want the financial institutions to dictate the choice of supermarkets. An E.F.T. system should be universal in the sense that all customers can gain access to the services, regardless of where they bank.

- Choice of store. Nearly 9 out of 10 customers regularly shop more than one supermarket and the customer's ability to choose the store at which he or she shops is of utmost importance. An E.F.T. system that hinders this choice will clearly penalize the customer.

Customers recognize that high costs make it impossible to provide unlimited choice, but they feel that they are entitled to some choice or a clear and persuasive explanation as to why a choice is not possible. If the emerging E.F.T. system will require or cause a change in the set of choices currently facing the customer, then there will be a real need to explain this to customers. To reduce the choices without adequate justification, could cause a serious pitfall.

In conclusion, it appears that there is a good chance that the emerging E.F.T. system could have as significant an impact on the consumer's convenience and choice as it will on the better publicized

issues of privacy and security. For this reason, we would encourage you to look even more carefully into your future deliberations, at these two areas as the decisions on these matters will regularly affect millions of consumers. Since we also have a strong interest in these areas, we would like to volunteer, if you desire, to keep you apprised of what we learn on these issues from our regular dialogue with customers. It is clearly in the customer's best interest to keep you informed of what's happening in the stores. Thank you.

Testimony
before
National Commission on Electronic Funds Transfer
Presented by
Thomas K. Zaucha, Director of Public Affairs
The National Association of Food Chains
October 28, 1976

I'm Thomas K. Zaucha, Director of Public Affairs for the National Association of Food Chains.

The Joint NAFC/SMI Electronic Funds Transfer Committee has discussed the October 7, 1976 resolution by the Committee on Regulatory Issues, and is pleased to have this opportunity to offer you our comments. While we are perceived by some as being on the sidelines of the debate as to whether a terminal should or should not be defined as a branch, the resolution of this question will have a major impact on both our customers and our stores.

It has been suggested that the current situation contains certain inequities that must be resolved. We are thinking here of the suggestion that in today's regulatory environment, one group of depository institutions is able to develop their EFT systems with few limitations while the activities of another group of institutions are constrained. We are also thinking of the suggestion that the consumers in some states may be deprived of the potential benefits of EFTS simply because of conflicting or incompatible approaches taken by some states. However, at this point in time we are unconvinced that this evidence alone is necessary and sufficient support for pre-emptive legislation.

In adopting this stand, we recognize the need to promote competition and minimize government involvement in the emerging EFT systems. We subscribe to the power and efficiency of the market as the primary regulator of economic activity in our society. It is from this position, however, that we feel the need to urge a more cautious approach to the question before you today.

249i

While there is a need to encourage competitive development, it would be premature to make a decision on the status of a terminal at this time. One of the stated principles of your Commission is that EFT should be advanced to benefit the consumer, and yet this benefit has not yet been clearly established. Our own testimony before the Consumer Hearings pointed out a number of important and yet unresolved questions which will have a major impact on the consumer's final valuation of EFT. Is it correct to encourage broadscale deployment with so many questions still outstanding?

We believe that it would be wise to delay this decision until the social and economic benefit of retail EFT is better understood. We are keenly aware of the open issues that are confronting both the consumer and the retailers. We are concerned for example about the wording of paragraph two in your resolution dealing with regulation of business enterprises housing terminals. Does this paragraph pertain only to customer-operated terminals, or does it have more general application? This point must be clarified to us. At the same time, we sense that other groups involved in EFT have similar concerns. Until more of the questions are answered, it is our position that action on the October 7 resolution should be deferred.

CHAIRMAN WIDNALL: The next witness is John Barber,
Director of Planning, Mercantile Bankshares Corporation,
Baltimore, Maryland.

1 (Witness sworn.)

2 STATEMENT OF JOHN BARBER, DIRECTOR OF PLANNING,
3 MERCANTILE BANK SHARES CORPORATION

4 CHAIRMAN ATWATER: I might add that Mr. Barber
5 is also former executive director of the Middle Atlantic
6 Clearinghouse organization and established an automated
7 clearinghouse for Maryland, Northern Virginia and the
8 District of Columbia.

9 If you would like to present your 10 minutes of
10 testimony, we will hold our questions.

11 MR. BARBER: Certainly.

12
13 I was invited, I assume, because I do have practical
14 experience within automated clearinghouse activities.
15 I also am a former bank operations officer, in which I
16 actually dealt hand-to-hand with our present manual check
17 clearing processes.

