

OFFICE OF JUSTICE PROGRAMS BJA BJS NIJ OJDP OVC SMART

The author(s) shown below used Federal funding provided by the U.S. Department of Justice to prepare the following resource:

Document Title:	Mass Marketing Elder Fraud Intervention
Author(s):	Lynn Langton, Ph.D., Edward Preble, Ph.D., Daniel Brannock, Erin Kennedy
Document Number:	308661
Date Received:	March 2024
Award Number:	2019-R2-CX-0053

This resource has not been published by the U.S. Department of Justice. This resource is being made publicly available through the **Office of Justice Programs' National Criminal Justice Reference** Service.

Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. **Department of Justice.**

Mass Marketing Elder Fraud Intervention NIJ Final Report

Prepared for

National Institute of Justice 810 Seventh Street, NW Washington, DC 20001

Prepared by

Lynn Langton, PhD Edward Preble, PhD Daniel Brannock Wayne Pitts Erin Kennedy

RTI International 3040 E. Cornwallis Road, PO Box 12194 Research Triangle Park, NC 27709 <u>https://www.rti.org</u>

Marti DeLiema, PhD University of Minnesota

RTI Project Number 0217211.000.005

December 2023

This resource was prepared by the author(s) using Federal funds provided by the U.S. Department of Justice. Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Mass Marketing Elder Fraud Intervention Study NIJ Final Report

Prepared for

National Institute of Justice 810 Seventh Street, NW Washington, DC 20001

Prepared by

Lynn Langton, PhD Edward Preble, PhD Daniel Brannock Wayne Pitts Erin Kennedy

RTI International 3040 E. Cornwallis Road, PO Box 12194 Research Triangle Park, NC 27709 https://www.rti.org

Marti DeLiema, PhD University of Minnesota

December 2023

RTI International is a trade name of Research Triangle Institute. RTI and the RTI logo are U.S. registered trademarks of Research Triangle Institute.



Contents

1.	Sun	nmary of the Project	1-1		
	1.1	Background1-1			
	1.2	Goals and Objectives1-3			
	1.3	Research Questions			
		1.3.3 Survey1-8			
	1.4	Research Design/Methods1-10			
		1.4.1 Secondary Data Analysis 1-10 1.4.2 Intervention Experiment 1.47			
		1.4.2 Intervention Experiment			
	1.5	Expected Applicability/Impact			
2.	Part	Participants and Collaborators 2			
	2.1	Advisory Board2-1			
	2.2	Interviews with Persons Impacted by Fraud2-2			
	2.3	Cognitive Testing of Intervention Materials 2-5 2.3.1 Recruitment and Interview Procedures			
	2.4	Experiment Participants2-10			
	2.5	Survey Respondents2-14			
3.	Cha	inges to the Originally Proposed Design	3-1		
	3.1	Reduced Sample Sizes3-1			
	3.2	Changes to One of the Experimental Conditions			
	3.3	Shorter Intervention Follow-up Period3-2			
4.	Find	dings	4-1		
	4.1	Secondary Data Analysis4-1 4.1.1 Prevalence of Mail Fraud Victimization4-1			
	4.2	Intervention Experiment4-9			
	4.3	Survey4-8			
	4.4	Limitations4-15			

5.	Artifacts		
	5.1	Products Resulting from the Project5-1	
		5.1.1 Materials5-1	
	5.2	Datasets Generated5-1	
	5.3	Dissemination Activities5-2	
		5.3.1 Papers	
		5.3.2 Presentations	
Refe	rence	s	R-1
Арре	endic	es	
A:	MME	FI Intervention Materials	A-1
B:	MMEFI Victim Interview Report		
C:	MMEFI Cognitive Interviewing Report C-		

Page

Figures

Number

1-1.	Timeline for Intervention Experiment Mailings	1-20
1-2.	Timeline for Follow-up Survey Mailings	1-23
4-1.	Number of Victimizations (Payment Envelopes Received) During the Scammers' Periods of Operation, 1999-2018	4-1
4-2.	Proportion of Total Losses and Proportion of Repeat Victims in Scammer CRM Databases	4-2
4-3.	Average Payment Amount Per Solicitation Over Consecutive Victimization Incidents	4-4
4-4.	Percent of Victims Who Experienced Each Scam Type and the Average Number of Victimization Incidents	4-4
4-5.	Time (Days) Between Consecutive Victimization Incidents	4-5
4-6.	The Relationship Between Victim Age at First Victimization, Losses, and Victimization Incidents	4-7
4-7.	Count of Mail Fraud Incidents by Month	4-8
4-8 .	Seasonal Variation of Mail Fraud Incidents, by Type of Scam	4-9

Page

Tables

Number

		•
1-1.	Scam Summary Information	1-13
1-2.	Prevalence of Identification Confidence Scores and Associated False Match Rates (FMR)	1-15
2-1.	Victim Interviewees by Sex, Victim Status and Age Range	2-2
2-2.	Characteristics of Target Participants and Actual Participants	2-6
2-3.	Count of Addresses Included in the Intervention Experiment	2-11
2-4.	Demographic Characteristics of Known Victims Included in the Intervention Experiment	2-12
2-5.	Household Characteristics of Known Victims Included in the Intervention Experiment	2-13
2-6 .	Survey Response by Experimental Group and Number of Known Mail Fraud Victimizations	2-14
2-7.	Demographic Characteristics of Survey Respondents	2-15
2-8.	Household Characteristics of Survey Respondents	2-16
4-1.	Types of Payment Methods Recorded in the DMI Dataset	4-6
4-2.	Calculated Repeated Seasonal Variation of Mail Fraud Incidents, by Month	4-9
4-3.	Number of Victims in the Intervention Experiment Responding to a Mail Scam Solicitation in the Post-intervention Monitoring Period, by Control and Treatment Groups	4-3
4-4.	Prevalence and Counts of New Responses to Scam Mail During the 4 Months Following the Intervention	
4-5.	Number and Percent of Victims With One or More Scam Mail Responses During the 4 Months Following the Intervention, by Victim Demographics	4-5
4-6 .	Number and Percent of Victims With One or More Scam Mail Responses During the 4 Months Following the Intervention, by Household Demographics	4-6
4-7.	Memory of and Reaction to Receiving Intervention Mailing(s)	4-7
4-8 .	Demographic Characteristics of Long-term Repeat, Repeat, and New Victims	4-9
4-9 .	Household Characteristics of Long-term Repeat, Repeat, and New Victims	4-10
4-10.	Experiences With Fraud or Financial Abuse, Playing the Lottery or Purchasing Scratch-off Tickets Among Long-term Repeat, Repeat, and New Victims	4-11
4-12.	Loneliness, Financial Fragility, and Willingness to Take Financial Risk Among Long-term Repeat, Repeat, and New Victims	4-14

1. Summary of the Project

1.1 Background

Estimates suggest that up to 16% of American adults—approximately 40 million people—fall victim to mass marketing scams each year (Anderson, 2019). Mass marketing scams include any attempts to fraudulently solicit money from consumers through mass communication methods, such as the internet, telephone, and mail. Complaints to consumer protection agencies have risen 240% in the past 10 years (Federal Trade Commission [FTC], 2013, 2023). According to conservative estimates from the most recent Consumer Sentinel Network Report (FTC, 2023), Americans reported more than \$2.7 billion in direct losses from fraud in 2022. In addition to financial costs, consequences to victims include feelings of shame and embarrassment, loss of trust, depression, and, in the most severe cases, suicidal ideation (Buchanan & Whitty, 2014; Button, Lewis, & Tapley, 2014; Cross, 2018; Deem, 2000). These consequences of fraud are particularly impactful for older adults who suffer higher losses per incident, on average (FTC, 2022) and face greater challenges recovering from losses after retirement. Research on elder mistreatment in general has shown that older victims consume 30% more mental health and substance abuse services (Schonfeld, Larsen, & Stiles, 2006) and are hospitalized more often than non-victims (Dong & Simon, 2013).

According to the United States Postal Inspection Service (USPIS), the federal law enforcement agency with jurisdiction over all crimes perpetrated via the mail, mail scams typically involve fake prize, lottery, or sweepstakes notifications that request upfront payment in return for a much larger cash prize or other reward, such as a luxury vehicle (<u>https://www.uspis.gov/tips-prevention</u>). Other common mail scams include letters from supposed psychics claiming to possess important information about the future but asking the target to first pay a fee to have their future foretold. Other schemes may involve fake utility bills, donation requests, employment

opportunities, or letters demanding payment from government impostors. Scam victims who mail in the requested payment continue to be inundated with additional scam letters as their addresses and personal information are added to "suckers lists" to be traded, rented, and sold to other mail fraud enterprises (Balleisen, 2018). This increases their exposure to further fraud solicitations and their likelihood of repeat victimization.

A growing body of research indicates that older adults face a greater risk of fraud victimization than younger adults (Lachs & Han, 2015). Reasons include age-related changes in cognitive functioning that affect decision-making even in adults without dementia (James, Boyle, & Bennett, 2014; Han et al., 2016; Yu et al., 2021); lower knowledge about phishing (Gavett et al., 2017); greater wealth (Butrica, Smith, & Iams, 2012); and Ioneliness and social isolation (Greenfield & Russell, 2011; James, Boyle, & Bennett, 2014; Xing et al., 2020). Lee and Soberon-Ferrer (1997) found that adults more susceptible to fraud tended to be older; female; less educated; and widowed, divorced, or never married.

Mass marketing scams are some of the most common types of fraud targeting older adults (FTC, 2022; Lonsdale et al., 2016). These scams convince susceptible targets that they have won bogus sweepstakes, merchandise, free vacations, or lotteries, but they first need to pay money to claim their winnings. Based on data from one major investigation from 2011 to 2016, the USPIS found that Americans sent \$558 million in checks, credit card payments, and money orders through the mail in response to such scams (USPIS internal data). Overall, the USPIS estimates that 3% of U.S. adults—7.5 million Americans—have mailed a payment in response to mass marketing fraud and that 60%–70% of these individuals are revictimized by a similar solicitation or an entirely different offer. Given these figures, reducing the incidence of mass marketing fraud could save millions of dollars annually.

Although the FTC, the National Council on Aging, the Consumer Financial Protection Bureau, the Better Business Bureau, AARP, and other agencies and organizations routinely disseminate fraud education and awareness materials, it is unclear how much of these materials reach the most vulnerable populations. Much of the content is available online, yet according to the Pew Research Center, only 75% of adults older than age 65 use the internet, and only 64% have home broadband (Perrin, 2021). Printed materials are also disseminated at senior centers, libraries, legal service offices, and outreach events, but older adults who are socially isolated and most susceptible to fraud (Alves & Wilson, 2008; DeLiema, Li, & Mottola, 2023) are unlikely to be reached through these venues.

Most organizations also have no means of tracking what interventions were received by whom or assessing whether the fraud prevention messages significantly reduced the likelihood of future victimization. For instance, the USPIS has dedicated more than \$50 million to consumer fraud protection over the past 10 years, engaging in wide-ranging fraud prevention efforts such as public service announcements, billboards, one-on-one phone calls from victim specialists, lectures at senior centers and community events, visits to victims' homes, and even a multi-episode television show about a mail scam. However, like most other agencies and organizations that have invested heavily in fraud prevention, the USPIS lacks the internal capacity to systematically evaluate the efficacy of its intervention approaches. Without rigorous testing of materials using randomized controlled trials, little is known about who receives prevention messages, which ones are most effective, and for whom they are effective.

1.2 Goals and Objectives

To address gaps in intervention research, RTI International and the University of Minnesota conducted the Mass Marketing Elder Fraud Intervention (MMEFI) Study with collaboration and support from the USPIS. This multiphase research project included a secondary analysis of USPIS administrative data on prior scams and a randomized controlled trial test of the efficacy of two variations of a mailed intervention for preventing revictimization by mail fraud. The overall objective was to provide specific policy recommendations to the USPIS and other consumer

protection agencies regarding the effectiveness of a mailed intervention. The MMEFI Study had the following specific goals:

- Enhance knowledge and understanding of repeat victimization among older victims of mass marketing scams.
- Engage in rigorous testing of the efficacy of two versions of a fraud intervention strategy geared toward preventing repeat victimization among older victims of mass marketing scams.
- Assess victims' perceptions of the intervention and collect self-report data on experiences with other types of fraud by surveying individuals in the intervention study.

The first goal was accomplished through a secondary analysis of 20 years of USPIS administrative data on millions of U.S. fraud victims who were originally recorded in mail scammers' customer relationship management (CRM) systems. CRM systems are traditionally used by legitimate businesses to monitor and track customer interactions and sales over time. However, mail fraud enterprises have also used CRM systems to record how often households responded to their solicitations and how much money they enclosed each time. The CRM files analyzed in the MMEFI Study were seized by USPIS as part of their investigations of these enterprises' criminal activities.

We linked victim addresses across the four CRM databases to assess the incidence, cost, and frequency of repeat victimization, as well as the relationship between repeat victimization and age. With these longitudinal data, we identified the prevalence of repeat victimization, the losses experienced by victims, victim susceptibility to the same versus different types of mail scams (e.g., psychic scams and bogus lottery/prize/sweepstakes scams), and the average time between victimization incidents for repeat victims. The findings have important implications for consumer advocacy organizations and law enforcement agencies around the need to address repeat fraud victimization and potential points for intervention.

The second goal of the MMEFI Study was to evaluate the efficacy of a simple, scalable mass marketing fraud intervention that can be implemented by the USPIS, and to test variations of that intervention for reducing levels of mass marketing fraud revictimization relative to no intervention. Postal inspectors can identify P.O. Boxes or addresses that scammers are using to collect victim payments and can detain the envelopes headed to those addresses for investigative purposes and victim protection. After a delay period of few months, the USPIS returns the payment envelope to the victim's address.

The proposed study built on the idea of a mailed intervention to prevent mass marketing fraud revictimization. Using return addresses on unopened victim mail detained by the USPIS, we tested the effectiveness of two versions of mailed intervention materials. Victims' return addresses were randomly assigned to one of two treatment groups or to a control group. Treatment groups received either (1) a letter from the USPIS informing them that they paid money in response to a mail scam and may be targeted by additional scams, as well as education on how to spot mail scams, or (2) the same letter from the USPIS along with a brochure giving victims a call to action for preventing fraud and four additional fraud awareness materials mailed 2 weeks apart. The control group received no mailed intervention during the study period. The effectiveness of the intervention was assessed through actual victim behavior. USPIS collected return addresses from detained victim mail for 4 months following the initial mailing. RTI analysts identified revictimization by matching the return addresses from the newly detained mail to the addresses of victims in the experiment.

The interventions are designed to improve victims' resiliency against subsequent scams, but receiving the materials from the USPIS could also be distressing or have a negative effect on victims' well-being. It is also important for consumer advocates to know *for whom* the different intervention approaches were most effective. Therefore, we mailed a survey to all victims in the intervention and the control group to ask whether those in the intervention conditions recalled

receiving the materials and what the impact of receiving those materials was. We also collected basic demographic and behavioral characteristics and experiences with other types of fraud and financial exploitation in the past year.

1.3 Research Questions

1.3.1 Secondary Data Analysis

In the area of mass marketing fraud, law enforcement agencies, consumer protection agencies, and victim advocates have recognized the need to interrupt the cycle of repeat fraud victimization. However, there is limited empirical research on the scope of the problem, the extent of the harms experienced by repeat victims, or when intervention might be most effective. To address these gaps, we combined and analyzed data on victims and payments originally compiled by four separate mail fraud enterprises as part of their CRM protocols. We sought to answer the following research questions using the merged longitudinal dataset that spans nearly 20 years, from 1999 to 2018:

- What are the prevalence and incidence of repeat mass marketing fraud victimization?
- Which of the scams identified by the USPIS have the highest incidence of repeat victimization?
- Does revictimization result in an escalation in the amount of money paid in response to another scam?
- Do repeat victims respond to different types of scams (e.g., lottery vs. sweepstakes vs. psychic) or one consistent type?
- What is the average duration of time between victimization experiences?
- What methods of payment are used in mass marketing mail scams (e.g., check, cash, credit card, money order)?

 Are there patterns in repeat victimization associated with victim age, geography, or seasonality?

1.3.2 Intervention Experiment

We conducted a randomized controlled trial to test the efficacy of several intervention approaches for preventing revictimization among older victims of mass marketing fraud. The interventions included different fraud awareness materials that were sent to households identified by the USPIS as recent victims of mail fraud. Households in the intervention experiment were randomized into one of three conditions:

- Treatment group 1 received an official letter from the USPIS informing them that a piece of their mail was sent to an address or P.O. Box currently under investigation for mass marketing fraud. The letter explained that they should have received their original payment envelope back in the mail and that their personal information was likely added to a list used by multiple criminal organizations for future fraud targeting attempts. The letter warns the receiver to be on the lookout for subsequent fraudulent solicitations by mail or phone.¹ On the backside, the letter provides written tips and visual examples of fraudulent offers to educate the receiver on common mail scam tactics.
- Treatment group 2 received additional materials mailed weeks apart to cultivate a "Fraud Fighter" mentality. In addition to the warning letter, treatment group 2 received a fraud prevention brochure with a perforated, tear-off panel encouraging them to join in the USPIS's effort to protect others from fraud by sharing their stories and tips for detecting and avoiding scams. In addition to the letter and brochure, treatment group 2 was mailed new fraud awareness and empowerment materials every few weeks. The additional mailings included a flyer introducing the recipient to the USPIS and how to report mail

¹ Based on prior research by Beals, Carr, Mottola, Deevy, and Carstensen, 2017, all intervention messages will avoid calling the recipient a "victim," because this can present a threat to self-image and cause the prevention message to backfire.

fraud, a newsletter with stories from other victims and a crossword puzzle, a brochure showcasing the criminals behind the scams and how they use victims' money, and a "Thank you for being a Fraud Fighter" greeting card.

 The control group did not receive any communication or materials from the USPIS but did receive their original payment returned in the original envelop with a yellow "Return to Sender" United States Postal Service sticker on it.

Our research questions were as follows:

- Is any intervention better than no intervention? In other words, is the incidence of revictimization during the follow-up period significantly lower for the two treatment groups compared with the control group?
- Does dosage and fraud empowerment messaging matter? When we compare levels of revictimization across treatment groups 1 and 2, is the incidence of revictimization lower among those who received repeated reminders and an enhanced call to action?

We hypothesized that compared to the control condition, recipients in treatment groups 1 and 2 would be less likely to respond to a subsequent mail scam during the follow-up period. We also predicted that those randomized to treatment group 2 would be less likely to experience a subsequent victimization than those in treatment group 1. The hypotheses were preregistered with aspredicted.org **Z**.

1.3.3 Survey

In the final phase of the MMEFI Study, both intervention and control groups received a survey. There were three versions of the survey, all of which captured demographic information, fraud risk behaviors, and experiences with other types of fraud in the prior year. Among the individuals randomized to treatment groups 1 and 2, we also assessed the extent to which respondents recalled receiving the intervention materials, their perceptions of the materials, and any positive or negative reactions to the materials. Individuals in treatment group 1 received a version of the survey that included questions about recall and reactions to the letter from the USPIS, while individuals in treatment group 2 received the same questions about the letter as well as questions about the other Fraud Fighter materials. Survey responses were linked to each victims' intervention results. This allowed us to address the following research questions:

- Did the randomization procedure used in the experiment yield similar treatment and control groups with respect to victim age, household income, sex, race/ethnicity, educational attainment, living arrangement, marital status, and household composition?
- What is the prevalence of other forms of fraud and financial victimization among known victims of mass marketing mail scams?
- What is the prevalence and frequency of other risk factors and risky behaviors (e.g., answering calls from unknown individuals, entering personal information into sweepstakes drawings, using social media, feelings of loneliness)?
- What is the prevalence of reporting to law enforcement or consumer protection agencies?
- What demographic, psychological, and behavioral factors predict intervention effectiveness?

Additional research questions applied to those in the treatment groups:

- To what extent do respondents recall receiving the intervention materials?
- To what extent did respondents feel distressed after receiving the materials, if at all?
- To what extent do respondents say they would share fraud awareness information with others?
- To what extent do respondents feel they are able to identify scam letters?

1.4 Research Design/Methods

1.4.1 Secondary Data Analysis

Data Source

As part of their criminal investigations into mail fraud, the USPIS seized CRM databases from four mail fraud enterprises: Maria Duval, Maria Rochefort, Fennel-Kern, and Data Matrix Inc. (DMI). The CRM databases are longitudinal, capturing the dates and number of separate payments victims mailed, in addition to how much they paid at each incident. Victims' names and addresses are also stored in the CRM databases; in the case of the two psychic scams, dates of birth were also collected purportedly to offer a more accurate psychic reading. All transactions ended in 2018 when the organizations were investigated and stopped by the USPIS.

For RTI's analysis, the USPIS added an 11-digit ZIP code to each address record in the CRM databases. These 11-digit ZIP codes correspond to each victim household's exact delivery point. The 11-digit ZIP codes helped to facilitate linking incidents to unique addresses within and across each of the CRM databases.

The USPIS also attached a chaining address file to the Maria Duval and Maria Rochefort files. The address chaining file was intended to enable the research team to identify whether a victim moved to a new address over the nearly 20-year data period. For the Maria Duval and Maria Rochefort databases, the address chaining file was linked to less than 0.1% of 11-digit ZIP codes in the address databases. Because of the size of the DMI file and the time and resources required to do address chaining, the USPIS was not able to include an address chaining file with the DMI or Kern databases. Thus, the chaining file was not used in the analysis.

Data Transfer

For each of the four scams, encrypted drives containing the datasets were sent to RTI via registered mail. Files were immediately loaded onto secure computers meeting Federal Information Processing Standards (FIPS) for handling moderately sensitive, personally identifiable data (FIPS-mod). Because of the process of adding the 11-digit ZIP codes and the need to reduce the size of the original databases, which contained large amounts of unusable data, the USPIS sent the databases to RTI over the course of several months. The Maria Duval and Maria Rochefort files were received in December 2020, followed by the DMI file in mid-February 2021, and the Fennel-Kern data in May 2021.

Data Cleaning

The full databases contained transactions from both the United States and international addresses, which presented multiple hurdles: (1) There was no consistent character encoding that allowed for easy digestion into an open-source relational database. (2) It was not always clear if a transaction should be included in U.S. totals. (3) Foreign currencies were not consistently labeled or converted to U.S. dollars, masking international dollar totals.

An iterative process was used to resolve character encoding challenges, repeating a cycle of two steps: (1) the data were fed into an ingestion pipeline that logged when a problematic character was encountered; and (2) common problematic characters were identified and replaced with compatible alternatives in the raw text data. Approximately 1,000 records (out of more than 83 million) could not be systematically resolved and were dropped. After the encoding challenges were resolved, the data were imported into a structured format into an SQL Server.

Transactions outside of the United States were excluded from all analyses. If the address associated with a transaction did not include a country, it was kept only if the state field was one of 51 valid U.S. state values (including Washington, DC). U.S. territories were also excluded, as

were military post offices (cities of APO, FPO, or DPO and/or states of AA, AE, or AO). A total of 30.5 million foreign transactions were removed: nearly all from DMI, but approximately 140,000 from Maria Duvall.

The databases also contained about 2.9 million transactions with a recorded amount of zero dollars. Transactions of zero dollars were not considered a victimization event for the purpose of these analyses. Therefore, if a person had exclusively zero-dollar transactions, they were also excluded from the analysis. This resulted in the exclusion of about 470,00 unique persons. As noted, the USPIS supplied the research team with 11-digit ZIP codes for most addresses. The 11-digit ZIP codes could not be assigned for 3.7% of transactions, where the USPIS could not identify a delivery point due to an invalid or mistyped address. To reduce inconsequential discrepancies in addresses, all transactions with the same 11-digit ZIP code were assigned a canonical address depending on what was most common for that 11-digit ZIP code. The canonization of addresses dramatically reduced common address inconsistencies (e.g., Drive vs. Dr, East vs. E).

The DMI database required processing steps not needed in the other databases. Transactions could only be matched to individuals through an intermediate file with a machine-generated ID particular to DMI. Out of 9.5 million U.S. transactions, 6.7 million were successfully matched through the intermediate file to a name and address. The remaining 2.8 million transactions (summing \$49.3 million in victimization events) could not be included in the analysis because they could not be deduplicated or linked to transactions in the other databases.