18 I am not an attorney, and therefore know very
19 little about the points of law, other than in
20 practicality.

21 My request to this group is to consider my basic
22 position, which is to leave financial institutions alone in
23 the development of EFTS.

At this point in
24 time no one really knows what we are doing, or what avenue
25 to take. We are using our own money, dealing with our own

1 customers, in a very highly competitive market. The image
2 that we, internal to banking, have is different from the
3 external image. We go to a great deal of trouble to consider
4 our customer in terms of the consumer protection that you
5 are talking about.

6 We also go to great effort to consider the questions
7 of restraint of trade and the effect upon our corporate
8 customers and their activities. We feel that for financial
9 institutions to be successful in the EFTS area, an institution
10 must have an established plan of attack, a good marketing
11 structure, and must be well based operationally, in order to
12 handle the activity.

13 We would like to find ways of curtailing our present
14 paper-check reject rate, in that there is an error rate involved
15 in our present activity, and those who have played with the
16 computer for a while feel like the computer will be a more
17 effective way of handling a transaction.

18 We have a problem in this type of EFT installation,
19 in that our marketing studies have shown us, in essence, every-
20 one is happy with the present check system except for bank
21 operations officers and some knowledgeable chief executive
22 officers of banks. The consumer is happy with his check. The
23 corporate customer is happy with his check. And the banks
24 see the full paper as being proper and correct in its
25 activities. My concern is cost and convenience when we get

CONTINUED

5 OF 6

1 to the customer himself. We feel like the present corporate
2 and retail customer will have the same consumer protections he
3 presently has, but with increased convenience and decreased
4 cost.

5 From the standpoint of the financial institution,
6 we will have a new and better clearing mechanism. I think here
7 analysts missed the general point we are talking about. We
8 are looking for a simpler operating environment. The physical
9 handling of paper checks is a mess. We have an error rate
10 from our computers -- an error being a rejected item which will
11 not process through our reader-sorter machines -- and every
12 member of the Commission should visit the operations center
13 of a major bank at 10:00 or 11:00 o'clock at night when they
14 are attempting to make the clearing deadlines. It is an
15 amazing thing to watch the checks go through the system.

16 The main device in reading the paper check is called
17 a reader-sorter. It will process checks at a very high rate
18 of speed, and very efficiently. The difficulty is that it
19 rejects -- refuses to read, reads incorrectly -- 1 to 2
20 percent of these items on every pass through the machine.

21 When we have a rejected item, someone must
22
23
24
25

1 manually process that individual item. A major bank will
2 handle millions of checks in a given night. One million
3 checks stacked one on top of the other is about the height
4 of an 80-story building, and that is an awful lot of checks
5 to be moved in a given period of time.

6 Therefore, we have difficulty within banks with
7 their operating costs. Inflation, cost of doing business,
8 and even diseconomies of scale -- because of the increase
9 in the number of checks and increased number of accounts--
10 give us great difficulties, so we are looking for a way that
11 will reduce the cost to our customers of handling an account.

12 We are concerned about privacy, but from our
13 standpoint, most of the information that would be contained
14 within an EFT system is presently available. The major
15 difference is that we're talking in terms of a computer
16 search rather than a manual microfilm search. Today,
17 most checks in the
18 system are microfilmed as they are processed. Within that,
19 you have both the front and the back of the check. Therefore,
20 you can see who wrote it, for how much, to whom, what date,
21 and their endorsements as it goes through the system, so you
22 can follow it.

23 We have the same kind of access to information
24 today, only slower, as what we would have in the future.
25 We probably will establish consortia to create this EFT

1 system. We do not see consortia as being improper in our
2 activities. The automated clearing houses are consortia in
3 one form or another. We see each individual financial insti-
4 tution providing distinct services that are created within
5 different images and different costs of operation.

6 Therefore, the activities in the consortia are
7 primarily created to provide a clearing mechanism to handle
8 it, whether it be in the private sector, the public sector,
9 whether it be in banking or whether it be supplied by outside
10 firms who are providing it as services within the concept
11 of EFT.