Although each of the databases included victims' names and addresses, entries had frequent inaccuracies and inconsistencies. For example, victims' first names and last names were generally split across two fields and were sometimes reversed from one record to the next. Addresses were similarly disorganized, and misspellings and non-alphanumeric characters were common across all fields. To address data formatting and encoding issues, the

researchers programmed several heuristics to standardize names, addresses, and ZIP codes: first names and last names were sorted alphabetically and concatenated into a single field, multi-field addresses were reverse-sorted by field length and concatenated, and ZIP codes were represented in multiple standard fields depending on the number of available digits.

Combining Scams

To measure repeat victimization, researchers identified victims who paid money more than once (had multiple transaction records) within each database. An open-source deduplication algorithm— Dedupe.io—was supplied with victims' names, location information (address, city, ZIP code), dates of birth, and DMI identifiers where available. Dedupe.io is an active learning algorithm that prompts users to label pairs of records as a match (same victim) or not a match (different victims). After learning from a sufficient sample of researcher-labeled pairs, the algorithm is applied to unseen records. The researchers labeled a minimum of 100 matching pairs and 100 disparate pairs for each database prior to fine tuning the algorithm with additional labeled pairs after manually reviewing the output for accuracy.

After identifying victim matches within each database, the four databases were combined, and the deduplication process was conducted across the full sample using the same personal identifiers. The results of the deduplication efforts, summarized in **Table 1-1**, show the scale of the different enterprises in the United States.

Scam Name	Туре	Operation Years	Unique Victims	Victimization Amount, \$
Maria Duval	Psychic	1999-2014	918,126	184,599,164
Maria Rochefort	Psychic	2000-2014	217,624	32,811,383
Fennel-Kern	Sweepstakes	2000-2018	128,750	17,498,840
DMI	Sweepstakes/lottery	2005-2018	462,255	112,224,976

Table 1-1. Scam Summary Information

Data Quality Assessment

The deduplication process was validated by determining a false match rate (FMR) and a missed match rate (MMR) among all U.S. transactions (including zero-dollar transactions). A false match occurs when the deduplication algorithm identifies two transactions as belonging to the same victim, but human review determines that the records belong to distinct individuals. A missed match occurs when the deduplication algorithm fails to detect that two transactions belong to the same individual. In addition to a unique identifier for each victim, Dedupe.io provides a confidence score (range 0–100) for each transaction that the identifier is correctly specified, where a higher score corresponds to a more confident classification. A single victim will have 1 identifier but may have 20 transactions with a range of confidence scores. To estimate the FMR, transactions were binned into the following confidence score bands (the left term is inclusive): 0-50, 50-95, 95-99.0, 99.0-99.9, 99.9-100, and equal to 100. Table 1-2 includes a summary of the number of transactions in each score band. Fifty random transactions were chosen from each score band for evaluation. To determine whether the transaction was correctly linked, all transactions linked to a chosen transaction via the victim identifier were evaluated. If a randomly selected identifier included two transactions from distinct individuals, then it was considered a false match. Records likely belonging to married individuals—where the address matches and the records share a surname—were considered a correct match. The FMRs for each score band were weighted by their prevalence in the data and combined to form a final FMR of 0.4%; i.e., 0.4% of the unique victim identifiers include transactions spanning multiple individuals.

Table 1-2. Prevalence of Identification Confidence Scores and Associated False Match Rates (FMR)

Score Band	Number of Records	Dollars, \$	Sampled FMR, %
Confidence < 50.0	4,644 (0.0%)	126,797 (0.0%)	2
50.0 ≤ Confidence < 95.0	861,211 (5.8%)	20,332,788 (5.9%)	6
95.0 ≤Confidence < 99.0	1,380,815 (9.4%)	29,068,965 (8.4%)	0
99.0 ≤ Confidence < 99.9	6,288,707 (42.7%)	133,855,500 (38.6%)	0
99.9 ≤ Confidence < 100	2,196,681 (14.9%)	61,614,603 (17.7%)	0
Confidence = 100	3,991,959 (27.1)	102,135,709 (29.4%)	0

To evaluate MMR, two inter-scam identifiers were available to potentially search for missed matches: 11-digit ZIP codes and birthdays (including the month, day, and year). The following process was used for each, using the 11-digit ZIP code as an example:

- Find all 11-digit ZIP codes that are associated with multiple victim identifiers.
- Sample 50 random 11-digit ZIP codes from #1.
- Extract all transactions associated with any victim identifiers included among the 50 sampled 11-digit ZIP codes.
- Manually review transactions to determine how many of the victim identifiers should have been matched to a different victim identifier associated with the same 11-digit ZIP code.

The 50 randomly selected 11-digit ZIP codes had a total of 109 distinct victim identifiers. Human review discovered eight missed matches for the same individual and six missed familial matches (sharing an address and surname), resulting in an MMR of 7.3% for individuals or 13% for families. However, only 4.2% of victim identifiers have an 11-digit ZIP code associated with multiple unique identifiers. Extrapolating to the full sample then yields an MMR of 0.3% for individuals or 0.5% for families.

The same process was repeated for birthdays. Sharing a birthday is significantly more common than sharing an 11-digit ZIP code: practically all (99.7%) victims with a known birthday share

that birthday with another victim. However, not all victims have a known birthday, since only psychic scams collected that information. The result is that 69.0% of victims have a shared date of birth with another victim. A random sample of 50 birthdays yielded 806 unique victim identifiers. Human review yielded 28 missed matches, resulting in an MMR of 3.5% among those with known birthdays, or 2.4% total. The two calculated missed match rates are distinct and can be summed to form a new MMR estimate of 2.9%. However, this remains an underestimate of the total MMR, as there may be transactions associated with different 11-digit ZIP codes as well as different dates of birth that were erroneously assigned to distinct individuals.

In summary, the matching algorithm was conservative: it had an estimated FMR of 0.4% and MMR of approximately (but no less than) 2.9%. Because more of the links were missed than erroneously identified, the repeat victimization estimates will also be slightly conservative.

Data Analysis

Data analysis was performed using the combined, deduplicated data. Descriptive statistics were calculated using victimization events from all four scams to characterize repeat victimization: timing, changes in payments, and overlap between scams. Only the two psychic scams (Maria Duval and Maria Rochefort) consistently included victims' dates of birth. Dates of birth for victims of the remaining two scams were available only if the victims were linked to one of the psychic scams in the record-linkage process. The analyses were run in SAS on de-identified data. Because this was the first time that administrative records from scammers were linked and used to understand repeat victimization, the focus was on descriptive statistics generated through the *proc freq* procedure.

1.4.2 Intervention Experiment

Intervention Materials Development

Developing the content and wording of the intervention materials was a critical component of the experiment. To ensure that messaging was aligned with current knowledge on resistance to persuasion and behavior modification, we first conducted a literature review to identify effective messaging in the fraud prevention and in health behavior change fields. Next, we conducted indepth, trauma-informed interviews with older victims of mass marketing fraud or their proxies to identify the factors that contributed to their susceptibility. Third, we convened an Expert Panel of practitioners who work with fraud victims and a psychologist with expertise on behavior modification to assist with messaging and design. Once drafts of the materials were designed, we conducted cognitive interviews with victims and non-victims to learn about their perceptions of the materials and the messaging. Adaptations were made based on the feedback received during these interviews. Ultimately, we developed, tested, and refined six mailings, intended to appeal to the different reasons victims may respond to a scam and be deterred from responding to scams. These materials, which can be seen in **Appendix A**, include:

- Standard forewarning letter
- USPIS tabloid newspaper
- Call-to-action Fraud Fighter brochure
- "Meet Your Team" flyer

 "Thank you for being a Fraud Fighter" greeting card

• "Who Are the Scammers?" brochure

Procedure to Identify Victims of Mass Marketing Mail Fraud

Postal Inspectors combat mail fraud by identifying a P.O. Box or address that scammers are using to collect victim payments. They detain the envelopes headed to those addresses for investigative purposes and victim protection. The law requires that payment envelopes be securely detained for 3 months while Postal Inspectors inform the intended recipient that they are suspected of engaging in mail fraud. If the recipient does not respond with evidence that they are *not* engaged in mail fraud, the payment envelopes are returned to the victims. To send the original payment envelopes back to victims, batches of envelopes are placed into a machine that reads the victims' return address using optical character recognition and adds a yellow "Return to Sender" sticker on the envelopes before automatically routing them back into the mail stream.

The roster of victim addresses used in the intervention experiment included all readable return addresses from payment envelopes that were intercepted by the USPIS between July 2021 and January 2023 (17 months). As described in Section 3, this was a significantly longer period of payment envelope collection than originally anticipated. Unfortunately, the list of addresses did not include postmark information or any way to identify *when* during the period a victim's envelope had been intercepted. The USPIS did add 11-digit ZIP codes to each address before securely sharing the file with RTI data analysts.

File Processing and Randomization

The roster of victim addresses was securely transferred to RTI and uploaded into the FIPS-mod network in February 2023. Analysts first reviewed the addresses for completeness and any errors that would result in mail being undeliverable. Of the 26,230 addresses on the initial roster, 8,625 were removed from the frame because they included only a "Parcel Return Service" ZIP code and no street address. An additional 702 addresses were removed because they were missing key parts of the address, such as street name or number, or a P.O. Box number for P.O. Box addresses. Because the roster did not include names, the analysts also had to remove all addresses that were identified as an apartment building but were missing an apartment number. With the invalid addresses removed from the roster, we were left with a frame of 16,903 valid addresses (64.4% of the total).

Next, analysts used Dedupe.io to identify duplicate addresses. Of the 16,903 valid addresses, only 2,857 unique addresses or clusters of addresses remained after the deduplication process (10.9% of the original list). This represented a substantially higher rate of repeat victimization among the roster addresses than expected.

Researchers then used Dedupe.io to identify the number of unique clusters from the intervention experiment roster that were also in the CRM databases. Of the 2,857 intervention experiment addresses, 2,000 (~70%) were also present in the CRM data from scams operating between 1999 and 2018. We labeled this group as the "long-term repeat victims" because their experiences with mass marketing fraud were known to span nearly 4 years. Of the remaining 857 addresses that were not present in the CRM databases, 379 had appeared multiple times on the roster and were labeled "repeat victim," and 478 appeared only once on the initial roster and were identified as "new victims."

Because of the potential for differences among the long-term repeat, repeat, and new victims in the effectiveness of the intervention materials for preventing revictimization, it was important to incorporate these groups into the randomization for the experiment. Thus, we randomized addresses in each of these three groups into the two treatment groups and the control group. This resulted in 952 addresses in the control group and treatment group 1, which received the USPIS letter only, and 953 addresses in treatment group 2, which received all the mailings.

Mailing the Intervention Materials to the Treatment Groups

After getting quotes from multiple printing companies near RTI's headquarters, we selected a local company, DocuSource, to do the printing and mailing of the intervention materials. We selected DocuSource because of their ability to handle complex jobs and to securely store addresses in a FIPS-mod environment. The initial intervention experiment mailing was sent on March 20, 2023. For treatment group 1, the initial mailing was the single letter from the USPIS. For treatment group 2, the initial mailing was the letter and the call-to-action Fraud Fighter

brochure. Importantly, the mailings appeared as though they were coming from the USPIS. The external envelopes included the USPIS logo in the upper right corner. The return address had "United States Postal Inspection Service," followed by an unrecognizable RTI address in Raleigh, NC. The mailings were addressed to "Postal Customer" because we did not have victim names on the roster. For the initial mailings to treatment group 2 that included a business reply envelope, that return envelope was addressed to "United States Postal Inspection Service, ATTN: Fraud Fighter Program" and the same RTI address used for the return address. All materials were reviewed, edited, and approved by USPIS's communications and legal departments. Figure 1-1 shows the timeline for the intervention mailings.

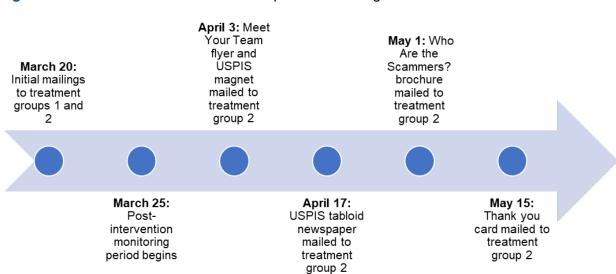


Figure 1-1. Timeline for Intervention Experiment Mailings

In May 2023, when the mailings to treatment group 2 were nearly complete, the USPIS provided two additional lists of addresses pulled from payment envelops interdicted between the end of January 2023 and the end of March 2023. Since these addresses had responded to a scam prior to the start of the intervention, but it was too late to add them to a treatment group, we initially decided to add them to the control group. The lists contained 1,531 unique addresses that were not already included in one of the treatment groups.

Assessing Intervention Efficacy

The post-intervention monitoring period lasted 4 months, from March 25, 2023 to July 26, 2023. During this period, the UPSIS continued to track, detain, and investigate suspected mail fraud. The USPIS provided the research team at RTI with a new list of victim addresses on August 10, 2023. This list included victims who responded to mail scams after the intervention materials were mailed to the treatment groups on March 20. Again, the exact date that the victim payment envelopes entered the mail stream (the postmarked date) was not known. Because of this, it is possible that envelopes collected in late March may have been mailed by the victim prior to receiving the intervention materials. This would reduce the likelihood of finding that the intervention had a significant effect on repeat victimization (a Type II error).

As the USPIS was tracking and detaining suspected mail fraud, the RTI team tracked intervention mailings that were being returned to sender as undeliverable. Despite inconsistencies in the returned mail (e.g., addresses in treatment group 2 that received five mailings would sometimes have fewer than five bounce-backs), any address that bounced at least once was removed from the intervention experiment. This rule was established because we could not be sure whether the address was still valid and whether mail was reaching the intended recipient or being sent out by the intended recipient.

After removing all the undeliverable addresses from the frame, RTI analysts repeated the deduplication procedure and compared the post-intervention monitoring period addresses to the list of victim addresses in the experiment to identify whether victims in the experiment responded to a subsequent mail scam.

1.4.3 Survey

In the final phase of the MMEFI Study, all individuals from the initial three lists of addresses provided by the USPIS were invited to complete a survey. After the undeliverable addresses were removed from the list, the frame included 4,081 unique addresses. As noted, the survey was designed to learn more about the characteristics of victims for whom the mailed interventions are effective at preventing revictimization, and whether the interventions had any unintended, unexpected, positive, or negative effects on seniors and other vulnerable victims. Since the address lists provided by the USPIS did not include any information about the victims living in the households, the survey data provided context for the intervention findings and assistance in determining whether extra safeguards should be implemented to prevent any undue trauma from a similar mailed intervention.

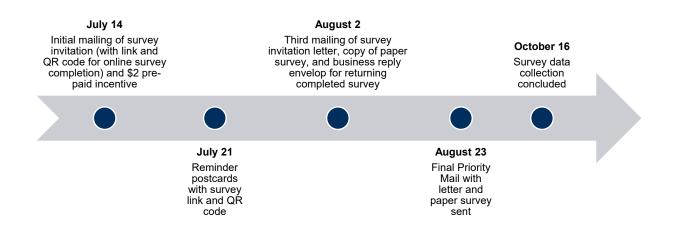
The survey was multi-mode with a web-based option and a mailed paper-and-pencil version. Because web-based surveys reduce the potential for errors in skip patterns and marked responses and are less expensive, addresses were first offered the web-based option. For the first mailing, each address received a letter explaining the purpose of the survey, informing respondents that participation was entirely voluntary, and providing a unique link to the survey. To increase response rates, a QR code a type of two-dimensional matrix barcode, was also included with instructions on how to access the online survey.

To increase credibility, the invitation letter was co-branded with the RTI International, USPIS, and University of Minnesota logos. We included a \$2 cash stipend with the initial letter, following the example of the Bureau of Justice Statistics' Local Area Crime Survey, a mailed survey that received a 47% response rate and collected information from more than 94,000 households about experiences with victimization (Brick et al., 2020). The pre-paid incentive was a U.S. \$2 bill, a collectable note that could increase response rates due to the relative rarity of and interest in the unique bill. The bill was taped into the envelope so that the corner could be seen through the clear window of the envelop. Knowing that the potential respondents were receiving promises of future payment from scammers, we did not offer a promised incentive.

The follow-up survey was designed to be completed in no more than 15 minutes. Respondents were asked to complete and return the survey within 2 weeks. After the 2 weeks, RTI started a

postal nonresponse strategy that involved issuing a postcard reminder, mailing a paper copy of the survey, and sending a final copy of the survey by Priority Mail. Priority Mail was used in the last stage of nonresponse follow-up to emphasize the urgency and value of the response, and no subsequent refusal conversion efforts were made. The survey research protocols for the protection of human subjects were developed by the team and ultimately approved by the Institutional Review Boards of RTI, the University of Minnesota, and the National Institute of Justice on June 23, 2023. **Figure 1-2** shows the timeline for the survey mailings.

Figure 1-2. Timeline for Follow-up Survey Mailings



The survey data collection was concluded on October 16, 2023, as survey responses had steadily dwindled. Ultimately, we collected 144 web-based surveys and 789 paper-and-pencil surveys for a total of 933 completes and an overall response rate of 23%. We believe this relatively high response rate was because this specific population has already demonstrated a propensity to respond to mail correspondence. Previous research has shown that older persons generally respond to surveys at a higher rate than younger ones (Bech & Kristensen, 2009; Tolonen et al., 2006; Watson & Wooden, 2010), perhaps increasing the likelihood that they are targeted by mass marketing fraud.

1.5 Expected Applicability/Impact

To date, this project is one of the largest, most comprehensive, and rigorous efforts to test an intervention to prevent repeat mass marketing fraud victimization. From a research perspective, the study represents the first time that data collected by perpetrators have been used to examine fraud victimization over a multi-year period. Most fraud victim research has relied on individuals to self-report their victimization experiences. The self-report methodology has known reliability issues due to challenges with victim recall or lack of knowledge or acknowledgment of victimization. For instance, studies have found that victims aged 55 or older are significantly less likely to acknowledge fraud victimization in self-report surveys compared with younger victims (Pak & Shadel, 2011). The information obtained through the CRM databases does not suffer from the same potential bias as self-report studies. Thus, findings from this study will have utility for comparison against other self-report studies to better understand the magnitude of underreporting. The findings from the secondary data analysis will also shed light on the frequency of victim responses to scam solicitations, the amount of money paid in response to individual scams, and the total accumulation of monetary loss in a way that self-report studies have previously not been able to do.

Similarly, prior studies of the effectiveness of fraud interventions have relied on the use of hypothetical or mock scam scenarios to determine changes in fraud susceptibility. Because this study uses observed behavior to assess the effectiveness of the intervention and rates of actual repeat fraud victimization, it will serve as a bellwether for future studies examining the impact of interventions on fraud behavior.

Finally, results from the study could directly inform the actions that the USPIS and other consumer protection and advocacy groups take in responding to mass marketing mail fraud. This study sheds light on the value of the USPIS continuing to implement a mailed intervention and the potential impact this intervention could have on rates of repeat victimization.

Additionally, this study can inform the development of similar interventions and prevention messaging to be deployed in other settings (e.g., online or in person) by other organizations or agencies focused on reducing rates of repeat fraud victimization, particularly among older adults.

2. Participants and Collaborators

2.1 Advisory Board

To assist with developing the intervention materials and designing the survey, we convened an Expert Panel of practitioners and researchers who work directly with fraud victims and a psychologist with expertise on behavior modification. Panel members included Greg Walton, a Professor of Psychology at Stanford University; Gary Mottola, Research Director at the FINRA Investor Education Foundation; Melodye Kleinman, former Executive Director at the National Telemarketing Victim Call Center; Amy Nofziger, Director of Victim Support for AARP's Fraud Watch Network; and Kate Lawrence, former Fraud Prevention Coordinator for USPIS.

The Expert Panel met three times virtually during the study period to discuss the intervention conditions, review interview findings, and provide feedback on early drafts of the materials. The first Expert Panel meeting was held in August 2020 and focused on introducing the experts to the project and proposed activities, including the planned approaches for the intervention. Based on input from Panel members, we altered the content of the final intervention condition. Instead of repeat mailings with the same education information and call to action, we developed novel materials for each separate mailing: a newspaper, flyer, brochure, and thank you card. The Expert Panel also suggested including a small item in an early mailing to encourage victims to open future mailings from USPIS. Therefore, we added a "Fraud Fighter" magnet to the final condition. Panel members also advised subtle alterations to the text in various mailings to reinforce the "Fraud Fighter" mentality.

The Expert Panel recommended that we speak to former mail fraud victims to better understand their motivations for responding to mail scam solicitations. We met with the Expert Panel in October 2020 to talk through the structure and approach to asking the questions and eliciting feedback from victims, what to expect from their responses, and how to overcome the

challenges of not conducting face-to-face interviews as initially planned due to COVID-19. The Expert Panel reviewed our interview guide and suggested several additional questions and revisions to the wording. A third virtual meeting was held in June and focused on findings from the victim interviews and the development of the intervention materials.

The Expert Panel also provided written feedback on a draft of the survey instrument. Panel members returned copies with their mark-up. Based on this feedback, we revised the survey to make it more comprehensible to the intended audiences (e.g., we simplified the language, added labels to several of the Likert scale items), and altered the phrasing of some questions measuring victimization by other types of fraud.

2.2 Interviews with Persons Impacted by Fraud

With recruitment assistance from the USPIS, we interviewed three former mail fraud victims and two adult children of mail fraud victims to obtain their perspectives on why they (or their parent) responded to mass marketing fraud solicitations. The information learned through the interviews was designed to help inform the development of the intervention materials. Interviews were

Table 2-1.

conducted via Zoom and were facilitated by one or both co-investigators on the study. All participants provided verbal consent. **Table 2-1** presents descriptive information about the participants, and **Appendix B** presents more details about the recruitment procedure, interview guide and procedures, and detailed findings.

	n	%
Male	3	60
Female	2	40
Victim	3	60
Adult child of victim	2	40
50–59	2	40
65–69	1	20
	Female Victim Adult child of victim 50–59	Male3Female2Victim3Adult child of victim250–592

Victim Interviewees by Sex, Victim Status and Age Range

Key Findings and Themes

Some participants described receiving (or their parent receiving) up to 10 pieces of mail per day, but most said they (or their parent) received about 3–5 pieces of mail per day. Victims who stopped responding to scams added that the amount of fraudulent mail they receive dropped off quickly after they stopped responding; one victim recalled that after not responding to o or 2 letters from a scammer, the scammer stopped sending them mail altogether.

Victims described the scam mail they received as appearing to come from Publisher's Clearinghouse, offering fortune telling or palm reading services, offering sweepstakes lists (e.g., a list that tells the recipient which sweepstakes are going on right now and encourages them to send money to learn about more sweepstakes and/or improve their chances), or being from foreign-sounding entities. Among their reasons for responding to scam mail, victims cited enjoying gambling and treating the scams like a game at the casino; feeling lonely or bored (especially with COVID-19 making it difficult to socialize) and looking to fill a void; and truly believing that they had won and responding to claim their winnings. One victim also described daydreaming that if they won, all their financial problems would be resolved. Another described the offer of potential prize money as a "blessing." Adult children of victims reported their parents' primary reasons for responding as dementia/mental decline; wanting to win a large sum of money to leave behind as inheritance for children and grandchildren; and being depressed or lonely since the passing of a spouse.

Victims described not telling many people (or anyone) about the scam because they felt embarrassed, did not want to share information until the winnings arrived, and/or did not want to be talked out of responding to fraudulent opportunities. Some adult children of victims described only finding out about their parents' involvement due to something else. One found out that their parent was responding to scams when beginning estate planning with their parent and a

financial advisor; another described learning about their parent's involvement when they became an agent under power of attorney.

Two victims described receiving something after interacting with scam mail, but neither was the promised or expected prize: one victim received some small pieces of jewelry, and the other received a small toy/joke prize (e.g., the prize promised was a bicycle, and they received a miniature toy bicycle instead). One victim and the two adult children of victims did not receive any prizes (to their children's knowledge). One victim's total losses were about \$50,000– \$60,000; other victims were unable to estimate their total losses.

When asked to recall any signs that the letters were fake, victims described that they had to "pay to play," as well as the fact that they only had a limited amount of time to respond. Another victim described a scam letter that asked him to send money to an address that the victim knew to not have a business located there (it was a local highway, not a commercial street). The same victim also described a letter that advised them that they had won a large prize but that they needed to pay the customs processing fee. One victim admitted to having an inkling that the mail may have been fraudulent, but they were so addicted to daydreaming about the potential winnings that they ignored their instincts and continued to engage with the scammers.

One victim described having no idea that they had participated in a scam until they heard from the USPIS. Had they received a letter from the USPIS that their address was found in a mail fraud case, they would have stopped participating right away.

The following were among the advice participants would give to others, or to their younger selves:

- "Pay to play" games are not legitimate.
- If it seems too good to be true, it probably is.

- Sending money to an unknown address (whether cash, check, money order, or gift card) is not legitimate.
- If there is a return address or phone number, check the address or call the phone number to determine whether it is legitimate.
- Show any mail requests to a trusted friend or family member (such as an attorney) who can provide guidance on whether to respond.

Victims noted that they consulted AARP and their local news stations for information on scams. Two participants felt that knowing that the money they sent to scammers was going to criminals would have motivated them to stop responding. Another victim noted that learning that there was zero chance of winning a prize (rather than "a small chance") would have compelled them to stop sooner. One of the adult children of a victim described their parent as having sent in small sums (\$5–\$10) over the course of many years and felt that their parent probably saw that as a small risk that might have a big payoff eventually.

2.3 Cognitive Testing of Intervention Materials

The cognitive interviews focused on the effectiveness and clarity of the messaging of the drafted intervention materials, the look and content, perceptions of what the messages communicated, the likelihood of completing and returning the tear-off advice card, and how memorable the materials were. The complete cognitive interview report is available in **Appendix C**.

30

2.3.1 Recruitment and Interview Procedures

Participants were recruited through Minnesota and California organizations that work with older adults (n=11) and via Facebook (n=18). We attempted to recruit 10 participants aged 50-64, 10 participants aged 65-74, and 10 participants aged 75 or older,

Actual Participants								
Survey Characteristic	Total Target Participants	Actual Participants Completed						
	Type of Interview							
Victim	20	17						
Non-Victim	10	13						
	Age							
50–64	10	9						
65–74	10	14						
75+	10	7						

30

Table 2.2 Characteristics of Target Dertisinants and

including 20 older adults who had previously been victims of fraud, and 10 individuals who were not victims. In both cases, participants were sent a copy of the study materials via FedEx. All participants received 7 items but were randomized for whether they would receive Version A or B of the "call to action" Fraud Fighter brochure, and Version A or B of the "Meet Your Team" flyer. The characteristics of participants are presented in Table 2-2.

Total count

Most interviews were conducted over Zoom and lasted 1 hour, although two Minnesota-based participants were interviewed in person in their homes by the co-investigator. All participants provided verbal consent to participate.

Participant Feedback on Intervention Materials

Standard letter: Some participants found the standard letter to be confusing and wanted the text to be clearer and more concise. Participants generally affirmed that they learned something new from reading the letter. In general, participants did not like the format of the fraud detection tips on the reverse side, but they found the information and examples to be useful. Most participants said they would feel relieved after receiving the letter and knowing the USPIS is looking out for them (even after some initial embarrassment). Most participants also noted that getting this letter would make them review their mail more carefully.

Adaptations to the Standard Letter: We shortened the text by removing phrases that were confusing to participants. We also changed the mail scam education on the reverse side by adding another example fraud solicitation, using a shaded background, and placing the education tips all on the right side of the letter.

Call-to-action brochure: Initial impressions of the call-to-action brochure were largely positive, with respondents noting the brochure was engaging, informative, and provided steps on how to fight fraud (including sharing information with family and friends). They appreciated that they were being asked for help from Postal Inspectors to stop scams and that those who fall for scams are not alone. When asked what it means to be a Fraud Fighter, respondents largely responded that a Fraud Fighter is someone who reports fraud, helps catch the scammers, informs other people about fraud, and is "on alert" about fraud. Most respondents said that being a Fraud Fighter seemed like not too much effort.

Some victims did not understand that they were being asked to return the completed prompts. For example, it was not clear that the brochure was meant to be cut and respondents encouraged a perforated line to make it clearer. Respondents mentioned liking the fact that their responses to the brochure would be used to help other consumers but also noted that they were not sure if they would respond. Several respondents indicated that sharing a personal fraud story seems to make more sense than providing tips to USPIS, because USPIS should know about those tips anyway. When asked how USPIS should use the advice that it collects from Fraud Fighters via the brochure mail-in, respondents suggested pulling it all into a database or report and following up with Fraud Fighters to confirm receipt of their advice, to thank them, and to keep them informed of plans to fight fraud.

Adaptations to the call-to-action brochure: We changed the fold of the brochure and replaced the main image with cropped photo of a person filling out the response card. This was to help demonstrate the intended behavior. We developed a new stand-alone prompt that states: "Please share your advice to others about ways to protect themselves from fraud. Fill out the back of this card and mail it to USPIS in the enclosed postage paid envelope."

Meet Your Team flyer: We tested two versions of the flyer with different images. Feedback on the images was mixed, with some participants pointing out that they appreciated the race and gender diversity of those presented and that they were real employees of the USPIS. Others did not like that the agents were smiling (Version A) or that in every picture an agent was holding up their badge (Version B). Other impressions of the flyer were largely positive. Victims were pleased to learn there was an agency that combats mail fraud and that the flyer provided actionable steps. Some respondents (largely victims) said it makes them feel more connected to other Fraud Fighters and the USPIS. When asked how likely they were to take the action steps, respondents largely said that they would and that the steps for reporting fraudulent letters, ignoring scams, and warning friends and family made sense.

Adaptations to the flyer: Because respondents preferred the image that had diversity and more of a law enforcement feel, we replaced the image with a photo of USPIS employees in their law enforcement uniforms. We also spelled out "USPIS" at the top of the flyer to give an additional reminder of what the acronym stands for.

Newsletter tabloid: In general, participants found the stories to be engaging, realistic, believable, and relevant to their life, but they were divided on whether they liked the newsletter format. Participants who were self-professed "newspaper and crossword lovers" appreciated the newsletter, but others thought it was gimmicky. Most participants said they would send potential fraud letters to the USPIS per the instructions.

Adaptations to the newsletter: We added several details to the Fraud Fighter news stories to reflect new scams that the USPIS intercepted in the past year. The request to send in scam letters using an enclosed pre-addressed, pre-paid envelope was removed, since the USPIS was not able to provide envelopes and return labels to the research team. Instead, the image on the

2-8

back of the newsletter was expanded, and the call-to-action instructions were revised to remind receivers to report fraud to the toll-free reporting line.

Scammer brochure: In general, participants liked this flyer and had only a few minor suggestions, such as changing several images. Participants who mentioned learning something new, most commonly cited learning about the connections between fraud and other criminal activity and that scammers keep lists and share the lists with other scammers. Victims were more likely than non-victims to say they appreciated the brochure, and non-victims were more likely to say they might just throw it away without reading.

Adaptations to the scammer brochure: We increased the contrast of the map so that the countries are more visible against the darker background. We also replaced three of the images to better reflect the scammers' activities and to remove the images that did not appeal to participants.

Thank you card: Victims were more likely than non-victims to appreciate the card and understand its purpose. Most participants liked the format and the color scheme. The majority of participants found the bookmark to be helpful information and said they would keep it for later.

Adaptations to the thank you card: We removed language about sending back the enclosed postcard as we are no longer offering that option.

General feedback: Most participants stated that the information made them realize that mail fraud was an important issue and understand how to protect themselves. If they were to actually receive the letters, many said they would feel embarrassed for having given money to scammers or would be mad that the information got to them *after* they fell for a scam. However, the majority of participants, despite citing embarrassment, would feel grateful that someone was on the case, watching out for them and trying to get their money back. Several victims stated that it may feel embarrassing to receive the mailings, but being protected and informed

outweighs those negative feelings. Most participants said that they would feel empowered by the letters because they knew that someone is working to protect them, and they had information on what steps to take to detect and prevent fraud and how to inform friends and family.

2.4 Experiment Participants

As noted in Section 1, the initial list of victim addresses provided by the USPIS for the intervention experiment included 2,857 deduplicated addresses. As seen in Table 2-3, of the 2,857 intervention experiment addresses, 2,000 (~70%) were also present in the CRM data from scams operating between 1999 and 2018. We labeled this group as the "long-term repeat victims" because their experiences with mass marketing fraud were known to span nearly 4 years. Of the remaining 857 addresses that were not present in the CRM databases, 379 had appeared multiple times on the roster and were labeled "repeat victim," and 478 appeared only once on the initial roster and were identified as "new victims."

Attempting to mail the intervention materials and survey to these addresses highlighted that many of the addresses on the initial list were not good addresses. This could have been because they were misread by the mail reader technology or because there was no longer a resident living at that address. Any addresses that bounced back one or more times as undeliverable following either an intervention mailing or survey mailing were removed from the intervention. This resulted in a final experiment sample of 2,253 addresses, with 766 in the control group, 763 in treatment group 1, and 724 in treatment group 2. About 75% of the final sample were long-term repeat victims, 13% were repeat victims, and 12% were new, first-time victims.

2-10

Addresses	Total	Control group	Treatment 1	Treatment 2
Initial deduplicated list	2,857	952	953	952
Long-term repeat victims ^a	2,000	667	667	666
Repeat victims ^b	379	159	160	159
New victims	478	126	126	127
Returned mail	604	186	190	228
Final experiment sample	2,253	766	763	724
Long-term repeat victims ^a	1,682	570	573	539
Repeat victims ^b	297	106	98	93
New victims	274	90	92	92

Table 2-3. Count of Addresses Included in the Intervention Experiment

^a Includes addresses that were present in the historical customer relationship management data seized by the USPIS.

^b Includes addresses that were not in the historical data but were included multiple times in the intervention experiment list.

No information was known about the intervention experiment participants, unless they responded to the follow-up survey after the experiment was complete. Overall, 562 (25%) of the 2,253 addresses in the experiment responded to the survey. **Tables 2-4** and **2-5** show the characteristics of intervention experiment participants, by self-reported demographic and household characteristics. There were no significant differences in the known characteristics of participants across the control group or two treatment groups, suggesting that the randomization worked as intended. However, it should be noted that for addresses with more than one household member, there is no way to know whether the person who completed the survey is the same person who responded to the mail scams or received the intervention materials.

Table 2-4. Demographic Characteristics of Known Victims Included in the Intervention Experiment Experiment

		Control group		Treatr	Treatment 1		ment 2
	Characteristics	Number	Percent	Number	Percent	Number	Percent
Total		766	100.0	763	100.0	724	100.0
	No survey received	576	75.2	545	71.4	570	78.7
	Survey completed	190	24.8	218	28.6	154	21.3
Sex							
	Male	81	42.6	94	43.1	72	46.8
	Female	93	48.9	105	48.2	70	45.5
	Other	3	1.6	8	3.7	4	2.6
	Unknown	13	6.8	11	5.0	8	5.2
Hispa	nic Origin						
	Yes	19	10.0	15	6.9	22	14.3
	No	152	80.0	183	83.9	118	76.6
	Unknown	19	10.0	20	9.2	14	9.1
Race							
	White	107	53.2	116	50.4	93	57.8
	Black	44	21.9	57	24.8	29	18.0
	American Indian or Alaska Native	9	4.5	11	4.8	7	4.3
	Asian	12	6.0	14	6.1	7	4.3
	Other ^a	9	4.5	11	4.8	13	8.1
	Unknown	20	10.0	21	9.1	12	7.5
Age							
	18-60	13	6.8	20	9.3	8	5.1
	61-70	37	19.5	32	14.8	25	16.0
	71-80	47	24.7	67	31.0	41	26.3
	81+	73	38.4	71	32.9	54	34.6
	Unknown	20	10.5	26	12.0	28	17.9
Educa	ation						
	No high school diploma or equivalent	14	7.4	19	8.7	19	12.3
	High school graduate, diploma or GED	52	27.4	57	26.1	42	27.3
	Some college credit, no degree	25	13.2	44	20.2	22	14.3
	Trade/technical/vocational training	22	11.6	29	13.3	20	13.0
	Associate degree	16	8.4	14	6.4	10	6.5
	Bachelor's degree	20	10.5	21	9.6	21	13.6
	Master's, Professional, Doctorate	22	11.6	22	10.1	11	7.1
	Unknown	19	10.0	12	5.5	9	5.8

^aIncludes Native Hawaiians and Other Pacific Islanders

Table 2-5. Household Characteristics of Known Victims Included in the Intervention Experiment Experiment

	Gro	up 1 Group 2		up 2	Group 3	
Characteristics	Number	Percent	Number	Percent	Number	Percent
Total	766	100.0	763	100.0	724	100.0
No survey received	576	75.2	545	71.4	570	78.7
Marital status						
Married / domestic partnership	41	21.6	58	26.6	37	24.0
Widowed	71	37.4	67	30.7	53	34.4
Divorced	32	16.8	42	19.3	25	16.3
Separated	3	1.6	4	1.8	4	2.
Never married	27	14.2	33	15.1	21	13.
Unknown	16	8.4	14	6.4	14	9.
Living arrangement						
Live alone	89	44.1	95	42.0	78	49.
Live with a spouse/partner	40	19.8	60	26.5	35	22.
Live with dependent children or adult children	31	15.3	25	11.1	16	10.
Live with extended family, such as siblings or grandchildren	17	8.4	20	8.8	10	6.
Live with roommates	6	3.0	5	2.2	7	4.
Unknown	19	9.4	21	9.3	12	7.
Housing						
Rent	57	30.0	74	33.9	47	30.
Own	101	53.2	112	51.4	86	55.
Other	14	7.4	17	7.8	9	5.
Unknown	18	9.5	15	6.9	12	7.
Household income						
Under \$20,000	48	25.3	58	26.6	42	27.
\$20,001 to \$50,000	47	24.7	56	25.7	47	30.
\$50,001 to \$100,000	19	10.0	22	10.1	18	11.
\$100,001 to \$150,000	6	3.2	9	4.1	4	2.
\$151,000 or more	7	3.7	4	1.8	3	1.
Don't Remember	16	8.4	17	7.8	9	5.
Prefer not to say	24	12.6	35	16.1	26	16.
Unknown	23	12.1	17	7.8	5	3.2

2.5 Survey Respondents

As noted, the survey response rate among intervention experiment participants was 25%. **Table 2-6** shows the distribution of survey respondents across the three experimental groups and by their number of known incidents of mail fraud. The response rates were fairly consistent across the three experimental groups, with treatment group 2 having slightly lower response rates (27%) than treatment group 1 (40%) and the control group (33%). This was particularly true among those respondents only known to have responded to one mail fraud solicitation.

Experiment group and number of victimizations	Nonrespondents	Resp	oondents
		Number	Percent
Total	1,691	562	25
Control group	576	190	33
1	67	14	17
2-5	56	28	33
6-19	152	33	18
20 or more	301	115	28
Treatment 1	545	218	40
1	66	23	26
2-5	67	31	32
6-19	118	44	27
20 or more	294	120	29
Treatment 2	570	164	27
1	76	6	7
2-5	77	20	21
6-19	107	31	22
20 or more	310	97	24

 Table 2-6.
 Survey Response by Experimental Group and Number of Known Mail Fraud

 Victimizations

Note: Includes victimizations identified during the experiment period and victimization in the historic data if the address was linked to the scammer data.

Tables 2-7 and **2-8** show the demographic and household characteristics for all survey respondents, regardless of which experimental group they were in. The majority of respondents were white, non-Hispanic, age 71 or older, had less than a college degree, and had a household income of less than \$50,000 per year. About 45% lived alone.

	Characteristics	Number	Percent
	Total	2,253	100.0
	No Survey Completed	1,691	75.1
	Survey Completed	562	24.9
Sex			
	Male	247	44.0
	Female	268	47.7
	Other (Transgender, Some other way, None of these)	15	2.7
	Unknown	32	5.7
Hispani	ic origin		
	Yes	56	10.0
	No	453	80.6
	Unknown	53	9.4
Race			
	White	316	53.4
	Black	130	22.0
	American Indian or Alaska Native	27	4.6
	Asian	33	5.6
	Native Hawaiian or Other Pacific Islander	33	5.6
	Unknown	53	9.0
Age			
	18-60	41	7.3
	61-70	94	16.7
	71-80	155	27.6
	81+	198	35.2
	Unknown	74	13.2
Educati	ion		
	No high school diploma or equivalent	52	9.3
	High school graduate, diploma or GED	151	26.9
	Some college credit, no degree	91	16.2
	Trade/technical/vocational training	71	12.6
	Associate's degree	40	7.1
	Bachelor's degree	62	11.0
	Master's, Professional, Doctorate	55	9.8
	Unknown	40	7.1

Table 2-7. Demographic Characteristics of Survey Respondents

Characteristics	Number	Percent
Total	2,253	100.0
No Survey Completed	1,691	75.1
Survey Completed	562	24.9
Marital status		
Married / domestic partnership	136	24.2
Widowed	191	34.0
Divorced	99	17.6
Separated	11	2.0
Never married	81	14.4
Unknown	44	7.8
Living arrangement		
Live alone	262	44.7
Live with a spouse/partner	135	23.0
Live with dependent children or adult children	72	12.3
Live with extended family, such as siblings or grandchildren	47	8.0
Live with roommates	18	3.1
Unknown	52	8.9
Housing		
Rent	178	31.7
Own	299	53.2
Other	40	7.1
Unknown	45	8.0
Household income		
Under \$20,000	148	31.2
\$20,001 to \$50,000	150	31.6
\$50,001 to \$100,000	59	12.4
\$100,001 to \$150,000	19	4.0
\$151,000 to \$200,000	14	3.0
\$200,001 or more	42	8.9
Unknown	42	8.9

Table 2-8. Household Characteristics of Survey Respondents

3. Changes to the Originally Proposed Design

3.1 Reduced Sample Sizes

The USPIS originally estimated that they intercepted 4,000–5,000 payment envelops per month that victims were sending in response to scam solicitations. This estimate was based on pre-COVID levels of mail scam prevalence and based on the USPIS having a contractor stationed at the JFK Airport USPS facility in New York to monitor outgoing mail patterns and identify and intercept mail likely being sent to a scammer's address.

When designing the intervention experiment, the project team used the estimates from the USPIS and assumed a 50% revictimization rate, meaning that only half of the intercepted payment envelopes would have a unique return address. The team then powered the intervention based on receiving 10,000 return addresses from payment envelopes intercepted by the USPIS over a 5-month period.

Our assumptions did not factor in the COVID-19 pandemic, which impacted the frequency with which mail traveled out of and into the United States, causing many scammers to change their tactics and switch to other modes of engaging in fraud. During the pandemic and afterward, the USPIS reported seeing a lower volume of scam mail and responses to scam mail. Additionally, the USPIS faced challenges with consistently filling the position at JFK Airport throughout the project period. When the post was vacant, mail scam payment envelopes were intercepted at a much lower rate.

The address file that the USPIS ultimately provided for the intervention experiment covered a 17-month period and included about 26,230 records. Of those, only 16,903 were valid addresses that included a street name and number, as well as a city, state, and ZIP code, all of which is critical information necessary for mail to be delivered. Of the nearly 17,000 valid addresses, only 2,857 were unique, indicating a significantly higher percentage of repeat victims

(88%) than the 50% anticipated. This higher percentage may be due to the longer period during which payment envelops had to be collected, or it may be due to mail scammers increasing their targeting of victims who consistently respond to the solicitations. Regardless, the 2,857 addresses represented a considerably smaller sample size than the target of 10,000.

The UPSIS sent two additional smaller lists of addresses collected just prior to the intervention. However, these lists were provided in May after RTI had already started the intervention experiment mailings. The lists, which provided an additional 1,531 unique addresses, were initially added to the control group of the experiment, but closer inspection of the addresses revealed substantial differences in the subsequent lists in terms of rates of repeat victimization within the list and in the addresses that linked to addresses from the historical CRM data. Because these victims seemed so different from the other victims in the sample, they were ultimately not included in the intervention experiment. Thus, the intervention experiment sample size was less than 30% of what we had estimated when powering the experiment.

3.2 Changes to One of the Experimental Conditions

The intervention experiment was initially intended to include one control group and three treatment groups. Because of the substantially lower sample sizes, the project team decided to drop the second experimental condition, which was the USPIS letter and the call-to-action Fraud Fighter brochure mailed together. Dropping this experimental condition meant that we could have approximately 952 addresses in the control group and each of the two remaining treatment groups. If we kept all three treatment groups, each of the four groups would have had just over 700 addresses per group.

3.3 Shorter Intervention Follow-up Period

The initial experiment was designed to have a post-intervention monitoring period of 6 months to 1 year, depending in part of findings from the secondary data analysis. Because of delays in

getting the intervention materials approved and receiving the intervention address list, the experiment started on March 20, 2023, several months later than anticipated. The final mailing for treatment group 2 was mailed in early May.

In July of 2023, the USPIS sent the first batch of post-intervention addresses. These addresses were taken from payment envelops interdicted between the end of March 2023 and the end of July 2023. For the addresses that received the single mailed letter, this represented a 4-month post-intervention monitoring period, but for the addresses that received their final mailing in early May, the post-intervention monitoring period was only about 2.5 months. The USPIS intended to provide a second batch of post-intervention addresses in September 2023, covering an additional 2 months. However, when we reached out to the USPIS to request the final batch of addresses, we were informed that they would not be able to provide the data because the contractor position at the JFK Airport USPS facility was vacated shortly after sending the July batch of addresses and they had not been able to fill it. Without this contractor, the USPIS would not be able to conduct the rigorous monitoring necessary to provide us with a complete list that could be used for monitoring purposes. Thus, our monitoring period ended up being shorter than planned.

4. Findings

4.1 Secondary Data Analysis

4.1.1 Prevalence of Mail Fraud Victimization

We used administrative data originally compiled by four separate mail scam enterprises to examine the cost, incidence, and prevalence of repeat mass marketing scam victimization. **Figure 4-1** presents the prevalence of each of the four scams (payment envelopes received) that were perpetrated between 1999 and 2018. The four scammer datasets included a combined total of 1,383,755 unique victims and 11,870,085 separate victimization incidents. Of the total victimization incidents, 54% involved psychic scams, and 46% involved sweepstakes/prize/lottery scams.

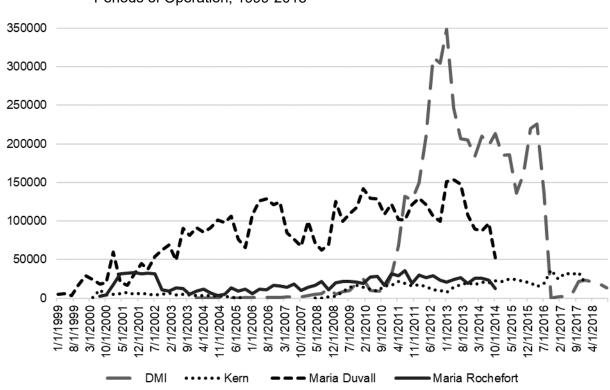
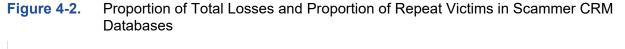


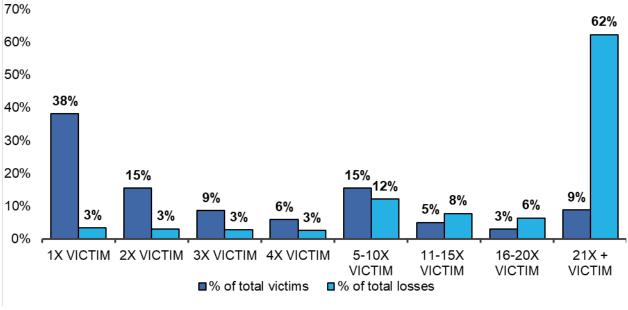
Figure 4-1. Number of Victimizations (Payment Envelopes Received) During the Scammers' Periods of Operation, 1999-2018

N=11,870,085

Frequency of Repeat Victimization

The rate of repeat mail fraud victimization was very high. Nearly 62% of victims in the sample paid money in response to multiple mail scam solicitations. Among all victims, the average number of victimization incidents was 9. As shown in **Figure 4-2**, approximately 38% of victims paid only 1 time in response to a fraudulent mail solicitation, 15% of victims paid 2 times, 9% paid 3 times, 6% paid 4 times, and 15% paid between 5 and 10 times. Victims who responded more than 20 times, who we define as "chronic victims," represent 9% of the sample. These individuals averaged 59 victimization incidents per person. The average frequency of repeat victimization was higher for sweepstakes/prize/lottery scams (8 incidents) than for psychic scams (5 incidents).