12 We presently warrant that a customer can return
13 an item if it is in error, or if he has some disagreement with
14 the originator of the item. We have a warranty such that
15 the originating banks accept the liability for an item, which
16 they have now, for cases of forged endorsements, etc.

17
18
19
20
21
22
23
24
25

1 They go back into the system, so we have not changed anything
2 with EFTS.

3 In order for an item to be posted, it must be
4 authorized, particularly on the debit side. On the credit side
5 we are at a point now where we are accepting incoming credits
6 without authorization being passed to the bank that is
7 receiving the item.

8 We are concerned about fraud, but we have fraud in
9 the present system. We have forged checks, we have forged
10 endorsements, we will have all of those kinds of things that
11 we have presently. We have lost cards, we have running credit
12 cards; we will have the same thing with debit cards.

13 There are very few ways to treat this until we can
14 actually define and handle the item. The main thing to
15 remember is that, in general, debit transactions under an
16 account will be handled from one account at a financial
17 institution into the account of a corporate customer for my
18 credit to the originating account holder. Each item must be
19 authorized in order for it to be processed.

20 We are happy with the computer and communications
21 capability that we see coming in in the near future. With
22 the present generation of computers we have had a magnificent
23 increase in reliability. We have
24
25

1 fewer downtime situations and fewer errors within the computer
2 itself. We are taking some time to work out the problems
3 within the software, because there are always problems within
4 the software, but we are learning about that activity as we go.

5 In summary, as an individual, divorcing myself from
6 the bank, I feel that I would be better off with EFTS than
7 I am now. My cost of the account will still be low, convenience
8 will improve, implementation will be a very slow process in
9 which I can pick and choose the services I wish to use.
10 Banks will lean over backward to insure that the consumer
11 is protected.

12 If I, as a retail customer, can go to my telephone
13 and, through a Touch-Tone phone, pay my bills, I am going
14 to smile greatly. I think that is magnificent. I, personally,
15 do not balance my checkbook. I cannot do it. We find a very
16 large number of people can't balance their checkbooks; but
17 under the new system, we are talking in terms of telephone
18 procedures where I can call in daily and find out the balance
19 in my account through audio response systems.

20 As a corporate treasurer, I would like to wait and
21 prove that EFTS works before I participate in it. That is
22 the reason it is going slowly. I have had many arguments in
23 the heat of the night about why
24
25

1 a corporation should accept this activity, and I can
2 make a very good argument for it, based primarily on the cost
3 of managing a payroll account or reconciling a general
4 disbursement account.

5 But, if I were a corporate treasurer, I would go
6 slowly in accepting it -- that is what we are finding within
7 the automated clearing house activity. On the other hand, I
8 know a number of these guys who are baiting me as I talk
9 because I talk also to their systems analysts, and they
10 are modifying their payroll and disbursement systems now
11 to be on-stream in one to two years, to be able to
12 participate in direct deposit of payroll and direct
13 disbursement systems.

14 As a banker, I shudder at the costs that are
15 going to be involved in implementation, because they will
16 be very large. Yet, we are willing to undergo them in the
17 short term in order to achieve a longer-term benefit to our
18 customers.

19 I personally am eager to participate in the system, because
20 in terms of computer technology in general, this is what we
21 would consider a "fun" system. It is something new; it is
22 something different. We would like to have it developed.

CHAIRMAN ATWATER: Mr. Anderson.

MR. WALTER ANDERSON: You had some favorable
comments on computer reliability. Do you have any
1 comments to share with us on the transmission line
2 reliability?

3 MR. BARBER: None, sir. We have a system; it
4 works. But I have not worked with actual data rates
5 or whatnot in handling it.

6 CHAIRMAN ATWATER: Are there other questions
7 among the commissioners.

8 CHAIRMAN WIDNALL: I would just like to
9 compliment the witness on his statement. It is very
10 forthright and to the point, and shows good practical
11 knowledge.

12 MR. BARBER: Thank you.

13 CHAIRMAN ATWATER: Thank you very much.

14 With that, I believe, Mr. Chairman, we can
15 adjourn our activities.

16 CHAIRMAN WIDNALL: I thank all of you for being
17 here today, and helping to make these hearings a success.
18 We hope that the others that will continue the next
19 three days, under two different subcommittees, will
20 be just as successful.

21 (Whereupon, at 5:30 p.m., the hearing was
22 adjourned.)
23
24
25

END