N=1,383,755

Cost of Victimization

The average total loss among victims was \$251 per person. Altogether, victims paid

\$347,100,135 across the four scams. As depicted in Figure 4-3, chronic victims accounted for

most of these losses. Chronic victims paid an average of \$1,771 per person, totaling more than \$216 million: 62% of the scammers' revenue. The 38% of victims who paid only 1 time lost an average of just \$22 per person, and their total losses amount to \$11,354,694: only 3% of the scammers' revenue. The average payment in response to a single sweepstakes/prize/lottery scam solicitation was only \$24, and the average payment in response to a single psychic scam solicitation was \$34.

Changes in Payment Amounts Over Time

Victims did not pay increasing amounts of money in response to mail fraud solicitations over time. As shown in **Figure 4-3**, sweepstakes/prize/lottery victims enclosed an average of \$24 in response to the first solicitation letter and \$22 in response to the second, which is a decrease in the amount lost. This amount stays relatively stable between the second and twentieth incident. The payment amount only increases to an average of \$25 after the twentieth sweepstakes/prize/lottery scam incident. For psychic scams, the first payment is \$20, on average. It increases to \$32, on average, the second time the victim pays, but after the second incident, payments increase only marginally (to \$37, on average) after many subsequent victimizations.

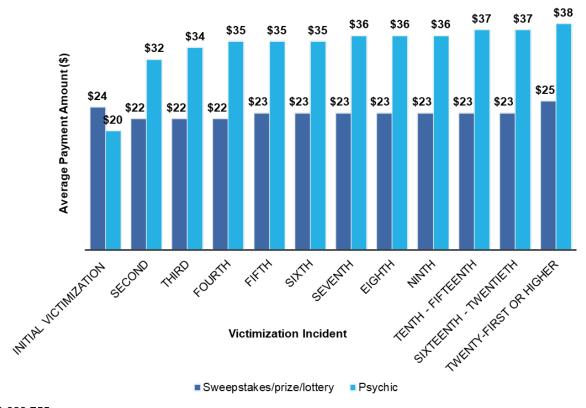
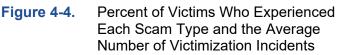


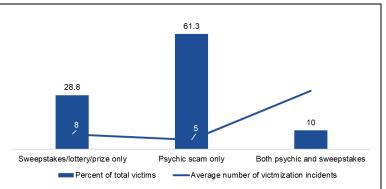
Figure 4-3. Average Payment Amount Per Solicitation Over Consecutive Victimization Incidents

N=1,383,755

Repeat Victimization across Scam Types

As shown in **Figure 4-4**, repeat victimization involving different types of mail fraud was not very common in the available data. Only 10% of victims responded to both a psychic scam *and* a sweepstakes/ prize/lottery scam. Of these individuals, the average number of





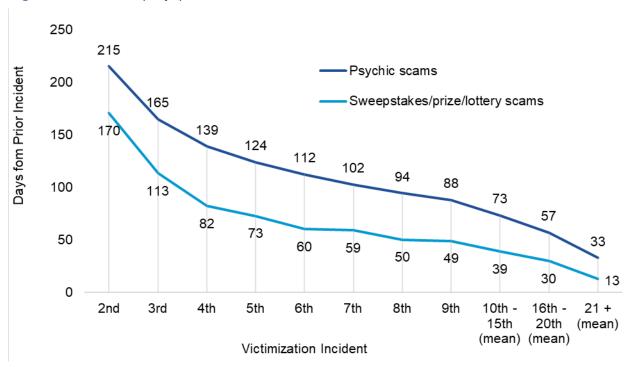
repeat victimization incidents was 31. Eighty-one percent of victims were in only one scammer dataset and responded 4 times to the same criminal enterprises' solicitations, on average.

Fifteen percent of victims were in 2 datasets, 3% were in 3 datasets, and just 1% of the victims

were in all 4. For those who appeared in all 4 scammers' datasets, the mean number of victimization incidents was 85.

Time Between Victimization Incidents

Figure 4-5 depicts the average number of days between victimization incidents over time. We found that the more times a victim responded to mail scam solicitations, the shorter the interval became between victimization incidents. The trajectory shows that between the first and second incident, the average duration for both scam types was 201 days, but by the twenty-first or higher victimization incident, the time between sequential incidents was only 20 days, on average.





N=10,486,330

Although the pattern of decreasing duration between incidents was similar across scam types, the time between incidents was significantly longer for psychic scams than for sweepstakes/prize/lottery scams. Specifically, the overall average time between victimizations incidents for sweepstakes/prize/lottery scams was 36 days, and the average time between psychic scam victimization incidents was more than 3 months (93.6 days). These differences may reflect the frequency with which the various mass marketing fraud enterprises were sending scam solicitations to victim households.

Payment Method

Payment method was consistently recorded only in the DMI dataset, which contained sweepstakes, lottery, and prize solicitations. There were 7,207,709 records available. As show in **Table 4-1**, the most common payment method was check (54%), followed by "unknown"

Table 4-1.

(21%), money order (15%), and credit card (910%). Significantly fewer payments were made with cash (less than 0.1%). "Collect on delivery" was also noted as a payment method but represented less than 0.1% of records.

Demographic Characteristics and Repeat

Victimization

Victim age was recorded for both the Maria Duval and Maria Rochefort psychic scams. As shown in Figure 4-6, results indicate that older victims account for a greater share of total losses and incidents. For example, although adults in their 80s represent only 15% of victims,

they account for 27% of all victimization incidents and 30% of all losses.

Payment Method	Frequency	Percent, %
Check	3,892,485	54.00
Money order	1,112,862	15.44
Credit card	694,125	9.63
Collect on delivery	4,255	0.06
Cash	2,753	0.04
Unknown	1,501,229	20.83

Types of Payment Methods

Recorded in the DMI Dataset

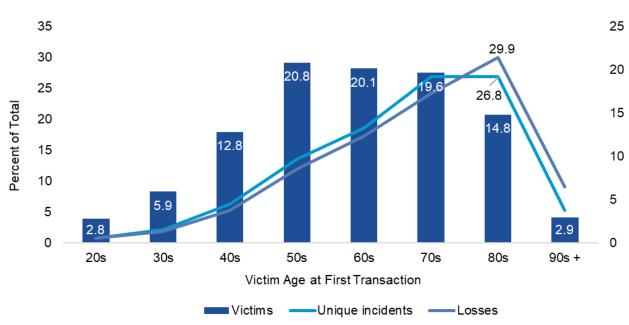


Figure 4-6. The Relationship Between Victim Age at First Victimization, Losses, and Victimization Incidents

N=960,295

We used a gender guesser to estimate the sex of each victim based on their first name. We found that victims estimated as female were approximately 7% less likely to be repeat victims than those estimated as male. We also integrated the Area Deprivation Index in the dataset, a measure of neighborhood disadvantage, and found that victims residing in more impoverished neighborhoods were less likely to be repeat victims, on average, than those from more advantaged neighborhoods.

Seasonality of Mail Fraud

We examined the seasonality of mail fraud victimization using data from all transactions included in the four CRM databases. **Figure 4-7** shows a plot of the monthly counts of victimization incidents (i.e., individual payments sent in response to scam solicitations). The figure focuses on a snapshot of CRM data from 2010 to 2015 when the scams were collectively most active. The trendline in **Figure 4-7** is a rolling 12-month average count of incidents.

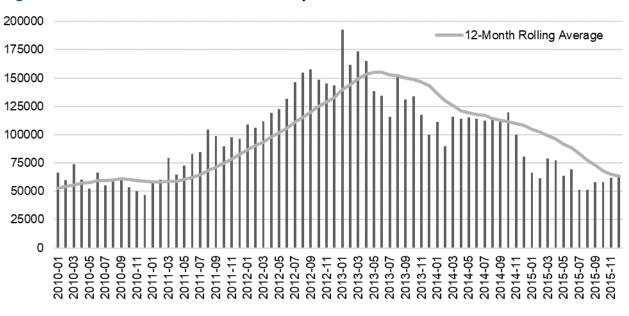


Figure 4-7. Count of Mail Fraud Incidents by Month

N=7,072,519

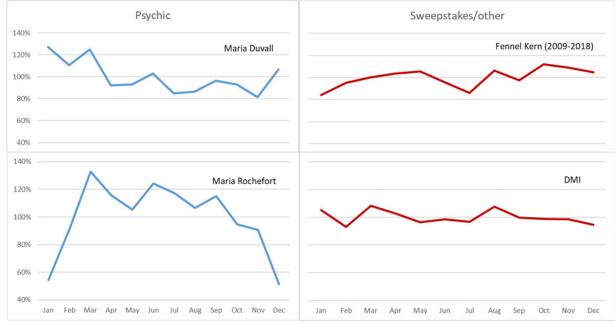
A time series decomposition was used to identify the peak and low seasons for mail fraud. **Table 4-2** shows the calculated repeated seasonal variation (trend + seasonal + residual) by month. As shown, across all scams, March was the peak month for mail fraud, at about 17% higher than the average. The months of October through December represent the low season, with November being the lowest at about 11% lower than average. This pattern of lower scam responses at the end of the year may be due to persons saving money during the holiday season.

There was variability in seasonal patterns across the scam types. **Figure 4-8** shows the seasonality for the four different scam enterprises. In general, the seasonality effects for the sweepstakes scams were less pronounced than for the psychic scams.

Month	Percent, %	Month	Percent, %	Month	Percent, %
January	108	May	98	September	103
February	104	June	104	October	-96
March	117	July	93	November	89
April	96	August	96	December	96

Table 4-2. Calculated Repeated Seasonal Variation of Mail Fraud Incidents, by Month

Figure 4-8. Seasonal Variation of Mail Fraud Incidents, by Type of Scam



N=11,765,672

4.2 Intervention Experiment

Table 4-3 shows the percentage of victims in the intervention experiment who were identified as having responded to a mail fraud solicitation during the post-intervention monitoring period. Results show that the percentage of repeat victims during the post-intervention period was higher among those in the control group compared to those in both treatment groups. Receiving the single letter with educational materials (treatment group 1) resulted in about a 2 percentage point reduction in the percentage of victims who responded to another scam in the 4-month monitoring period compared to victims in the control group. Although this was a modest decline,

it suggests that even a low-cost intervention like the letter could result in less money ending up in scammers' pockets.

Among victims in treatment group 2, who received multiple mailings, there was a statistically significant 5 percentage point reduction in the number of victims who responded to another mail scam solicitation during the monitoring period relative to the control group. In other words, the more intensive intervention resulted in a larger reduction in repeat victimization compared to the one-time letter and no intervention. However, it should be noted that treatment group 2 was still receiving intervention materials during part of the monitoring period, which may contribute to the larger reduction in repeat victimization.

The intervention experiment findings were largely driven by long-term repeat victims, who made up the largest percentage of the experiment sample. Among long-term repeat victims, the single letter treatment resulted in a 3 percentage point reduction in subsequent repeat victimization and the multiple mailings resulted in a 6 percentage point reduction in repeat victimization compared to the control group. Not surprisingly, victims only known to have responded to one scam prior to the intervention were much less likely to respond to a subsequent scam during the follow-up period (7%) than repeat (29%) and long-term repeat victims (29%). Although it was anticipated that the intervention materials would be most effective for this group, both treatment groups only had a 2 percentage point reduction in repeat victimization compared to the control.

Table 4-3.	Number of Victims in the Intervention Experiment Responding to a Mail Scam
	Solicitation in the Post-intervention Monitoring Period, by Control and Treatment
	Groups

			ubsequent scam itation
Type of victim and group	Number of addresses	Number	Percent
Total	2,253	589	26.1
Control group	766	219	28.6
Treatment 1	763	200	26.2
Treatment 2	724	170	23.5
Long-term repeat victimsª	1,682	482	28.7
Control group	570	180	31.6
Treatment 1	573	164	28.6
Treatment 2	539	138	25.6
Repeat victims ^b	297	87	29.3
Control group	106	31	29.2
Treatment 1	98	30	30.6
Treatment 2	93	26	28.0
New victims ^c	274	20	7.3
Control group	90	8	8.9
Treatment 1	92	6	6.5
Treatment 2	92	6	6.5

^a Includes addresses that were present in the historic customer relationship management data seized by the USPIS.

^b Includes addresses that were not in the historic data but appeared multiple times in the initial intervention experiment list.

^c Includes addresses that were not in the historic data and only appeared once in the intervention experiment list.

 Table 4-4 shows the number of times that victims in the intervention experiment responded to

 new scams during the monitoring period. Across the control and treatment groups, a lower

 percentage of new victims responded to a subsequent scam compared to repeat and long-term

 repeat victims.

The distributions of the number of responses to subsequent scams were not significantly

different across the treatment and control groups. However, compared to the control group,

treatment group 1 saw an 8.3% reduction in the rate of repeat victimization, while treatment

group 2 saw a 17.9% reduction in the rate of repeat victimization (not shown in the table).

Type of victim and responses	Contro	trol group Treatm		ment 1 Treat		tment 2	
to new fraud letters	Number	Percent	Number	Percent	Number	Percent	
Long-term repeat victims ^a	570	100.0	573	100.0	539	100.0	
0	390	68.4	409	71.4	401	74.4	
1	101	17.7	80	14.0	63	11.7	
2	27	4.7	35	6.1	28	5.2	
3-5	41	7.2	36	6.3	34	6.3	
6 or more	11	1.9	13	2.3	13	2.4	
Repeat victims ^b	106	100.0	98	100.0	93	100.0	
0	75	70.8	68	69.4	67	72.0	
1	13	12.3	14	14.3	8	8.6	
2	5	4.7	5	5.1	5	5.4	
3 or more	13	12.3	11	11.2	13	14.0	
New victims ^c	90	100.0	92	100.0	92	100.0	
0	82	91.1	86	93.5	86	93.5	
1 or more	8	8.9	6	6.5	6	6.5	

Table 4-4. Prevalence and Counts of New Responses to Scam Mail During the 4 Months Following the Intervention Following the Intervention

^a Includes addresses that were present in the historic customer relationship management data seized by the USPIS.

^b Includes addresses that were not in the historic data but were included multiple times in the intervention experiment list.

^c Includes addresses that were not in the historic data and only appeared once in the intervention experiment list.

We also examined intervention experiment results among victims for whom demographic and household characteristics were known, because they responded to the follow-up survey. **Tables 4.5** and **4.6** show the numbers and percentages of repeat victims during the post-intervention monitoring period by demographic and household characteristics. In part because of the small sample sizes, the analysis revealed few significant differences in repeat victimization across the treatment and control groups by victim and household characteristics. Both interventions appeared to work better for people who reported their race as black than those who reported their race as white and for people who were divorced or separated compared to those who were married.

Table 4-5.Number and Percent of Victims With One or More Scam Mail Responses During
the 4 Months Following the Intervention, by Victim Demographics

		Contro	ol group	Treat	tment 1	Treatment 2	
Ch	aracteristics	Number	Percent	Number	Percent	Number	Percent
Total		64	33.7	70	36.8	58	30.5
Sex							
Male		24	29.6	36	38.3	23	31.9
Fema	ale	34	36.6	30	28.6	31	44.3
Othe	r/Missing	6	37.5	4	21.1	4	33.3
Hispanic ori	gin						
Yes		6	31.6	3	20.0	8	36.4
No		50	32.9	61	33.3	45	38.1
Unkn	iown	8	42.1	6	30.0	5	35.7
Race ^a							
White	e	30	28.0	42	36.2	38	40.9
Black	(18	40.9	15	26.3	8	27.6
Othe	r ^b	9	30.0	11	30.6	6	22.2
Unkn	iown	9	45.0	5	23.8	6	50.0
Age							
70 or	under	12	24.0	12	23.1	9	27.3
71-80	0	15	31.9	19	28.4	20	48.8
81+		27	37.0	35	49.3	20	37.0
Unkn	iown	10	50.0	4	15.4	9	32.1
Education							
High less	school equivalent or	23	34.8	22	28.9	20	32.8
Some degre	e college credit, no ee	14	56.0	16	36.4	12	54.5
	e school or ciate's degree	11	28.9	14	32.6	9	30.0
Bach	elor's degree	7	35.0	6	28.6	7	33.3
	er's, Professional, or orate degree	4	18.2	10	45.5	4	36.4
Unkn	iown	5	26.3	2	16.7	6	66.7

Note: Includes addresses included in the experiment and that responded to the survey

^a Details may not sum to total because respondents could select multiple races.

^b Includes American Indians and Alaska Natives; Asian, Native Hawaiians and Other Pacific Islanders.

Table 4-6.Number and Percent of Victims With One or More Scam Mail Responses During
the 4 Months Following the Intervention, by Household Demographics

	Control group		Treatment 1		Treatment 2	
Characteristics	Number	Percent	Number	Percent	Number	Percent
Total	64	33.7	70	36.8	58	30.5
Marital status						
Married / domestic partnership	15	36.6	25	43.1	8	21.6
Widowed or never married	33	33.7	24	24.0	30	40.5
Divorced or separated	10	28.6	18	39.1	12	41.4
Missing	6	37.5	3	21.4	8	57.1
Living arrangement ^a						
Live alone	34	38.2	27	28.4	36	46.2
Live with a spouse/partner	15	37.5	26	43.3	7	20.0
Live with others ^b	14	25.9	15	30.0	8	24.2
Missing	8	42.1	4	19.0	7	58.3
Housing						
Rent	23	40.4	21	28.4	19	40.4
Own	32	31.7	41	36.6	31	36.0
Other/Missing	9	28.1	8	25.0	8	38.1
Household income						
Under \$20,000	14	29.2	20	34.5	21	50.0
\$20,001 to \$50,000	19	40.4	22	39.3	19	40.4
\$50,000 or more	11	34.4	13	37.1	5	20.0
Don't know/missing	20	31.7	15	21.7	13	32.5

Note: Includes addresses included in the experiment and that responded to the survey

^a Details may not sum due to respondents selecting more than one response.

^b Includes living with dependent children, extended family, or roommates.

One important consideration with the intervention experiment was whether receiving the materials would cause distress or other emotional responses for victims in either of the two treatment groups (**Table 4-7**). Additionally, we were interested in using the survey to assess whether victims recalled receiving the intervention materials. Among both treatment groups, about 60% of those who responded to the survey recalled receiving the letter with educational material. For both groups, the most common response to receiving the letter was concern about future fraud (about 22%), followed by anger at the scammers (about 20%) and relief (19% and 14% for groups 1 and 2, respectively). Across both groups, about 85% of victims said that they would want to be alerted again if they responded to another scam solicitation in the future. The

majority of victims also stated that they had not talked with anyone about the fact that they had experienced mail fraud (75% and 64%, respectively).

The victims in treatment group 2 were also presented with a series of logos, including the actual "Be a Fraud Fighter" logo included on their intervention materials, and asked if they recognized any of the logos. About 75% of respondents said that they remembered the actual logo included in the intervention materials, compared to less than 50% of respondents who thought they recognized other logos that had not been used in the intervention materials. This suggests that respondents were opening the mailed materials, looking at them, and recalling at least some of the messaging. However, only 13% of respondents reported that they had completed and returned the tear-away advice card included with the first intervention brochure.

	Treat	ment 1	Treatment 2	
Recall and reaction	Number	Percent	Number	Percent
Recall of letter				
Yes	68	31.2	55	35.7
No	135	61.9	91	59.1
No Response	15	6.9	8	5.2
Feelings related to letter				
Anger at scammers	36	18.7	35	21.5
Anger at Postal Inspector	5	2.6	8	4.9
Concern that letter was fake	8	4.1	12	7.4
Concern about future fraud	43	22.3	37	22.7
Disappointment	28	14.5	24	14.7
Relief	37	19.2	22	13.5
Embarrassment	20	10.4	15	9.2
Other	7	3.6	7	4.3
Does not apply or no response	9	4.7	3	1.8
Would want to be alerted again if a similar i	ncident occurred	ł		
Yes	66	85.7	50	84.7
No	3	3.9	2	3.4
Not Sure/Depends	8	10.4	7	11.9
Talked to someone about scam experience				
Yes	14	18.7	15	25.4
No	56	74.7	38	64.4

Table 4-7.	Memory of and Reaction to Receiving Intervention Mailing(s)
	Memory of and Reaction to Receiving Intervention Maining(s)

	Percent 2.7 4.0 ~ ~ ~ ~	Number 5 1 7 17 0	Percent 8.5 1.7 29.2 70.8 0.0
	4.0 ~ ~	1 7 17 0	1.7 29.2 70.8
	~	7 17 0	29.2 70.8
	~	17 0	70.8
	~	17 0	70.8
	~ ~	0	
	~		0.0
'	~	40	
,	~	4.0	
		13	48.1
	~	14	51.9
	~	0	0.0
	~	5	22.7
	~	17	77.3
	~	0	0.0
	~	31	75.6
	~	10	24.4
	~	0	0.0
	~	5	13.2
	~	20	52.6
	~	13	34.2
		~ ~ ~ ~ ~ ~	\sim 0 \sim 5 \sim 17 \sim 0

~Not applicable

4.3 Survey

Tables 4-8 and **4-9** show the demographic and household characteristics of long-term repeat, repeat, and new victims who completed the survey. Not surprisingly, long-term repeat victims were more likely to complete the survey than the new (one-time victims) victims. As demonstrated by their high numbers of mail fraud incidents, these most chronic victims appear to have a willingness to respond to materials sent via the mail.

A greater percentage of new victims were white and a lower percentage were black, compared to repeat and long-term repeat victims. Repeat and long-term repeat victims also tended to be older and less educated than new victims. Long-term repeat victims were more likely to own than rent compared to repeat and new victims.

		New	New victims ^a		Repeat victims ^b		Long-term repeat victims ^c	
	Characteristics	Number	Percent	Number	Percent	Number	Percent	
Total		274	100.0	297	100.0	1,682	100.0	
	No survey received	223	81.4	226	76.1	1,242	73.8	
	Survey completed	51	18.6	71	23.9	440	26.2	
Sex								
	Male	22	43.1	30	42.3	195	44.3	
	Female	24	47.1	36	50.7	208	47.3	
	Other/missing	5	9.8	5	7.0	37	8.4	
Hispar	nic origin							
	Yes	8	15.7	9	12.7	39	8.9	
	No	40	78.4	56	78.9	357	81.1	
	Missing	3	5.9	6	8.5	44	10.0	
Raced								
	White	38	74.5	31	43.7	247	56.1	
	Black	6	11.8	23	32.4	101	23.0	
	Other ^d	7	13.7	11	15.5	75	17.0	
	Missing	6	11.8	7	9.9	40	9.1	
Age								
	60 or under	10	19.6	3	4.2	28	6.4	
	61-70	13	25.5	16	22.5	65	14.8	
	71-80	10	19.6	21	29.6	124	28.2	
	81+	12	23.5	24	33.8	162	36.8	
	Missing	6	11.8	7	9.9	61	13.9	
Educa	ation							
	No high school diploma or equivalent	4	7.8	7	9.9	41	9.3	
	High school graduate, diploma or GED	10	19.6	21	29.6	120	27.3	
	Some college credit, no degree	8	15.7	13	18.3	70	15.9	
	Trade school or Associate's degree	13	25.5	12	16.9	86	19.5	
	Bachelor's degree	7	13.7	4	5.6	51	11.6	
	Master's, Professional, or Doctorate degree	6	11.8	9	12.7	40	9.1	
		3	5.9	5				

- ^a Includes addresses that were not in the historical CRM data and only appeared once in the intervention experiment list.
- ^b Includes addresses that were not in the historical CRM data but appeared multiple times in the initial intervention experiment list.
- ^c Includes addresses that were present in the historical CRM data seized by the USPIS.
- ^d Details may not sum to total because respondents could select multiple races

Table 4-9. Household Characteristics of Long-term Repeat, Repeat, and New Victims

	New victims ^a		Repeat victims ^b		Long-term repeat victims ^c	
Characteristics	Number	Percent	Number	Percent	Number	Percent
Total	274	100.0	297	100.0	1,682	100.0
No Survey Received	223	81.4	226	76.1	1,242	73.8
Survey completed	51	18.6	71	23.9	440	26.2
Marital status						
Married / domestic partnership	13	25.5	13	18.3	110	25.0
Widowed	12	23.5	26	36.6	153	34.8
Divorced or separated	14	27.5	17	23.9	79	18.0
Never married	9	17.6	7	9.9	65	14.8
Missing	3	5.9	8	11.3	33	7.5
Living arrangement ^d						
Live alone	27	52.9	32	45.1	203	46.1
Live with a spouse/partner	16	31.4	10	14.1	109	24.8
Live with others ^e	11	21.6	22	31.0	104	23.6
Missing	3	5.9	8	11.3	41	9.3
Housing						
Rent	23	45.1	40	56.3	115	26.1
Own	23	45.1	17	23.9	259	58.9
Other/missing	5	9.8	14	19.7	66	15.0
Household income						
Under \$20,000	12	23.5	18	25.4	118	26.8
\$20,001 to \$50,000	11	21.6	21	29.6	118	26.8
\$50,001 or more	12	23.5	10	14.1	70	15.9
Don't know/missing	16	31.4	22	31.0	134	30.5

Note: Includes addresses included in the experiment and that responded to the survey

^a Includes addresses that were not in the historical CRM data and only appeared once in the intervention experiment list.

^b Includes addresses that were not in the historical CRM data but appeared multiple times in the initial intervention experiment list.

^c Includes addresses that were present in the historical CRM data seized by the USPIS.

^d Details may not sum due to respondents selecting more than one response.

^e Includes living with dependent children, extended family, or roommates.

Table 4-10 examines differences among new, repeat, and long-term repeat victims in self-

identified experiences with other fraud or financial abuse and playing the lottery to see if these

experiences and behaviors are more common among repeat and chronic victims. Compared to new victims, a greater percentage of chronic victims had self-reported experiences with other types of fraud. The percentages were not significantly different between repeat and chronic victims and repeat and new victims. There were no other statistically significant differences among the three groups in experiences with financial exploitation or in playing the lottery.

	New v	New victims ^a		Repeat victims ^b		Long-term repeat victims ^c	
Characteristics	Number	Percent	Number	Percent	Number	Percent	
Total	51	100.0	71	100.0	440	100.0	
Prior experience with other types of fra	ud ^d						
Yes	25	53.2	45	68.2	286	71.3	
No	21	44.7	20	30.3	111	27.7	
Don't know/missing	1	2.1	1	1.5	4	1.0	
Prior experience with financial abuse ^e							
Yes	2	3.9	7	9.9	43	9.8	
No	43	84.3	58	81.7	344	78.2	
Don't remember/don't know	6	11.7	6	8.4	53	12.0	
Purchased instant win or scratch-off tic	kets ^f						
Yes	15	29.4	25	35.2	146	33.2	
No	34	66.7	39	54.9	259	58.9	
Don't remember/don't know	2	4.0	7	9.9	35	8.0	
Purchased other lottery tickets ^f							
Yes	16	31.4	35	49.3	167	38.0	
No	31	60.8	28	39.4	227	51.6	
Don't remember/don't know	4	7.9	8	11.3	46	10.4	

Table 4-10. Experiences With Fraud or Financial Abuse, Playing the Lottery or Purchasing Scratch-off Tickets Among Long-term Repeat, Repeat, and New Victims

Note: Includes addresses included in the experiment and that responded to the survey. Details may not sum to total due to missing data.

^a Includes addresses that were not in the historical CRM data and only appeared once in the intervention experiment list.

^b Includes addresses that were not in the historical CRM data but appeared multiple times in the initial intervention experiment list.

° Includes addresses that were present in the historical CRM data seized by the USPIS.

^d Includes prize or grant fraud, product or services fraud, investment fraud, charity fraud, or romance or impostor fraud.

^e Includes being tricked into making bad financial decisions or having money taken by someone close to the victim. ^f During the past 30 days. The survey also asked about activities that may serve as aggravating or mitigating factors in fraud susceptibility. Aggravating factors, potentially related to increased fraud susceptibility, include entering one's name in sweepstakes, answering the phone for unknown callers, using the internet, shopping online, and using social media. Mitigating factors, expected to be related to reduced risk of repeat fraud victimization, include hanging up on telemarketers, interacting regularly with friends and family, engaging in volunteer activities, and getting financial advice from trusted people. **Table 4-11** shows the distribution of these activities among new, repeat, and long-term repeat victims. As expected, repeat and long-term repeat victims were more likely than new victims to report entering their names in sweepstakes. New victims were more likely to report using the internet than repeat and chronic victims. The fact that this relationship is not in the expected relationship may suggest that persons using the internet have more opportunity to be exposed to internet-based scams than mail scams, and that new victims tend to be younger than long-term and repeat victims. There were no other statistically significant differences among the three groups, which may be a product of the relatively small sample sizes of new and repeat victims.

	New vi	ctimsª	Repeat victims ^b		Long-term repeat victims ^c		
Behaviors	Number	Percent	Number	Percent	Number	Percent	
Total	51	100	71	100	440	100	
Opens and reads most maild							
Yes	37	72.5	56	78.9	340	77.3	
No	12	23.5	12	16.9	72	16.4	
Missing	2	3.9	3	4.2	28	6.4	
Enters name in sweepstakes ^d							
Yes	10	19.6	28	39.4	194	44.1	
No	40	78.4	39	54.9	216	49.1	
Missing	1	2	4	5.6	30	6.8	
Answers the phone for unknown callers ^d							
Yes	14	27.5	12	16.9	112	25.5	
No	36	70.6	56	78.9	291	66.1	

Table 4-11.	Frequent Behaviors Among Long-term Repeat, Repeat, and New Victims
-------------	--

	New vi	ctims ^a	Repeat	victims ^b	Long-term repeat victims ^c	
Behaviors	Number	Percent	Number	Percent	Number	Percent
Missing	1	2	3	4.2	37	8.4
Hangs up on telemarketers⁴						
Yes	36	70.6	51	71.8	305	69.3
No	13	25.5	15	21.1	95	21.6
Missing	2	3.9	5	7	40	9.1
Uses the internet ^d						
Yes	26	51	21	29.6	141	32
No	23	45.1	43	60.6	269	61.1
Missing	2	3.9	7	9.9	30	6.8
Shops online ^d						
Yes	4	7.8	2	2.8	30	6.8
No	45	88.2	60	84.5	368	83.6
Missing	2	3.9	9	12.7	42	9.5
Use social media						
Yes	14	27.5	11	15.5	59	13.4
No	35	68.6	56	78.9	340	77.3
Missing	2	3.9	4	5.6	41	9.3
Interacts with friends ^d						
Yes	24	47.1	25	35.2	156	35.5
No	26	51	41	57.7	244	55.5
Missing	1	2	5	7	40	9.1
Interacts with family ^d						
Yes	26	51	34	47.9	193	43.9
No	25	49	33	46.5	211	48
No response in survey	0	0	4	5.6	36	8.2
Volunteers ^d						
Yes	1	2	4	5.6	20	4.5
No	48	94.1	62	87.3	389	88.4
Missing	2	3.9	5	7	31	7
Gets financial advice from truste						
Yes	3	5.9	7	9.9	35	8
No	47	92.2	57	80.3	376	85.5
Missing	1	2	7	9.9	29	6.6

Note: Includes addresses included in the experiment and that responded to the survey.

^a Includes addresses that were not in the historical CRM data and only appeared once in the intervention experiment list.

^b Includes addresses that were not in the historical CRM data but appeared multiple times in the initial intervention experiment list.

^c Includes addresses that were present in the historical CRM data seized by the USPIS.

^d "Yes" includes behaviors that are engaged in frequently (e.g., responses of 'almost every time' or 'usually'). "No" includes behaviors that are engaged in 'occasionally' or 'almost never.'

The survey also asked a series of questions to assess the respondent's financial fragility (measured as ability to come up with \$2,000 if a need arose), willingness to take financial risks, and social isolation (measured through questions about perceptions of loneliness, boredom, and companionship). Table 4-12 shows the distribution of responses for new, repeat, and long-term repeat victims. Although the responses to these items seemed to vary across the three types of victims, the only statistically significant difference was victims perceived lack of companionship. Long-term repeat victims more likely than new victims to report a frequent lack of companionship. The lack of companionship may contribute to someone becoming a chronic victim or it may be that experiencing chronic victimization causes a person to become more isolated. None of the other comparisons were statistically significant.

	New v	ictims ^a	Repeat	t victims ^b	Long-term repeat victims ^c		
Behaviors	Number	Percent	Number	Percent	Number	Percent	
Total	51	100	71	100	440	100	
Financial fragility ^d							
Yes	20	39.2	17	23.9	119 165	27.0	
No	18	35.3	31	43.7		37.5	
Missing	13	25.5	23	32.4	156	35.5	
Willingness to take financial risks ^e							
Yes	13	25.5	20	28.2	137	31.1	
No	23	45.1	26	36.6	213	48.4	
Neither	11	21.6	16	22.5	62	14.1	
Missing	4	7.8	9	12.7	28	6.4	
Frequent loneliness							
Often	8	15.7	11	15.5	73	16.6	
Some of the time	17	33.3	20	28.2	147	33.4	
Hardly ever or never	25	49	33	46.5	170	38.6	
Missing	1	2	7	9.9	50	11.4	
Frequent lack of companionship							
Often	12	23.5	13	18.3	84	19.1	
Some of the time	15	29.4	13	18.3	150	34.1	
Hardly ever or never	23	45.1	38	53.5	156	35.5	

 Table 4-12.
 Loneliness, Financial Fragility, and Willingness to Take Financial Risk Among

 Long-term Repeat, Repeat, and New Victims

	New v	victims ^a	Repeat	t victims ^b	Long-term repeat victims ^c		
Behaviors	Number	Percent	Number	Percent	Number	Percent	
Missing	1	2	7	9.9	50	11.4	
Frequent feeling of isolation							
Often	11	21.6	7	9.9	71	16.1	
Some of the time	11	21.6	24	33.8	144	32.7	
Hardly ever or never	29	56.9	34	47.9	181	41.1	
Missing	0	0	6	8.5	44	10.0	
Frequent feeling of boredom with life	9						
Often	7	13.7	9	12.7	60	13.6	
Some of the time	20	39.2	21	29.6	155	35.2	
Hardly ever or never	24	47.1	33	46.5	190	43.2	
Missing	0	0	8	11.3	35	8.0	

Note: Includes addresses included in the experiment and that responded to the survey.

^a Includes addresses that were not in the historical CRM data and only appeared once in the intervention experiment list.

^b Includes addresses that were not in the historical CRM data but appeared multiple times in the initial intervention experiment list.

^{c I}ncludes addresses that were present in the historical CRM data seized by the USPIS.

^d Confidence in being able to come up with \$2,000 if an unexpected need arose. 'Yes' includes responses of probably or certainly being able to come up with the money.

e "Yes" includes responses of somewhat or very willing.

4.4 Limitations

Mass marketing mail fraud is just one type of fraud targeting older Americans. Although mail scams have been a common mode of committing fraud against older adults for many years, technological advancements, including increased home internet use and the availability of smart phones, as well as changes in mail delivery during the COVID-19 pandemic, have resulted in scammers shifting to other modes of committing fraud. One limitation of this study is that it focused only on mass marketing mail fraud and was not able address other mass marketing scams. There is a possibility that victims identified as being one-time or repeat victims of mail scams may have been experiencing fraud perpetrated through other modes at the same or higher rates as chronic victims.

Another limitation of the study is that it was contingent on the USPIS identifying P.O. Boxes belonging to scammers and interdicting the payment envelopes going to those scammers.

There may have been other scams occurring during the post-intervention monitoring period that were undetected by the USPIS surveillance system. This means that rates of repeat victimization could be underestimated.

Another limitation is that for victims who did not complete the follow-up survey, we have no information about who they are or the circumstances that led them to respond to the scam mail. Victims who responded to the mail survey may be systematically different from victims who declined to respond. Thus, we are limited in our ability to draw definitive conclusions about the factors correlated with repeat or chronic victimization or about the characteristics of victims for whom a mailed intervention is likely to be most effective. Finally, as discussed in Section 3, two of the methodological limitations of this study were the smaller than anticipated sample sizes and the shorter than expected post-intervention monitoring period.

5. Artifacts

5.1 Products Resulting from the Project

5.1.1 Materials

The project resulted in several products that the USPIS could use to educate and empower victims of mail fraud to be aware of subsequent scam efforts. The first is the letter informing victims why their payment envelop was being returned to them. The USPIS used a similar strategy of communicating with victims of the Maria Duval psychic scam, but the letters were written with legal language that was likely not understandable to a large portion of households that received it. In contrast, the letter developed through this project, and approved by the USPIS, was written in plain language, with more accessible messaging, and included educational content in addition to the warning message.

The series of Fraud Fighter materials developed through the project could also have continued use by the USPIS or could be adapted by other entities trying to educate potential victims and appeal to the multitude of reasons that victims respond to scams. These materials were developed through a rigorous process that included the perspective of victims of mail fraud, as well as those of researchers and practitioners working with victims. The final letter and Fraud Fighter materials are included in **Appendix A**.

5.2 Datasets Generated

The project resulted in two datasets archived at the National Archive of Criminal Justice Data (https://www.icpsr.umich.edu/web/pages/NACJD/index.html ?). The public-use dataset contains deidentified responses to the post-intervention survey. Additionally, several variables were added to the file to identify the counts of prior mail fraud victimization—from both the historical CRM data and the intervention experiment—attributed to that address, by year. The lowest level of geography on the public-use file is state.

The project team also archived a restricted-use file containing the historical CRM data, linked to intervention and survey data. The restricted-use dataset contains city and state geographic identifiers and no other identifying information.

5.3 **Dissemination Activities**

5.3.1 Papers

Two papers based on the secondary analysis of the scammers' CRM data were under peer review at the time this report was drafted. The first article, titled "Using scammers' data to estimate the impact and importance of preventing repeat mail fraud victimization," is under review at *Criminology*. The second article, titled "Aging and fraud susceptibility: Evidence on repeat victimization using perpetrator data," is under review at the *Journal of Elder Abuse and Neglect*.

5.3.2 Presentations

Throughout the project period, members of the project team presented on the methodology and initial findings at a range of conferences for diverse audiences. **Table 5-1** presents the convenings and conferences where the team disseminated information about the project along with the month and year.

Table 5-1. MMEFI Conference Presentations

Date	Conference/Convening
November 2021	Gerontological Society of America (virtual)
November 2021	American Society of Criminology
June 2022	Presentation for Federal Trade Commission Division of Marketing Practices and Consumer Response and Operations in the Bureau of Consumer Protection (virtual)
September 2022	Minnesota Demography and Aging Seminar
November 2022	American Society of Criminology
May 2023	NIJ Research Conference
November 2023	Gerontological Society of America

References

- Alves, L. M., & Wilson, S. R. (2008). The effects of loneliness on telemarketing fraud vulnerability among older adults. *Journal of elder abuse & neglect*, *20*(1), 63–85.
- Anderson, K. B. (2019). *Mass-market consumer fraud in the United States: A 2017 Update.* The Federal Trade Commission. Washington, DC. Retrieved from <u>https://www.ftc.gov/reports/mass-market-consumer-fraud-united-states-2017-update</u>
- Balleisen, E. J. (2018). The" Sucker list" and the evolution of American business fraud. *Social Research: An International Quarterly*, *85*(4), 699–726.
- Bech, M., & Kristensen, M. B. (2009). Differential response rates in postal and Web-based surveys in older respondents. Survey Research Methods, 3(1), 1–6.
 <u>https://doi.org/10.18148/srm/2009.v3i1.592</u> Image: I
- Beals, M. E., Carr, D. C., Mottola, G. R., Deevy, M. J., & Carstensen, L. L. (2017). How does survey context impact self-reported fraud victimization?. *The Gerontologist*, *57*(2), 329-340.
- Buchanan, T., & Whitty, M. T. (2014). The online dating romance scam: Causes and consequences of victimhood. *Psychology, Crime & Law*, *20*(3), 261–283.
- Butrica, B. A., Smith, K. E., & Iams, H. M. (2012). This is not your parents' retirement: comparing retirement income across generations. *Social Security Bulletin.*, 72, 37-58.
- Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal*, *27*(1), 36–54.
- Cross, C. (2018). (Mis)Understanding the impact of online fraud: Implications for victim assistance schemes. *Victims & Offenders*, *13*(6), 757–776.

- Deem, D. L. (2000). Notes from the field: Observations in working with the forgotten victims of personal financial crimes. *Journal of Elder Abuse & Neglect*, *12*(2), 33–48.
- DeLiema, M., Li, Y., & Mottola, G. (2023). Correlates of responding to and becoming victimized by fraud: Examining risk factors by scam type. *International Journal of Consumer Studies*, *47*(3), 1042-1059.
- Dong, X., & Simon, M. A. (2013). Elder abuse as a risk factor for hospitalization in older persons. *JAMA internal medicine*, *173*(10), 911–917.
- Federal Trade Commission (FTC). (2018). Protecting older consumers 2021-2022: A report of the Federal Trade Commission. Report to Congress. Washington, DC. Retrieved from <u>https://www.ftc.gov/reports/protecting-older-consumers-2020-2021-report-federal-tradecommission</u>
- Federal Trade Commission (FTC). (2013). *Consumer Sentinel Network Data Book for January– December 2012*. Washington, DC. Retrieved from

https://www.ftc.gov/enforcement/consumer-sentinel-network/reports

- Federal Trade Commission (FTC). (2023). *Consumer Sentinel Network data book 2022.* Washington, DC. Retrieved from <u>https://www.ftc.gov/enforcement/consumer-sentinel-network/reports</u>
- Gavett, B. E., Zhao, R., John, S. E., Bussell, C. A., Roberts, J. R., & Yue, C. (2017). Phishing suspiciousness in older and younger adults: The role of executive functioning. *PloS* one, 12(2), e0171620.
- Greenfield, E. A., & Russell, D. (2011). Identifying living arrangements that heighten risk for loneliness in later life: Evidence from the US National Social Life, Health, and Aging Project. *Journal of Applied Gerontology*, *30*(4), 524–534.

- Han, S. D., Boyle, P. A., James, B. D., Yu, L., & Bennett, D. A. (2016). Mild cognitive impairment and susceptibility to scams in old age. *Journal of Alzheimer's Disease*, *49*(3), 845-851.
- James, B. D., Boyle, P. A., & Bennett, D. A. (2014). Correlates of susceptibility to scams in older adults without dementia. *Journal of Elder Abuse & Neglect*, *26*(2), 107-122.
- Lachs, M. S., & Han, S. D. (2015). Age-associated financial vulnerability: An emerging public health issue. *Annals of Internal Medicine*, *163*(11), 877-878.
- Lee, J., & Soberons-Ferrer, H. (1997). Consumer vulnerability to fraud: Influencing factors. *Journal of consumer affairs*, *31*(1), 70-89.
- Lonsdale, J., Schweppenstedde, D., Strang, L., Stepanek, M., & Stewart, K. (2016). *National Trading Standards–Scams Team*. RAND Corporation. Retrieved from https://www.rand.org/pubs/research_reports/RR1510.html
- Pak, K., & Shadel, D. (2011). Characteristics and behaviors of consumer fraud victims: AARP Foundation National Fraud Victim Study. AARP Research. Retrieved from https://www.aarp.org/research/topics/economics/info-2009/consumer-fraud-victimscharacteristics.html
- Perrin, A. (2021). *Mobile technology and home broadband 2021*. Pew Research Center. Available at <u>https://www.pewresearch.org/internet/2021/06/03/mobile-technology-and-home-broadband-2021/</u>
- Schonfeld, L., Larsen, R. G., & Stiles, P. G. (2006). Behavioral health services utilization among older adults identified within a state abuse hotline database. *The Gerontologist*, *46*(2), 193–199.

- Tolonen, H., Helakorpi, S., Talala, K., et al. (2006). 25-year trends and socio-demographic differences in response rates: Finnish Adult Health Behaviour Survey. *European Journal of Epidemiology, 21*, 409–415. <u>https://doi.org/10.1007/s10654-006-9019-8</u>
- Watson, N., & Wooden, M. 2010. The HILDA Survey: Progress and future developments. *Australian Economic Review*, *43*(3), 326–336.
- Xing, T., Sun, F., Wang, K., Zhao, J., Wu, M., & Wu, J. (2020). Vulnerability to fraud among
 Chinese older adults: Do personality traits and loneliness matter? *Journal of Elder Abuse & Neglect*, *32*(1), 46-59.
- Yu, L., Mottola, G., Bennett, D. A., & Boyle, P. A. (2021). Adverse impacts of declining financial and health literacy in old age. *The American Journal of Geriatric Psychiatry*, 29(11), 1129–1139.

Appendix A: MMEFI Intervention Materials

Mass Marketing Elder Fraud Intervention (MMEFI) Experiment Materials

Creative Review Revision 3

Prepared by: RTI International

Prepared for: U.S. Postal Inspection Service

Date: September 8, 2022

Contents

Background

Materials

- 1. Letter: Standard Forewarning
- 2. Brochure: BRM Tear-off
- **3. Flyer:** Meet Your Postal Inspection Service Team
- 4. Tabloid: Transformational Stories
- 5. Map: Who Are the Scammers
- 6. Card: Thank You with Bookmark
- 7. Magnet
- 8. Envelopes

Materials Summary



Description of Revisions

The revised intervention materials were updated to reflect feedback received during market testing of the materials with nearly 30 individuals representing the target population. The testing focused on the effectiveness and clarity of the messaging, the look and content of the materials, perceptions of what the messaging is communicating, and the persuasiveness of the materials. Based on the feedback received, we made the following non-substantive updates:

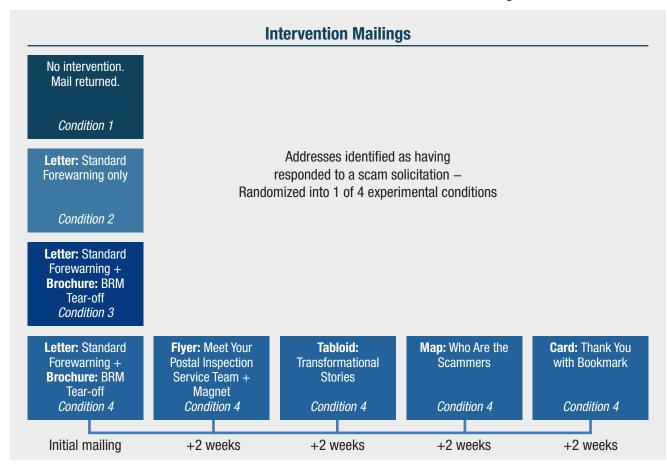
- Standard Forewarning Letter: Revised the language related to the Postal Inspection Service intercepting mail as testers found it difficult to understand; reduced the length of the letter to make it shorter and more concise and adjusted the look of the consumer education materials to respond to feedback that the original presentation was too busy.
- 2. Brochure BRM Tear-Off: Based on the testing, we decided to move forward with an altered version of the A option brochure; adjusted the image of the return card to make it clearer to recipients that they are being asked to complete the card and return it; changed the fold of the brochure so the image of completing the card is one of the first things the recipient sees; simplified and consolidated the response field and used a new image of a Postal Inspection Service investigator.
- 3. Flyer: Meet Your Postal Inspection Service Team: Because testers preferred the image that had diversity and more of a law enforcement feel but felt that the Version B image was intimidating, both images were replaced with a new option that better reflects testers' preferences.
- 4. Tabloid: Transformational Stories: no major changes.
- 5. Map: Who Are the Scammers: Created more contrast in the colors of the map to make it easier for older adults to see; switched several images on the crime board that did not appeal to testers.
- 6. Card: Thank You with Bookmark: Removed language about sending back enclosed postcard as we no longer offer that option.
- 7. Magnet: Added the magnet as a type of swag to send with the flyer.
- 8. Envelope: Added the #10 envelope with front and back printing with full color Fraud Fighter shield

Replaced uses of USPIS acronym and incorporated edits as marked in "13946-MMEFImaterials-revs-6-8-22_Fisher notes_20220721133205.pdf."

Background

RTI International is partnering with the U. S. Postal Inspection Service on a grant from the U.S. Department of Justice to develop a mailed fraud intervention strategy geared toward preventing repeat victimization among older victims of mass marketing scams. *The primary objective* of the intervention materials is to improve victims' resiliency against subsequent scams by giving victims a call to action for preventing fraud.

The materials will eventually be part of an experiment, in which addresses identified as having responded to a fraudulent solicitation via the mail will be sent one or more of the intervention products (see the diagram below for a pictorial representation of the materials that will be used in the experiment). First, RTI will conduct a market test of the materials with 30-40 older adults to assess how well the messages are received.



Belief Objectives: Intervention recipients will believe that...

- The materials are authentic.
- The information is relevant to them and represents their experience.
- "Fraud Fighter" is a national Postal Inspection Service campaign.
- They are important to the Postal Inspection Service and not alone.
- The Postal Inspection Service is looking out for and protecting them and their community.
- They are a collaborator with the Postal Inspection Service in the battle against fraud.
- They are one of the best tools in the fight against scammers.

Behavioral Objectives: Intervention recipients will...

- Know the clues to look for to tell if a letter is fake.
- Develop resiliency to fraud and remember what they learned.
- Internalize the strategies in the intervention and act on them.
- Understand why it is important not to send money to mail fraud criminals.
- Protect their community by alerting their neighbors to the signs of fake mail.

1 Letter: Standard Forewarning



July 15, 2022

Dear Postal Customer,

The United States Postal Inspection Service's, mission is to investigate scams and to protect Americans from mail fraud.

As part of our investigation of mail fraud, we work to identify and collect mail being sent to addresses associated with scam operations. We recently stopped mail with your return address that was being sent to scammers running a criminal mail fraud operation.

The scammers did not get away with stealing your money, and your envelope and its contents should have already been returned to you with a yellow "return to sender" sticker on the bottom. However, you should be on the lookout for future scam mail. Your name, address, and other personal information may be on a list that is traded and sold to other scammers who will try to trick you into sending them money.

Scammers work hard to make their messages look real. **Do not reply to mailings** that ask you to pay money to receive money or prizes or have your fortune told.

The back of this letter has tips to help you spot and avoid mail scams.

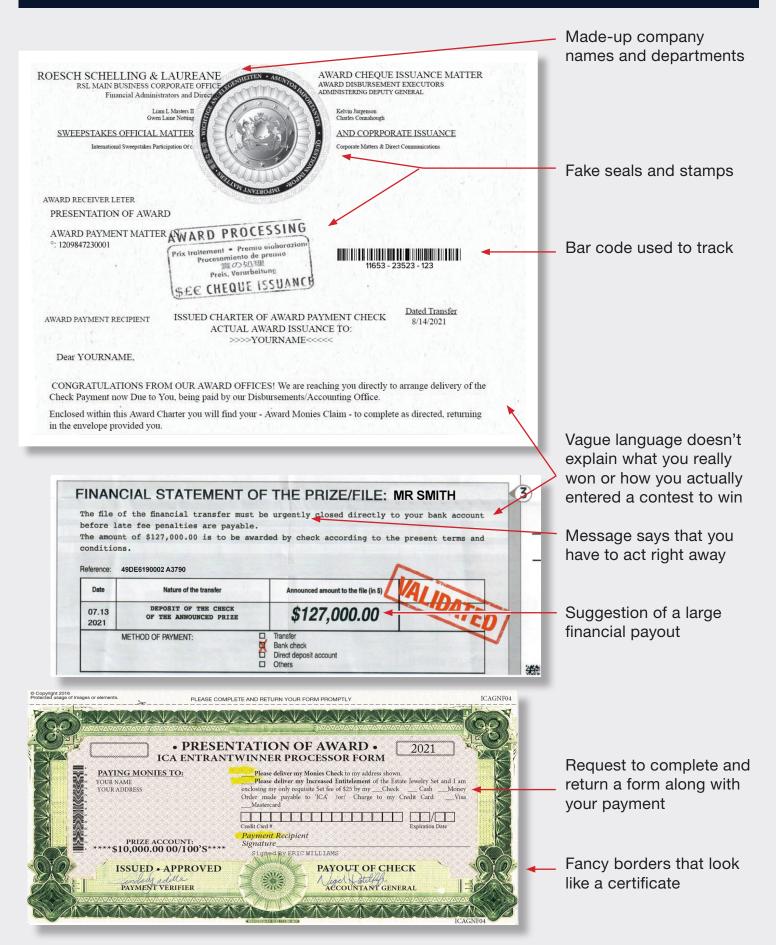
If you receive mail with any of the elements shown on the back of this letter, do not reply and **do not send payment or payment information.** Instead, report any suspicious mail to us at **www.USPIS.gov** or **1-XXX-XXX**.

Sincerely,

RTS

Gary R. Barksdale U.S. Postal Inspector

LOOK FOR THESE TRICKS:



2 Brochure: BRM Tear-off



Warn Your Friends and Neighbors. Report Mail Fraud.

Call the Postal Inspection Service toll free

XXX-XXX-XXXX

Submit a complaint online





Go to the USPIS website by taking a picture of this QR Code with a smart phone.



Keep this handy. Tear off and hang on your refrigerator.



UNITED STATES POSTAL INSPECTION SERVICE





BE A

FRAUD

FIGHTER

You are one of the best tools in the fight against scammers.

Please share your advice to others about ways to protect themselves from fraud. Fill out the back of this card and mail it to the Postal Inspection Service in the enclosed postage paid envelope.



Please fill out this card and mail it to the Postal Inspection Service in the enclosed postage paid envelope.

What can others learn from your experiences with mail fraud to avoid getting scammed?



You are not alone

Every day, tens of thousands of scam letters are sent to Americans to trick them into sending money to criminal organizations. Some people in your community have lost hundreds—or even thousands—of dollars by responding to fake mail. We need your help to protect them and other people from becoming victims of scams in the future.

You can help other people

The U.S. Postal Inspection Service invites you to share your tips on spotting fake mail and rejecting a scammer's attempts to steal your money. YOU are in the best position to help us inform other Americans about scams and encourage them to NOT respond, instead of sending money to criminals.

Become a Fraud Fighter

We are asking you to become a Fraud Fighter for the Postal Inspection Service and share advice on how to avoid mail scams. The advice that you and other Fraud Fighters mail back will be used in our **scam prevention** efforts to alert Americans about mail fraud. 3 Flyer: Meet Your U.S. Postal Inspection Service Team

MEET YOUR U.S. POSTAL FRAUD FIGHTER **INSPECTION SERVICE TEAM**

The U.S. Postal Inspection Service defends the nation's mail system from illegal scams that target Americans. Our Postal Inspectors work with local, state, and federal agencies to investigate mail scams and arrest and prosecute the scammers.

You can help us!

HOW WE STOP MAIL SCAMS

U.S. Postal Inspectors spot mail scam operations when payment envelopes from victims come through our distribution facilities before being shipped off to the criminals. We look for suspicious bulk mailings that are headed overseas. If a scam is discovered early enough, we can stop the payment envelopes from being sent to the criminals, who typically live in other countries.

But scammers are getting craftier. They constantly change their mailing addresses to evade law enforcement and to keep receiving money from their victims.

To make sure scammers don't get the upper hand, we rely on Fraud Fighters like you to spot and report fake mail that's sent directly to you from scammers.

HERE'S HOW YOU CAN **BE A FRAUD FIGHTER**

DO NOT RESPOND to suspicious mail that asks 1 you to send payment in order to receive a prize, sweepstakes, or large amount of money. Any letter that asks you to pay money in order to win money is definitely a scam.

MAKE A REPORT TO THE POSTAL INSPECTION SERVICE whenever you receive bogus letters or any suspicious requests in the mail. Call our fraud report line at XXX-XXX-XXXX to report the scam letter. In your voicemail, make sure you tell us:

- 1. Details about the scam letter, such as what it says and how much they're asking you to pay
- 2. The mailing address printed on the return envelope that scammers want you to use to mail back your payment.

We use this address information to start tracking the scammer and to build a case using reports from other postal customers.

TELL YOUR CLOSE FRIENDS AND FAMILY MEMBERS about what it means to be a Fraud Fighter and share tips on how to spot mail scams. We can't reach every American to warn them about fraud, so we are counting on you to spread the word. As a Fraud Fighter, you can protect people you care about from losing thousands of dollars to overseas criminals.



UNITED STATES POSTAL **INSPECTION SERVICE**

3

Call Toll-free XXX-XXX-XXXX



4 Tabloid: Transformational Stories



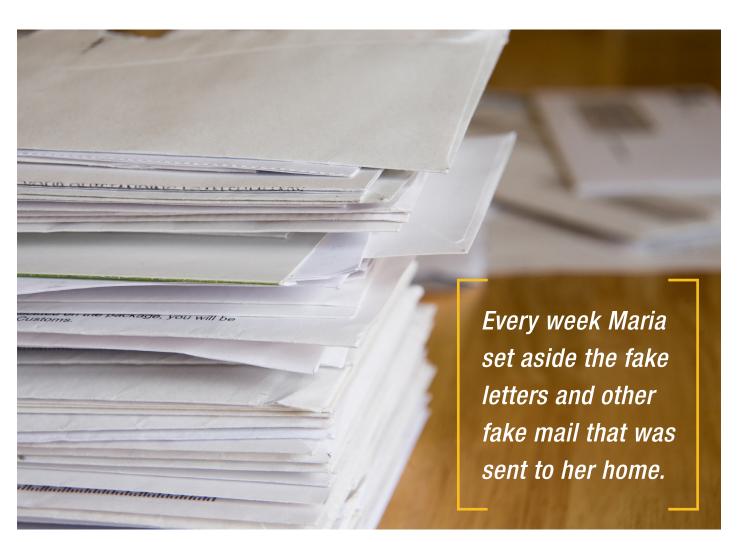
WOMAN BRINGS CRIMINALS TO JUSTICE INTERNATIONAL SCAMMERS CAUGHT POSING AS PUBLISHERS CLEARING HOUSE REPRESENTATIVES.

In early 2017, Maria received what looked like an official letter from Publishers Clearing House. It said that her name was randomly selected for a \$3.7 million grand prize sweepstakes.

She was excited by the thought of winning such a huge prize, so she mailed in the required processing fee of \$25 and waited patiently for her winnings to arrive.

But instead of receiving the money, she got more letters saying that she had won other prizes.

Before long, she was hooked on trying to get the prizes she was promised, and so she kept sending more of her own money to cover the new processing fees. She even started sending money to people who claimed they could see the future and said that they could improve her luck.



investigate the scammers. They found Maria through their investigation and reached out to her. They told her that the people who had been sending the letters and calling her on the phone were not actually from Publishers Clearing House—they were international scammers. Maria's name and address were on a list that was being circulated by criminals. she wanted to take action against the scammers. Maria became a Fraud Fighter to help Postal Inspectors catch the criminals who had tricked her.

money from other victims. They used that information to stop money from being shipped overseas to the scammers. And when they had enough evidence, they brought criminal charges against a major international criminal organization.

By April 2019, scammers had taken more than \$26,000, over half of Maria's retirement savings. The U.S. Postal Inspection Service learned about

the scam and began to

She was devastated that her money was gone, and

Every week she set aside the fake mail that was sent to her home. At the end of each week, she bundled all the pieces of mail together and sent them to the Postal Inspectors.

With Maria's letters, the Postal Inspectors could see how scammers collected Maria protected countless Americans from losing hundreds of thousands of dollars and helped put the criminals behind bars.

The Fraud Fighter's name was changed to protect her privacy.

Retiree protects friends and neighbors

Jim retired in 2010 with a modest state pension after working 38 years for the city. After losing his wife to cancer in 2013, he started to feel lonely. He didn't have much money to travel and only saw his adult children a few times a year because they lived out of state.

2

When a letter came in the mail saying that he won \$250,000, Jim was thrilled! He thought about how happy his children and friends would be when they found out he had won.

The letter said that he needed to send \$20 for the money to be transferred and he sent the money right away.

Soon, Jim started getting more and more offers for lottery winnings, prizes, warranty extensions, and requests for charitable donations. He mailed back more checks, certain he would get what was promised, but all he got back were more requests for money.

> Jim finally realized that if he was asked to pay money to win money, it must be a scam.

When his children visited for the holidays they were concerned. They told Jim stories they had heard about scams and gave him information about how to spot fake mail. Jim finally realized that if he was asked to pay money to win



money, it must be a scam.

He decided that he'd had enough and wanted to take action. So, he filed fraud reports with his state's Attorney General's Office and the Federal Trade Commission. And he told his friends and members of his church about what had happened.

Whenever he received a new letter he would demand that the scammers remove him from their mailing list and reimburse the money he sent before.

Jim became known in his community as a Fraud Fighter. He gave presentations on how to spot scams at local churches, community centers, and senior living facilities. He handed out brochures at the farmer's market and started a support group for people who lost money to scammers.

> Jim made sure that scammers didn't get another dime from the people he helped.

Becoming a Fraud Fighter helped Jim connect with people in his community. Although he never won millions of dollars, he protected hundreds of his friends and neighbors, making sure that scammers didn't get another dime from the people he helped.

The Fraud Fighter's name was changed to protect his privacy.



"What would you do?" Fraud Fighter TIPS /





You won't believe what I got in the mail today.... my Fraud Fighter tips from the U.S. Postal Inspection Service that say **if you have to pay money to win money, it's a scam**.

THANK YOU for being a Fraud Fighter and stopping me from falling for that scam. I thought it sounded too good to be true!

				 1						 				1	1	1
		1				3					8					
	2															
	2															
											9			10		
				4												
			_											ļ		
			5										11			
							13			 						
		6											12			
													12			
							14									
				10												<u> </u>
				16												
7															20	
							4 -						10			<u> </u>
							15						19			
			17													
			18						21							
				22												
				L	l	L			I	L			I			

FRAUD FIGHTER CROSSWORD PUZZLE

DOWN

- 1. Maria was a _____.
- 3. Maria was contacted by the U.S. ____ Inspection Service.
- 4. Jim's children shared information about how to spot _____ mail.
- 5. Jim received a letter in the _____ saying that he won \$250,000.
- 6. Maria talked with people on the _____who claimed to work for Publishers Clearing House.
- 7. Maria and Jim are both Fraud _____.
- 8. Maria helped the Postal Inspectors catch the

ACROSS

- 2. ____ took thousands from Maria.
- 3. The Postal Inspection Service helped Maria stop her _
- 4. Jim filed _____ reports with his state's Attorney General's Office.
- 6. Postal Inspectors contacted Maria and told her the _____ letters were not actually from Publishers Clearing House.
- 7. Maria paid a processing _____ of \$25.
- 9. Jim mailed back more _____, certain he would get what was promised.
- 11. Maria's name and address were on a _____ that was being circulated by criminals.
- 12. Jim finally realized that if he was asked to pay money to ____

- criminals who had _____ her.
- 10. Maria's evidence led to charges against a major international _____ organization.
- 13. Maria bundled all the pieces of mail together and sent them to the Postal _____.
- 16. Jim got more and more letters, some that asked for a charitable _____.
- 19. More than half of Maria's retirement _____ was gone.
- 20. Jim received messages about other _____ winnings.

- money, it must be a scam.
- 14. Jim and Maria helped _____ others from mail fraud.
- 15. Maria's scammers were located _____.
- 17. Maria received what looked like an official _____ from Publishers Clearing House.
- 18. What Jim got back was more requests for _____.
- 21. Jim received fake _____ extensions.
- 22. Maria was told she was randomly selected for a \$3.7 million grand prize _____.

ANSWER KEY

ACROSS: 2. SCAMMERS; 3. PAYMENTS; 4. FRAUD; 6. PRIZE; 7. FEE; 9. CHECKS; 11. LIST; 12. WIN; 14. PROTECT; 15. OVERSEAS; 17. LETTER; 18. MONEY; 21. WARRANTY; 22. SWEEPSTAKES DOWN: 1. VICTIM; 3. POSTAL; 4. FAKE; 5. MAIL; 6. PHONE; 7. FIGHTERS; 8. TRICKED; 10. CRIMINAL; 13. INSPECTOR; 16. DONATION; 19. SAVINGS; 20. LOTTERY



Be A Fraud Fighter

Use the enclosed envelope and prepaid address label to collect recent examples of scam letters you have gotten in the mail and send them to the U.S. Postal Inspection Service.

These examples will help Postal Inspectors to investigate and stop new scams.

JUSTICE BEGINS WITH YOU



4

UNITED STATES POSTAL INSPECTION SERVICE

Call Toll-free XXX-XXX-XXXX Submit a complaint online at https://www.uspis.gov/report

5 Map: Who Are the Scammers?



WHERE DOES MONEY GO WHEN IT'S SENT TO A SCAMMER?



UNITED STATES POSTAL

Most Americans who reply to scam letters don't have any idea who actually gets their money.

A

Most mail scammers live outside the U.S., but they use either foreign or U.S. return addresses on the envelope.

U.S. federal agencies have worked with countries like Germany, Spain, England, Canada, Jamaica, China, Nigeria, Israel, and the United Arab Emirates to bring down scam operations.

www.uspis.gov



The United States Postal Inspection Service, FBI, and Immigration and Customs Enforcement spend a lot of time and resources investigating scammers. Here's what they've discovered that Fraud Fighters like you should know.



Help spread the word!

Encourage your family and friends to think twice before sending money to a person or company they don't know. The money could end up anywhere in the world, including in the hands of international criminals.

Scammers are sophisticated con artists. They often imitate real business mailings and play on people's emotions to trick them into sending money.

Scammers often use the money they steal from Americans to fund terrorism, human trafficking, and drug and weapon purchases.

Scam artists build contact lists of Americans who have paid in response to their letters. These lists are sold and traded between criminal organizations.

Some mail scammers use phone calls to put more pressure on victims to pay.

MISSING

6 Card: Thank You with Bookmark



These nonprofit organizations offer free services to support victims of scams, fraud, and exploitation:



Victim Connect Resource Center: 1-855-4VICTIM (1-855-484-2846)



National Elder Fraud Helpline: 1-833-FRAUD11 (1-833-372-8311)



AARP Fraud Watch Network Helpline: 1-877-908-3360









Thank you for being a Fraud Fighter!

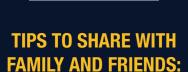
Your efforts to spot mail scams and educate your friends and neighbors help to protect them and others against scams. Thanks to the tips and advice you provided, Postal Inspectors can do more to keep Americans safe.

We'd like to share some of those important fraud fighting tips that were shared with the U.S. Postal Inspection Service.

STRENGTHEN YOUR COMMUNITY

It is important for Fraud Fighters like you to support others who have been tricked by scammers. If someone you know is struggling after having their money stolen, talk with them—listen to their story and kindly let them know that help is available.

Please tear off and share the helpful information in this complimentary bookmark.



You know it's a scam when they ask you to pay money so you can win money. Real sweepstakes don't ask for any money up front.

16 Don't respond to letters from companies that you have never done business with or interacted with in person.

1 Talk to a friend and show them the letter before responding.

Sending in money one time will cause a tidal wave of more junk mail in your mailbox. Just throw the letter away the first time!



Refrigerator Magnet - business card size







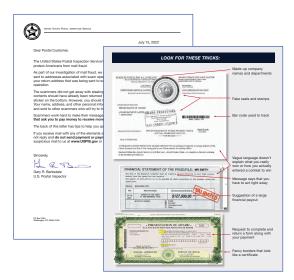
United States Postal Inspecition Service 5265 Capital Boulevard Raleigh NC 27690-1652





Materials Summary

Materials Summary



1. Letter: Standard Forewarning



4. Tabloid: Transformational Stories



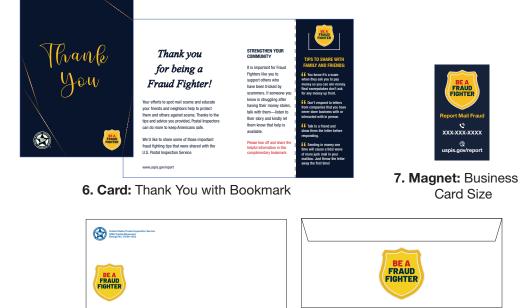
2. Brochure: BRM Tear-off



5. Map: Who Are the Scammers?



3. Flyer: Meet Your U.S. **Postal Inspection Service** Team



8. Envelope: #10 (front/back)

Appendix B: MMEFI Victim Interview Report

Mass Marketing Elder Fraud Intervention: Victim Interviews

Erin Kennedy & Lynn Langton, RTI; Marti DeLiema, University of Minnesota

This memo details mail fraud victim interviews conducted by the Mass Marketing Elder Fraud Intervention (MMEFI) technical team between January and April 2021.

Background

As the federal law enforcement agency tasked with enforcement of all crimes involving the mail, the U.S. Postal Inspection Service (USPIS) collects victim data from the payment envelopes victims mail in response to mass marketing fraud scams. Their historical databases, dating back over a decade, contain millions of victims and transactions. Although the USPIS recognizes that rates of revictimization among victims of mass marketing fraud are high, they have not empirically assessed patterns in the prevalence and frequency of revictimization across their databases. Over the years, the USPIS has also tried, but never evaluated, a number of approaches to educating residents about mass marketing fraud and preventing repeat victimization. For instance, at one point, the USPIS sent a brochure and an official letter to fraud victims whose cash payment was intercepted, explaining that they were a victim of fraud and how to prevent fraud in the future. The USPIS is interested in understanding whether this type of mailed intervention can be effective at preventing repeat victimization.

The MMEFI Study had the following specific goals:

- (1) Enhance knowledge and understanding of repeat victimization among older victims of mass marketing scams.
- (2) Engage in rigorous testing of the efficacy of two versions of a fraud intervention strategy geared toward preventing repeat victimization among older victims of mass marketing scams, and
- (3) Conduct a follow-up study with a subset of victims to assess victims' perceptions of the intervention and collect self-report data on experiences with other types of fraud by surveying individuals in the intervention.

The first objective will be accomplished through secondary analysis of 20 years of USPIS investigative data on millions of U.S. fraud victims. The second and third objectives will be accomplished through developing a mailed intervention (a letter and informational brochures) to be administered to identified victims of mass marketing fraud, testing the effectiveness of the intervention, and conducting a survey on victim perceptions of the intervention.

The goal of the victim interviews was to obtain victims' perspectives on why they responded to mass marketing fraud materials. The information learned through the interviews will help to inform the development of the intervention materials that will be mailed to identified victims of mass marketing fraud to prevent revictimization. Staff from RTI and the University of Minnesota interviewed older victims of mail fraud or adult children of victims to understand how victims think and feel about receiving and responding to fraudulent mail and to identify points and strategies for intervention.

Methods

Recruitment

The USPIS provided MMEFI staff with approximately 50 redacted summaries of interviews that inspectors conducted with victims of mass marketing fraud. MMEFI staff reviewed the summaries and identified potential interviewees based on how much time had passed since their victimization and the amount of financial loss they experienced (attempting to obtain variation in chronic versus less serious victims) and discussions with the inspector about their likely willingness to participate. Based on these factors, MMEFI staff developed an initial list of 23 victims that the USPIS contacted to determine their willingness to participate in an interview; of these, 8 agreed to be contacted. The USPIS inspector identified an additional 5 recent interviewees (3 victims, 2 adult children of victims) who expressed interest in learning more about the interview for a total of 13 potential interviewees.

Once an individual provided consent to be contacted about an interview, the USPIS inspector alerted the recruiter of their interest via email, and provided victim contact information (full name, phone number, and any contact notes, such as the best time to call) on the recruiter's secure voicemail.

The recruiter contacted each potential participant by phone up to 8 times or until they scheduled an interview or declined to participate. Because all the potential participants were older adults who had previously fallen victim to scams, the recruiter used many tactics to attempt to reach them, including

- varying the time of day calls were made;
- leaving detailed voicemail messages, including referencing the USPIS inspector by name; and
- calling back to back to allow potential participants enough time to get to the phone.

The recruiter explained the study to potential participants, including the purpose of the project, how the project was funded, what types of questions would be asked, and the incentive offered (\$40 Visa gift card). If potential participants expressed interest, the recruiter screened them to determine eligibility (<u>Appendix A: Recruitment and Screening Script</u>). If eligible, potential participants were then scheduled for an interview via the Zoom videoconferencing platform.

Of the 13 potential participants,

- 5 scheduled and completed interviews; of these,
 - 3 were victims themselves and
 - 2 were adult children of victims;.
- 1 scheduled an interview but was unavailable at the scheduled time and was unreachable after several follow-up attempts;
- 2 were ineligible after completing the screener;
- 4 chose not to participate in an interview; and
- 1 was unreachable after several attempts.

Conducting Interviews

Interviews were conducted via the Zoom videoconferencing platform. Of the 5 interviews conducted, 2 participants were familiar with Zoom and joined the videoconference using a link sent to them by the recruiter. The other 3 participants were not familiar with Zoom; the recruiter "invited"

these 3 participants to their respective interviews by having the Zoom platform contact them directly by phone. Upon answering the call from Zoom, participants were instructed to press 1 to join the videoconference in progress.

Interviews were conducted by one or both co-PIs on the study. They administered verbal consent, including asking participants whether they consented to the interview being audio-recorded (<u>Appendix B: Informed Consent</u>). The interviewers then transitioned to the semi-structured interview guide (<u>Appendix C: Semi-Structured Interview Guide</u>).

After the interview was concluded, the interviewers left the videoconference. The recruiter remained on the line with the participant to obtain their mailing address to send the incentive.

Findings

Demographics

Figure 1 shows descriptive information about the participants.

Characteristic		n	%
Sex	Male	3	60
	Female	2	40
Victim status	Victim	3	60
	Adult child of victim	2	40
Age range	50–59	2	40
	65–69	1	20
	75–79	1	20
	85–89	1	20

Figure 1. MMEFI Victim Interviewees by Sex, Victim Status, and Age Range

Key Findings and Themes

Findings are presented by interview guide sections.

Background information

Victims described their hobbies, which included being involved in their churches, reading, volunteering, going to the casino, socializing, and gardening. All victims described things having changed with COVID-19 and not being able to socialize as much as they had before. One victim had recently gone through a breakup and noted that with the onset of COVID-19 and social distancing, they were struggling with boredom and loneliness. None of the victims lived alone, but rather with family (spouse, adult children and/or grandchildren) or in an assisted living facility. Adult children of victims described their parents as living alone when they fell victim to fraud and noted that to the best of their knowledge their parents' involvement with scams started after they were widowed.

Interaction with mail

Participants described receiving (or their parent receiving) up to 10 pieces of mail per day in some cases, but most said they received about 3–5 pieces of mail per day. Participants noted that not all the mail they received on a daily basis was fraudulent.

Interaction with scam mail

Victims who have stopped responding to scams added that the amount of fraudulent mail they received dropped off quickly after they stopped responding. One victim recalled that after not responding to 1 or 2 letters from a fraudster, the fraudster stopped sending them mail altogether. One of the adult children of a victim mentioned that they received their parent's mail for a few months while their parent was recuperating from surgery; when the adult child did not respond to any of the scam mail, the letters stopped within a few months. Another victim described burning any mail that they felt was fraudulent.

Victims described the scam mail they received as appearing to come from Publisher's Clearinghouse, offering fortune telling or palm reading services, offering sweepstakes lists (e.g., a list that tells the recipient which sweepstakes are going on right now and encourages them to send money to learn about more sweepstakes and/or improve their chances), or being from foreign-sounding entities.

Among their reasons for responding to scam mail, victims noted that they enjoyed gambling and treated the scams like a game at the casino; feeling lonely or bored (especially with COVID-19 and largely not being able to socialize) and looking to fill a void; and truly believing they had won and that their response was all that was needed to claim their winnings. One victim also described daydreaming that if they won, all their financial problems would be resolved; another described the offer of potential prize money as a "blessing." Adult children of victims reported their parents' primary reasons for responding as dementia/mental decline; wanting to win a large sum of money to leave behind as inheritance for children and grandchildren; and being depressed or lonely since the passing of a spouse and looking to fill a void.

Victimization experience

Victims described not telling many people (or any people) about the scam mail due to feeling embarrassed, not wanting to share any information until the winnings arrived, and/or not wanting to be talked out of responding to fraudulent mail. Adult children of victims described only finding out about their parents' involvement due to something else (e.g., one found out that their parent was responding to scams when beginning estate planning with their parent and financial advisor; another described learning about their parent's involvement when they retained power of attorney after the parent became ill).

Two victims describing receiving something after interacting with scam mail, but neither was the promised/expected prize: one victim received some small pieces of jewelry, and the other received a small toy/joke prize (e.g., the prize promised was a bicycle, and they received a miniature toy bicycle instead). The other victim and the two adult children of victims did not receive any prizes (to their children's knowledge). One victim's total losses were about \$50,000–\$60,000; other victims were not able to estimate their total losses.

When asked to look back for any signs that the mail was a scam, victims described the fact that they had to "pay to play" as a sign, as well as the fact that they only had a limited amount of time to respond to win. Another victim described a scam letter that asked him to send money to an address that the victim knew to not have a business on it (it was a local highway, not a commercial street). The same victim also described a letter that advised them that they had won a large prize but that they needed to pay the customs processing fee. One victim admitted to having an inkling that the mail was fraudulent

but was so addicted to daydreaming about the potential winnings that they ignored their instincts and continued to engage with the scammers.

One victim described having no idea that they had participated in a scam until they heard from the USPIS. Had they received a letter from the USPIS that their address was found in a mail fraud case, they would have stopped participating right away. Another victim described going into a Wal-Mart at the scammer's direction to purchase gift cards to send and was alerted by Wal-Mart staff that this was a common scam.

Current perceptions

Among the advice they would give to others, or to their younger selves, participants included the following:

- "Pay to play" games are not legitimate.
- If it seems too good to be true, it probably is.
- Sending money to an unknown address (whether cash, check, money order, or gift card) is not legitimate.
- If there is a return address or phone number, check the address or call the phone number to determine if it is legitimate.
- Show any mail requests to a trusted friend or family member (such as an attorney) who can provide guidance on these matters.

Adult children of victims added the following advice to other families:

- It is never too early to be aware of scams and to start educating your parent.
- Sharing objective facts/data about scams (vs. trying to appeal to their sense of reason or emotions).

The victims had mixed feelings about the fact that they had responded to scams. Two victims were embarrassed for having been "so stupid," and both mentioned the fact that they had felt depressed/lonely around the time they responded to scams. Both adult children of victims were angry that their parent had fallen for scams and lost so much money and that the scammers were taking advantage of elderly people.

Other scams

Many of the victims described receiving scam phone calls as well as scams in the mail, and some noted that the calls were related to the mail they were receiving. One victim noted that when they did not respond to one of the mailed fraudulent requests, they received aggressive phone calls telling them they needed to respond. Some victims described screening their calls, not answering any call from toll-free numbers, or waiting for callers to leave voicemails before returning the call or picking up the next time they called.

Wrap-up

Victims noted that they consulted AARP and their local news stations for information on scams. One of the adult children of a victim suggested that perhaps funeral home staff might share information with widows/widowers upon the death of a spouse, as they may be feeling depressed and lonely and may be more likely to respond to scams. Two participants felt that knowing that the money they sent to scammers was going to criminals would have motivated them to stop responding. Another victim noted that learning that there was zero chance of winning a prize (rather than "a small chance") would have compelled them to stop sooner; they kept believing there was a slim chance they could win.

One of the adult children of a victim described their parent as having sent in small sums (\$5–\$10) over the course of many years and felt that their parent probably saw that as a small risk that might have a big payoff eventually.

Conclusion and Next Steps

The ways in which victims begin responding to scams and their reasons for stopping (or not stopping) their involvement are quite varied. as such, there is likely no one intervention that would work for every type of victim. Thus, the MMEFI team will use findings from these interviews to create intervention materials that target the problem in various ways.

Appendices

A. Recruitment and Screening Script

Hi [Respondent Name],

This is [Recruiter Name] from RTI International. I'm following because the US Postal Inspection Service provided us with your contact information because you were interested in participating in research interviews.

This research is being conducted by researchers at RTI International and the University of Minnesota, in partnership with the United States Postal Inspection Service. The research is funded by the National Institute of Justice. The purpose of the study is to develop consumer awareness brochures to protect Americans from losing money by responding to misleading letters sent through the mail.

We'll be talking with you about the type of mail that you receive on a daily basis and about any times that you may have responded to letters that have promised you a prize or large sum of money that you never received. We're hoping to talk with you up to two times for about an hour total. If you choose to participate, you will be sent a \$40 VISA gift card.

Do you have any questions so far? Does this sound like something you are interested in participating in?

[IF YES, PROCEED WITH ELIGIBILITY QUESTIONS. IF NO, THANK THEM FOR THEIR TIME.]

Great. I need to ask you a few questions to ensure that you're eligible and able to participate in the study.

Q1. Do you have a private and safe area where you could complete up to two interviews for approximately 1 hour and where other people will not be able to hear you or interrupt you?

- a. Yes
- b. No → INELIGIBLE

Q2. Are you worried that participating in an interview about losing money after responding to misleading letters in the mail may bring up negative feelings or stress?

- a. Yes → INELIGIBLE
- b. No

Q3. COGNITIVE ABILITY TEST

[USE THESE QUESTIONS TO DETERMINE IF RESPONDENT IS COGNITIVELY INTACT BASED ON REASONING AND MEMORY.]

Now because the interviews will require you to recall pieces of mail that you received in the past, I'm going to ask you some questions that will require you to use your memory.

At the beginning of this call I told you what this research study is about. Can you recall what I said about the purpose of the study? It's okay if you say it in your own words.

a. 'Consumer awareness' 'Americans losing money' 'scams' 'misleading letters sent in the mail' \rightarrow all OKAY

- b. Don't know/Don't remember → Provide HINT: It involves the US Postal Inspection Service
 - i. 'consumer awareness' 'Americans losing money' 'scams' 'misleading letters sent in the mail' \rightarrow all OKAY
 - No/Don't Remember \rightarrow **INELIGIBLE**

Q4. COGNITIVE ABILITY TEST

What is YOUR STATE'S CAPITAL?

- a. Correct state capital named
- b. Don't know/Don't Remember \rightarrow **INELIGIBLE**

Q5. COGNITIVE ABILITY TEST

What year were you born?

- a. Correct year identified (based on information provided in MOIs)
- b. Don't know/Don't Remember \rightarrow **INELIGIBLE**

Q6. ARTICULATION/CREATIVITY SCREENING QUESTION

[USE THIS QUESTION TO DETERMINE IF RESPONDENT IS ARTICULATE, CREATIVE AND CAN EXPRESS HIM/HERSELF EASILY AND CLEARLY.]

Now please use your imagination for a moment - there are no right or wrong answers to this multi-part question. If you could invite someone famous (dead or alive) to your home for dinner – who would this person be and why? What type of food would you serve and why?

- a. Yes, respondent passed the articulation test. [SUBJECTIVE JUDGEMENT OF RECRUITER]
- b. No → INELIGIBLE

[IF INELIGIBLE]

I'm sorry but based on your responses you are not eligible to participate in this study. Thank you for your interest.

[IF ELIGIBLE]

Great. You are eligible to participate in the study. Would this be a good time to go ahead and schedule your interview?

[RECRUITER WORKS WITH PARTICIPANT TO SCHEDULE A DATE/TIME]

You have the option of being interviewed over the phone or using the Zoom videoconferencing platform on a computer where you and the interviewer would be able to see each other, more like a face-to-face conversation. Which would you prefer?

[If ZOOM] Do you have a webcam on your computer? Do you have an email address where I could email you the link to log into the interview?

[If PHONE] Do you have a pen or pencil and a piece of paper where you could write down the phone number that you will call at the time of your interview? [PROVIDES PHONE NUMBER] And do you have a number at which we could reach you the day of the interview in case there are any problems with the technology, or you misplace the phone number? [GET PHONE NUMBER] NUMBER]

[RECRUITER WILL DOCUMENT PARTICIPANT'S NAME, EMAIL, PHONE NUMBER, AND INTERVIEW DATE/TIME IN A SPREADSHEET THAT IS SECURELY STORED BEHIND THE RTI FIREWALL]

B. Informed Consent

[Interviewer reads aloud]

Thank you for your interest in talking with us today. My name is Marti DeLiema and I'm a professor at the University of Minnesota. My colleague, Dr. Lynn Langton, is also joining us on the call to take notes and possibly chime in with some follow-up questions. Lynn is also a researcher but with an organization called RTI that is also a collaborator on this study with the US Postal Inspection Service.

We would like to record the audio of the interview to help us make sure our notes are accurate. Nothing you say in the interview will be attributed to you directly and the interview recording will be destroyed shortly after the interview. You can say yes or no. Is it okay if I audio record this interview? [*Wait for response.*]

Before we begin, I am going to discuss some details about the interview and ask you for your verbal agreement to proceed. Some of the information I will cover was already shared with you by the person who scheduled the interview, but I want to go over it again together.

You have been invited to take part in a study being conducted in collaboration with the US Postal Inspection Service. This study is funded by the National Institute of Justice, which is part of the U.S. Department of Justice. The purpose of the interview is to discuss the types of mail you get on a regular basis and any experiences you have had where you sent money to receive a prize or large sum of money, but never got what was promised to you. This discussion will help us develop public awareness messages and brochures that will be used to help other Americans know when a piece of mail is not legitimate.

This interview will last about 30 minutes and we will schedule one additional interview as needed. If you choose to participate in the interviews, you will receive a \$40 VISA gift card, but your participation is completely voluntary. You may decide to skip any questions and you may stop participating at any time. There are no negative consequences for choosing not to participate in the study.

There are no known risks from your participation in the discussion. However, during the conversation we will be discussing sensitive topics involving potential experiences such as losing money. Therefore, please think carefully about where you are located right now, and whether other people might be able to overhear you speaking. **We want to ensure your privacy, safety, and confidentiality while participating.** Finally, it is possible that you may feel uncomfortable with the nature of some of the questions. We will provide immediate support resources if you experience distress from participating.

To keep your information confidential, we will not use your name or contact information in notes or reports. The information provided during our discussion will only be used in summary form. Nothing that you say will be directly shared outside of the study team. All recordings and notes will be stored safely and then destroyed at the end of the study.

If you have questions as we go, please feel free to ask. If you have any questions about the study after we are done, please contact the study's Principal Investigator, Lynn Langton, at 202-974-7878, or Marti DeLiema at 805-729-4189. If you have any questions about your rights

as a study participant, contact the RTI Office of Research Protection at 1-866-214-2043. You can also call the University of Minnesota's Toll Free Research Participants' Advocate Line at 1-888-224-8636 or go to z.umn.edu/participants.

Do you agree to participate in this interview? [*If yes, continue*.]

C. Semi-Structured Interview Guide

To get started I want to emphasize that there are no wrong answers here. It's very important for the research if you can be as open as possible. We are working hard to raise awareness about fake offers sent in the mail, so the more honest you are, the better job we can do in helping people learn the difference between legitimate mail and fake mail. We so appreciate your willingness to assist us with this project. Your stories are experiences are so important for helping others.

Warm-up:

- Just so we can get to know each other a bit better, let me first tell you about myself. [Marti shares personal story about being a gerontologist, working as a professor, moving to Minnesota from CA, two-year-old son, hobbies.] Now can you tell me about yourself?
 - a. How do you spend your time?
 - b. What are your interests?
- 2. Tell me about the people in your life. Who are you close with?
 - a. What do you do when you are together?

Interaction with mail in general:

- 3. As you know, we are interested in learning more about the offers and requests that you receive in the mail. But before we get into the details, can you describe the mail that you receive in general? What's in your mailbox on a typical day? [*Interviewers will redirect participant if they talk at length about non-scam mail.*]
 - a. PROMPTS: How many pieces of mail do you get per day, in general?
- 4. Do you open all the mail that gets sent to you? Why or why not?

Interaction with scam mail:

- 5. I now want to talk about letters that ask you to pay money in order to receive some sort of gift or prize or lottery money. Do you receive this kind of mail? Can you describe those letters?
 - POTENTIAL PROMPTS:
 - a. What do these letters look like? What do they say?
 - b. How often do you get letters like those?
- 6. How do you feel when you open them?
- 7. How do you decide whether or not to respond?

[Participant Check] Okay, I just want to make sure you're okay to keep talking about your experiences getting this kind of mail.

Victimization experience:

8. Do you recall a time when you sent money in response to a letter that told you you would receive a [prize/large sum of money/lottery winnings]? If this has happened more than once, could you tell me the story of what happened with the most memorable letter or experience. .

POTENTIAL PROMPTS:

- a. Can you describe what was going through your mind when you read it?
- b. Was there anything specific about the offer that made you want to respond to it?
- c. What kind of prize or money were you promised?
- d. Before you sent the money, did you run the letter by a friend or family member to get their opinion? Why or why not?
- e. How did you feel immediately after you put your payment in the mail?
- f. What did you think when you didn't get what the letter promised?
- g. And while you were waiting, did you tell anyone you know about the [prize/winnings]? Why or why not? [Did the letter specifically tell you not to say anything to anybody else?]
- 9. At any point did you suspect that something was suspicious or that maybe the letter was fake [OK to say "scam" or "fraud" if participant uses the word first.]?
- 10. Looking back, were there any warning signs that the letter was fake?

[Participant Check] Just want to check on how you're feeling. Are you okay to keep talking about these experiences?

Current perceptions:

- 11. How do you feel now about that experience?
- 12. [*If multiple incidents*] You mentioned you have responded to letters like these multiple times. Can you tell me more about the first time you responded and how it all started?
- 13. If you could go back in time before it all started to give yourself advice about the letters, what would you say?
- 14. And what are things like for you now? Has your reaction to the letters changed?

Other scams (if time is available):

- 15. Aside from the letters, do you ever get phone calls from people telling you you won something but first have to send some money or give them personal information about yourself?
 - a. How do you respond to those calls?
- 16. [If they use email/text messaging.] Aside from mail and phone calls, do you ever get emails or text messages asking you to send money after you are told you won something or are entitled to some money?
 - a. How do you respond?

Wrap-up:

- 17. As you know, we want to help people become better at telling the difference between a legitimate letter and a fake letter. Do you have any advice on how we help inform others?
- 18. Is there anything else you would like to share?

Before we wrap up, I just want to make sure that you understand that Lynn and I are not law enforcement or fraud investigators. So we aren't involved in any efforts to help people get their money back or recover lost funds. This interview was about hearing your story to help raise awareness.

Following completion of the interview, participants will be asked if they would like information about resources available for victims of fraud and scam. If yes, the following resources will be provided:

National Elder Fraud Hotline

Telephone: 1-833-FRAUD-11 (1-833-372-8311) https://stopelderfraud.ovc.ojp.gov/

AARP Fraud Watch Helpline Telephone: 877-908-3360

Appendix C: MMEFI Cognitive Interviewing Report



Mass Marketing Elder Fraud Intervention: Cognitive Interviewing Report

Cognitive Testing Feedback

Introduction

The Mass Marketing Elder Fraud Intervention (MMEFI) Study aims to develop and test an intervention that the United States Postal Inspection Service (USPIS) can use for preventing the repeated victimization of older adults through mass marketing scams. Based on one investigation from 2011-2016, the USPIS found that Americans sent more than \$558 million through the mail in response to scams and that two-thirds of these victims were age 50 or older. RTI is partnering with the USPIS and gerontologist and fraud researcher, Dr. Marguerite DeLiema, to enhance our understanding of patterns of revictimization among older adults. This will be done through secondary data analysis of USPIS investigatory databases containing millions of records of fraud victims, as well as through a randomized study testing the efficacy of a mailed intervention for preventing the revictimization of identified victims of mass marketing fraud. The outcome of interest, revictimization, will be measured through observation of actual victim behavior, rather than traditional self-report studies or mock scam scenarios. For up to 1 year, the USPIS will provide RTI with return addresses from all detained fraud payment envelopes to track whether victims from the experiment respond to subsequent scams. A follow-up survey with a sample of victims will collect data on victim characteristics, including age, any unintended consequences of the intervention, and victim susceptibility to other types of fraud. Findings from the study and return-on-investment analyses will inform the USPIS about the value of continuing to implement a mailed intervention versus exploring other prevention approaches.

This report details activities under Goal 2 of the study: *Engage in rigorous testing of the efficacy of two versions of a fraud intervention strategy geared toward preventing repeat victimization among older victims of mass marketing scams.* After developing intervention materials in conjunction with the USPIS, RTI and University of Minnesota staff cognitively tested the materials proposed for the three fraud intervention treatment conditions with the target population prior to the full intervention.

Cognitive Testing

The cognitive interviews focused on the effectiveness and clarity of the messaging of the materials, the look and content of the materials, perceptions of what the message is communicating, the likelihood of completing and returning the tear-off advice card, and how memorable the materials are.

Participant Recruitment

Participants were recruited through Minnesota organizations that work with older adults (n=11) and via Facebook (n=18). We also attempted to recruit via MTurk, but no participants were successfully

recruited through this method. We attempted to recruit 10 participants aged 50–64, 10 participants aged 65–74, and 10 participants aged 75 and older, including 20 victims and 10 non-victims.

The co-PI spoke with the Minnesota-recruited participants to ensure that they were cognitively able to consent and participate based on responses to a verbal articulation task and to schedule the interview. Virtual respondents expressed interest in the study by completing a study screener (shared via targeted Facebook ads). We focused on older adults who had previously been victims of mail fraud. These potential participants were also screened to ensure they were cognitively intact based on responses to the verbal articulation task. In both cases, participants were sent a copy of the study materials via FedEx. All participants received 7 items but were randomized for whether they would receive Version A or B of the blue brochure and Version A or B of the Meet Your Team flyer.

Cognitive Interview Characteristics

Survey Characteristic	Total Target Participants	Actual Participants Completed		
Type of interview				
Victim	20	17		
Non-Victim	10	13		
Age				
50–64	10	9		
65–74	10	14		
75+	10	7		
Total count	30	30		

Characteristics of target participants and actual participants are listed below.

Detailed Feedback on Materials

Standard Letter

Front

Back



- Some participants found the standard letter to be confusing, specifically the phrase, "We recently intercepted an envelope." They thought the language needed to be clearer. Some participants found the letter to be a little long. They suggested bullets to improve the length and ease of reading. Participants did not differ by victimization in this response.
- A few participants noted feeling like the letter itself might be a scam, citing the "intercepted" language and the images on the back: "Anybody could put USPIS on the front. It tells you not to reply to a letter, so how do I know I'm not giving something back to the scammer."
- One male participant aged 75 or older said the text was too small.
- Participants generally affirmed that they learned something new from this letter.
- A few participants suggested making the logo in the upper right corner more prominent.
- In general, participants did not like the format of the back of the standard letter. Although, on average, participants found the information to be useful, they were overwhelmed by the placement of the images.
- When looking at the specific images, participants found the examples to be helpful, and most found them to be familiar. However, interviewers noted that participants did best when they discussed the images out loud with the interviewer one by one. Participants did not seem to understand all of the images on their own without an interviewer present: "The back is confusing, a lot of clutter, kinda busy."
- A few participants noted that there was not enough detail on how to spot that the letters are fake. One participant noted, "You say this is a fake company, [but] how would I know that?"
- A few participants also noted liking the contact information on the letter. Most participants said they would feel relieved after receiving the letter, knowing the USPIS is looking out for them (even after some initial embarrassment). Most participants also noted that getting this letter would make them review their mail more carefully.

Blue Brochure



Version B Front



Version A Back



Version B Back



Version A – Victim feedback (n=11)

- Initial impressions to the blue brochure were largely positive, with respondents noting the brochure was engaging and informative and provided steps on how to fight fraud (including sharing information with family and friends).
- When asked what the brochure was trying to communicate, respondents reported that "we all have to work together to fight fraud," how to become a Fraud Fighter, that a lot of people get caught up in fraud (and the brochure indicates that they are not alone), how to report fraud, and that you should warn friends and family about fraud.
- When asked what action the brochure was asking them to take, respondents noted that it was a "mission that can be accomplished together," to be aware of scams and share information with other people so they do not get scammed, to report scams, to share their tips for spotting scams (i.e., to respond to the brochure prompts), and to become a Fraud Fighter. Some victims did not understand that they were being asked to return the completed prompts. This may be clearer when the return envelope is included with the mailing.
- Respondents found the following information to be most meaningful: the Post Office is asking for help to stop scams, those who fall for scams aren't alone, how to prevent fraud, and the value of sharing tips with family and friends.
- Words or phrases that stood out to respondents included "Fraud Fighter," "report mail fraud" in red ink, "you are not alone," and "you are one of the best tools to fight scammers." No respondents reported any words or phrases that bothered them.
- When asked if anything about the brochure was confusing, two respondents noted that the QR code was unclear (they were not sure how to do use it or if other seniors would understand it). Another respondent said it was not clear that the brochure was meant to be cut and

encouraged including a perforated line to make that clearer. Another respondent mentioned liking the fact that their responses to the brochure would be used to help other consumers, but also noted that they were not sure if they would respond.

- Respondents felt the material was easy to read, noting that the font size and colors were good, and the brochure was eye-catching. In terms of the length and "density" of the brochure, respondents felt that it had the right amount of information. One respondent noted that the brochure is small but contains a lot of information. Another respondent noted that if it was too long, many people would lose interest.
- All respondents reported that they would open and read the material. One respondent said that the phrase Fraud Fighter and the "law enforcement logo" (i.e., badge) would draw them in specifically.
- When asked what it means to be a Fraud Fighter, respondents largely responded that a Fraud Fighter is someone who reports fraud, informs other people about fraud, and is "on alert" about fraud. A few respondents reported some confusion at the question. Responses included: "Fraud is on the rise because nobody is doing anything about it." "I would like to report scammers but I don't have the right phone numbers to do so. Who would I report it to?" "Is being a Fraud Fighter just working with USPIS to avoid scams? I thought it was everyone working together to stop fraud."
- Most respondents said that being a Fraud Fighter seemed easy and not like a lot of effort. One respondent said that it sounded easy but also strange and didn't like the wording of "Fraud Fighter."
- When asked if they would complete the prompts and mail their responses back in, most respondents said they would. One respondent added "someone took the time to [send] this, so if I don't take the time then how will they know; its important, and to protect myself only takes a moment... it's something I should do." Two of the respondents who said they would probably not mail it back were prompted further: "What if we just asked you to tell your story? Would you be willing to send that back in?" Both said that they would be more likely to mail it back in this case.
- Respondents could not always verbalize how the USPIS should use the information that they mail in. How the information will be used should be clarified.
- Some victim respondents thought that the USPIS should already know the information that the brochure was asking for them to complete and that those tips should be shared with them.
- Interviewers asked respondents to answer the following brochure prompts:
 - Prompt 1: What clues can tip you off that a letter is fake?
 - Fake business names, seals, bar codes or number codes; mail that promises the reader that they won something but have to pay money to receive it; it comes from someone you don't know or haven't done business with; grammatical errors.
 - Prompt 2: What will you do the next time you receive a suspicious letter?
 - Report it; throw it away; share with someone I know and get their opinion.
 - \circ Prompt 3: Why is it important to you that the USPIS is working to fight fraud?
 - To keep vulnerable folks safe from scams; it's important to know that they are helping folks.
 - Prompt 4: Why is it important not to send money to criminals?

- This is not included in Version A, but was asked of 1 respondent, who responded "Because it's wrong."
- When asked how the USPIS should use the advice that it collects from Fraud Fighters via the brochure mail-in, respondents suggested pulling it all into a database or report and following up with Fraud Fighters (to confirm receipt of/thank them for the advice, to keep them informed of plans to fight fraud).
- When asked how important it was that others read the advice they mailed in, respondents largely said it was important to them, adding that a blog or a large group would be a great way to share that information, and suggesting that consumers may have ideas about mail fraud that the USPIS had not thought of.

Version A – Non-victim feedback (n=4)

- Initial impressions were mixed. One respondent was adamant that they would throw it away immediately due to the "Be a Fraud Fighter" message. Another said that the colors were too dark and did not catch the reader's attention. On the other hand, one respondent felt that the brochure was clear and had useful information. Another said that it was not clear how to become a Fraud Fighter but was comforted by the "you are not alone" message.
- Only one respondent was asked what the brochure was trying to communicate; she said, "that I can help, that I am not the only one, and that I can become a Fraud Fighter."
- When asked what action the brochure was asking them to take, responses were mixed. One respondent noted that the brochure is asking you to read it to learn how to help fight fraud, but also stated that it was unclear who she was being asked to fight fraud for and suggested showing people's faces on the brochure. Another said that the action she was being asked to take was to fill in the prompts and mail it back in.
- Respondents found the following information to be most meaningful: that the USPS is asking them to take action, that the USPS wants their help to fight fraud/stop others from being scammed, and that they are not alone.
- Respondents felt the material was easy to read, noting that the font size was good. Reactions to the length were mixed. One respondent mentioning multiple times that it was too long and that most recipients probably would not read the whole thing. Two other respondents noted that the brochure was "nice and short, which is good." The only respondent asked how likely they would be to read the brochure said that they would and noted that the badge was particularly drawing them in.
- When asked what it means to be a Fraud Fighter, respondents stated that Fraud Fighters would take the time and effort to contact the Better Business Bureau (adding that if fraud is such a serious problem, there should be collaboration with other groups that fight fraud) and would help the USPIS fight fraud "for people like me." Another respondent stated that being a Fraud Fighter is "nothing that you would expect me to spend my full time doing. [I would] talk to people, wear my badge...we are all in it together. If you see something, say something." Another respondent agreed that being a Fraud Fighter did not seem like a lot of effort, adding "all you are doing is asking me to fill this out and mail it in." One respondent felt that it was very time-consuming and hypothesized that "most people will take care of their own business, but probably won't step out to try and protect someone else."

- When asked if they would complete the prompts and mail their responses back in, responses were mixed. Two respondents said they would not. One of these stated that they "did not have time for this" and suspected that no one would reply unless they were bored. She suggested that a YouTube video would be more likely to get people's attention. The other respondent believed that mailing something back in would make them believe the brochure itself was a scam. When asked what would make them more likely to send in responses, this respondent said that they would automatically be suspicious because they received the brochure out of nowhere and suggested a PSA so recipients could get a heads-up that mailings like these were forthcoming. Two respondents noted that they probably would mail responses back, and one suggested including text on the envelope encouraging recipients to complete what is inside to help fight fraud. The other respondent said they would answer what they could and would send it back even if they did not have answers to all three prompts.
- Interviewers asked respondents to answer the following brochure prompts:
 - Prompt 1: What clues can tip you off that a letter is fake?
 - Fake or suspicious organization names, poor grammar and misspellings, logos that appear to be photoshopped, and asking the recipient to buy something that costs a lost of money.
 - Prompt 2: What will you do the next time you receive a suspicious letter?
 - Report it, throw it away.
 - Prompt 3: Why is it important to you that the USPIS is working to fight fraud?
 - Mail is something that everyone gets, so the USPIS is the best way to stop scammers from targeting vulnerable people; it is important that the post office be proactive if someone is doing something illegal.
 - One respondent noted that they were not aware that the USPIS was fighting fraud and added that they did not learn anything about the USPIS's efforts via the brochure; they further noted that the brochure is putting the job of fraud fighting onto the consumer.
- When asked how the USPIS should use the advice that it collects from Fraud Fighters via the brochure mail-in, one respondent suggested a large campaign, using people that seniors would recognize to share the message (the governor of their state; the president). Another respondent wished that the USPIS would follow up with individuals who provided information and expected the USPIS to be proactive instead of reactive.
- When asked how important it was that others read the advice they mailed in, two respondents said it was not important to them, with one adding that they wanted to be assist but did not imagine having insight that would be helpful. Most victim respondents said that it was important to them that their advice be read.

Version B – Victim feedback (n=6)

- Initial impressions were positive, with respondents noting the brochure was helpful, colorful, attention-getting, and engaging.
- When asked what the brochure was trying to communicate, respondents noted being a Fraud Fighter, informing the USPIS about fraud and tactics that scammers use, helping other people to avoid scams, and "deputizing me to go around and help people, letting friends and family know what kinds of things to look for."

- When asked what action the brochure was asking them to take, respondents noted they should throw away scam mail, not to send money to scammers in the mail, to become a Fraud Fighter (which includes helping people, spotting fake letters, and reporting fraud), to fill in the brochure prompts and mail it back to the USPIS, and to have people who have gone through scams spread the word to other people. However, one respondent added that they were not sure how effective the brochure would be to get people to fight fraud.
- "You are not alone" stood out to one respondent, who added that the more resources you can provide to people who need help, the better. Another respondent noted that being a Fraud Fighter helps them feel empowered to help others who have gone through the same thing.
- Respondents did not find anything upsetting or confusing about the brochure.
- Respondents felt the material was easy to read, noting that the length was good and the background color and text color "shout" at the reader (which they meant as a positive comment). Respondents said they were likely to read it, with one respondent noting that he would read it because he had been a victim.
- When asked what it means to be a Fraud Fighter, respondents stated that it means to fight fraud by helping others not fall for scams, to stop criminals from scamming people, and to be aware. One respondent said it means "don't be a dummy!"
- Most respondents said that being a Fraud Fighter seemed easy and not like a lot of effort. One respondent noted that this call would probably "ring true" more to people who had experienced fraud and wondered, "If I become a Fraud Fighter, what do you expect of me? How much time will it take?"
- When asked if they would complete the prompts and mail their responses back in, two
 respondents said that they probably would, three said they might or might not, and one said
 they definitely would not. When asked what would make them more likely to mail their answers
 back, one respondent suggested monetary incentives. When asked whether they might be more
 likely to send a response back if they were asked to tell their story, one respondent said that this
 would be more effective, and one said that it probably would not, noting that "a lot of people
 don't care to help others." One victim stated that sharing a personal fraud story seems to make
 more sense than providing tips to the USPIS, because the USPIS should know about those tips
 anyway; however, the agency would not know the person's story.
- Interviewers asked respondents to answer the following brochure prompts:
 - Prompt 1: What clues can tip you off that a letter is fake?
 - Made to look like Publisher's Clearinghouse or a sweepstakes; grammar and spelling mistakes; mail from someone you do not know.
 - Prompt 2: What will you do the next time you receive a suspicious letter?
 - Throw it away; don't send money; report the letter; research where it is coming from.
 - Prompt 3: Why is it important to you that the USPIS is working to fight fraud?
 - To stop criminal activity and prevent more people from being scammed; reducing scam mail will probably reduce the USPS's workload; saving people a lot of heartache (from being scammed); they have an obligation because the scammers use their platform [the mail] to scam people.
 - Prompt 4: Why is it important not to send money to criminals?

- You have no idea what criminals are doing with the money you send; you will never see the money again; you do not want to help with criminal enterprises; can be used for trafficking or terrorist activities (respondent referred to the "Who are the Scammers?" brochure).
- When asked how the USPIS should use the advice that it collects from Fraud Fighters via the brochure mail-in, respondents suggesting sharing them via a new letter or other pamphlets and following up with Fraud Fighters to thank them for sending in the information and update them on how they plan to use it.

Version B – Non-victim feedback (n=9)

- Initial impressions were mixed, with some respondents being confused about what is being asked of them ("What is a Fraud Fighter?") or wondering if the brochure itself was a scam ("I don't know about sending something back").
- When asked what the brochure was trying to communicate, respondents stated: information about fraud; that Americans need to be careful; that I am an important tool to fight fraud (by providing information); to share information and mail back the answers; how people can help with mail fraud; and learning what not to do with scam letters.
- When asked what action the brochure was asking them to take, reactions were mixed. One
 respondent was not clear that the brochure was asking them to respond and mail back their
 answers. Another respondent said that while the brochure was good, most people probably
 would not take it seriously until it happened to them or someone they love. Respondents who
 did identify actions named sharing information with other people and reporting fraud.
- Respondents found the following information to be most meaningful: how to report fraud, knowing they were not alone, and that they could help by informing their friends and family.
- Words or phrases that stood out to respondents included "Fraud Fighter," "you can help others," "tell your friends and neighbors," and the mechanisms for reporting fraud. No respondents reported any words or phrases that bothered them.
- When asked if anything was confusing about the brochure, one respondent mentioned wanting to know more about how the USPIS catches scammers. Another respondent was surprised that mail fraud "was such a big thing."
- Respondents felt the material was easy to read, noting that the font size was good. One
 respondent suggested that the white text be in a different color (such as yellow) to be more
 vivid. Some respondents did not like the colors (too dark) or the USPIS logo (they were used to
 USPS, not USPIS). Two respondents really liked the look of the brochure, noting that the colors
 were bold and attention-getting.
- In terms of the length and "density" of the brochure, five respondents felt that it had the right amount of information and was not too long. Two respondents felt the brochure was too long and wordy.
- Two respondents said they probably would not have read the brochure. One said that they would, and a fourth said that they would probably read it but probably would not respond to the prompts but might write in asking for clues to tell if a letter is fake.
- When asked what it means to be a Fraud Fighter, respondents said to help the USPIS fight scammers; to take action against fraud; to protect yourself; and to share the information with other people.

- Half of the respondents felt that being a Fraud Fighter seemed easy and not like a lot of effort. Two respondents felt that it would be a lot of work, with one suggesting that if you could just give fraud mail back to your mailman, people might be more likely to report it. Two respondents felt that it would be some effort, but not very much: one respondent said that "everything is an effort, but this isn't extreme. People would want to share information, because it's worthwhile." Another respondent said that it did not seem like much effort to them, but they thought some people may see it as too much effort, especially if sharing information with others might put them into a public light that they may not want.
- When asked if they would complete the prompts and mail their responses back in, most respondents said they would not. One respondent noted that if she had been scammed, she probably would, but if she had not been scammed, she probably would not. Another respondent said that it felt like a test. Three respondents said they might complete and return the card if there was a prepaid envelope. When asked what we could do to make them more likely to complete and return the card, respondents suggested using more red, white, and blue ("government colors"), shortening it, and adding the phrase "Please help us!" to the brochure.
- Interviewers asked respondents to answer the following brochure prompts:
 - Prompt 1: What clues can tip you off that a letter is fake?
 - Misspellings and grammar errors; if the letter asks for money; if the company name/sender is not familiar; and fake logos.
 - Prompt 2: What will you do the next time you receive a suspicious letter?
 - Give it to the mailman or take it to the post office; go online for more information; get advice from the phone number on the brochure; throw it away; report it.
 - Prompt 3: Why is it important to you that the USPIS is working to fight fraud?
 - To protect people; a government agency should be working for us; because it is a big problem; to keep us safe.
 - Prompt 4: Why is it important not to send money to criminals?
 - Once you respond, you will be on their lists and will get more and more scam letters; don't want to give your money to bad people.
- When asked how the USPIS should use the advice that it collects from Fraud Fighters via the brochure mail-in, respondents suggested giving people instructions/warnings rather than asking them questions; try to develop a way of catching it before it goes out.
- When asked how important it was that others read the advice they mailed in, respondents' replies were mixed. One respondent thought it was very important, especially if they took the time to send in their answers. Another respondent said that it would not be important to him at all, but what would be important was that an intervention that stopped fraud was successful. Another respondent said it would not be a big deal if the advice he gave was not "picked," but he did hope that the USPIS was reviewing the replies to ensure that they made sense.

Meet Your Team Flyer





Version A – Victim feedback (n=7)

- Initial impressions were largely positive, with respondents noting that they liked the image (people of color featured; it was nice to see the faces behind the work).
- When asked what the flyer was trying to communicate, respondents stated: how to combat mail fraud and stop scams; not to respond to suspicious mail; the confidence and security that there's a government entity that is protecting the public (the USPIS).
- When asked how the USPIS combats mail fraud, responses included:
 - When the mail gets to the post office, they try to take out suspicious mail before it gets distributed, and look for mail going overseas
 - If there is a fake address or fake name or the home is vacant
 - Drawing attention to the fact that mail fraud is going on (by mailing flyers like this)
 - They don't, they are not well funded
- When asked what actions you can take to combat mail fraud, respondents said they could talk to law enforcement (including the FBI) to have their mail investigated; talk to friends or family about it; and contact "the US mail service" if you get any fraudulent mail.
- When asked how likely they were to take the action steps, respondents largely said that they would do them. Two respondents felt that they would be most likely to take the second step (reporting the fraud); two felt that they would be most likely to take the third step (telling friends/family). One respondent reported they would be least likely to tell their friends and family; another said that making a report would be the hardest step.
- Words or phrases that stood out to respondents included "How we stop fraud" and "submit a complaint online" (because some people might not want to call).
- When asked if anything was confusing about the brochure, one respondent mentioned questioning whether foreign scammers were the biggest problems; another wondered why the flyer had been folded before mailing to her.

- Using their own words, respondents struggled to explain how the USPIS identifies mail fraud based on what they read from the brochure. They needed to refer to the text and started reading it aloud.
- Respondents felt the material was easy to read and was not too long.
- When asked if they learned anything new from the flyer, one respondent said no, that everything in the flyer was already on "the other one" (likely the letter and/or brochure, which would have been reviewed before the flyer). One respondent learned that the USPIS existed and was already working to fight fraud; another respondent learned to contact the "postal service;" a third respondent learned they did not need to be hesitant to throw fraud letters away.
- When asked if it made them feel more connected to other Fraud Fighters, most respondents said it did.
- Most respondents really liked the image, noting the mix of genders and races. One respondent
 suggested providing the names of the officers pictured. One respondent noted that they looked
 like "common people who want to help" and added that the badges were effective. Several
 were curious to know whether the people pictured were actually USPIS employees or actors.

Version A – Non-victim feedback (n=7)

- Initial impressions were largely positive, with respondents being pleased to learn there was a department that combats mail fraud, that there are real people on the flyer, and that the flyer gives actionable steps. One respondent said she thought that the flyer was "corny," that she did not know what a Fraud Fighter was, and that the logo did not make her want to read more, but she did admit that the information was important.
- When asked what the flyer was trying to communicate, respondents stated: the USPIS is real people; how to report fraud; tell other people about it; not to respond to mail fraud.
- When asked how the USPIS combats mail fraud, respondents said that the USPIS tries to stop fraud ("it tells us what they do but not how they do it"); that the USPIS scans payment envelopes from victims and looking at suspicious bulk mailings; and that we need to report fraud and tell others.
- When asked what actions you can take to combat mail fraud, respondents listed reporting fraud, not responding to the letter, and telling other people about it.
- When asked how likely they were to take the action steps, most respondents said they were likely to take the steps. One respondent said that they would if they got a scam letter, they would probably bring it to the post office. Another stated that they would set aside suspicious mail and report it if they had a lot of time on their hands, but currently they throw away suspicious mail.
 - Respondents felt that the easiest step was to not respond to scam mail.
 - No steps seemed too daunting, but two respondents stated that if they had to rank the steps by how likely they were to do each, they would rank "tell family/ friends" last.
- One respondent thought the phrase "Meet Your Team" really stood out. Another respondent said that the phrase "any letter that asks you to pay money in order to win money is definitely a scam" stood out and even suggested highlighting that phrase.
- Respondents did not report that anything was confusing about the flyer.
- Respondents felt the material was easy to read, noting that the font size and color scheme were good. One respondent mentioned the action steps being numbered was helpful. Most

respondents thought the length of the flyer was good; one respondent thought that the left column was too wordy.

- When asked if they learned anything new from the flyer, respondents mentioned the fact that they can report fraud to the USPIS and learning about the existence and purpose of the USPIS itself.
- When asked if it made them feel more connected to other fraud fighters, reactions were mixed. Two respondents said no; one said yes. The other three had mixed reactions, stating that the flyer made them more aware of the fact that there was a USPIS team, but they did not necessarily feel more connected to them or to other Fraud Fighters.
- Regarding the image, feedback was mixed. One respondent wondered whether it was necessary to include pictures of people at all (if the goal is for us to help them combat mail fraud, why do we need to know who "they" are?). Another thought that by smiling, the agents looked less serious. Three respondents liked the picture, noting that they looked like normal, everyday people who were ready to do their job.
- Respondents suggested some improvements, such as turning the right column into a magnet that lists the steps and spelling out what USPIS stands for more clearly (maybe in the title).

Version B – Victim feedback (n=7)

- Initial impressions were largely positive, with respondents noting it was eye-catching and gave information on how to become a Fraught Fighter.
- When asked what the flyer was trying to communicate, respondents stated: how the USPIS stops mail scams; that if you are asked to send money overseas, it is a scam; not to respond to fraud; how the USPIS goes about its job and detect scams; how to make a report.
- When asked how the USPIS combats mail fraud, respondents stated: the USPIS depends on me to report mail fraud and spread the word; looking for suspicious mailings; arresting and prosecuting scammers.
- When asked what actions you can take to combat mail fraud, respondents mentioned telling family and friends; not responding to suspicious mail; and making a report.
- When asked how likely they were to take the action steps, respondents largely said that they would and that the steps made sense. One respondent said they likely would not talk to friends and family about it because it might sound accusatory.
 - The most likely step for one respondent was reporting it; for another, it was not responding to the fraud.
 - One respondent said that making a report seemed the hardest; another said that they probably would not report every single scam letter they got.
- Words or phrases that stood out to respondents included "You can help us," "Be a Fraud Fighter," "report," that USPIS does not actually look at the mail and just passes it along to you, so you have to determine if it is a scam; "scammers get craftier."
- No respondents reported any words or phrases that bothered them.
- When asked if anything was confusing about the brochure, one respondent did not understand what "call 877-876-2455 for dedicated line and leave a message" meant.
- Respondents felt the material was easy to read, noting that the font size was good and the length of the flyer was not too long.

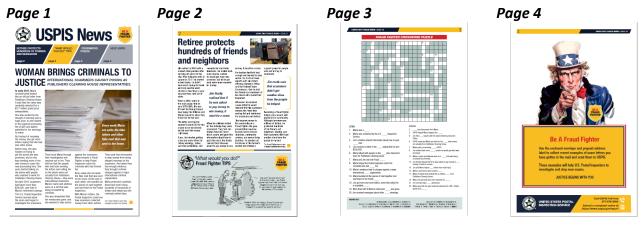
- When asked if they learned anything new from the flyer, one respondent stated they learned to contact "the post office." Another reported learning what number to call to report, and a third stated that a lot of scams are being sent overseas and the USPIS is stopping payments to individuals if they are known scammers.
- When asked if it made them feel more connected to other Fraud Fighters, three respondents said that they would, and one agreed that they felt more connected but was unenthusiastic. One respondent did not feel more connected but also said that they did not realize that they could contact the USPIS if they had problems with the mail.
- Respondents liked the image, with some of them pointing out that it was diverse in gender and race, and others noting the badges which made the individuals look more like law enforcement who are "on top of it." One respondent suggested maybe adding a USPIS sign behind them.
- Respondents suggested adding information about military scams to the flyer and bolding the 877-phone number.

Version B – Non-victim feedback (n=6)

- Initial impressions were largely negative, with one respondent saying that even if they were expecting it in the mail, they would throw it away. (Additional feedback is included below in response to specific prompts.)
- When asked what the flyer was trying to communicate, respondents stated: they are introducing us to the team; making people aware that they can help stop scams; the actions you can take are very clear and numbered; the USPIS is asking me not to send money to a scammer; that scammers change their addresses to avoid getting caught.
- When asked how the USPIS combats mail fraud, respondents listed: they stop it with the information we give them [about fraud]; they have a dedicated line where you can leave a message.
- When asked what actions you can take to combat mail fraud, respondents said that they can report the letters they receive; they should not respond to the scams; they should tell their friends and family.
- When asked how likely they were to take the action steps, respondents said they were pretty likely to take them.
 - One respondent said the step they were most likely to take was to report the fraud; another said not responding to fraud was most likely for them; a third said that telling friends and family and reporting the fraud were equally likely; and a fourth said that telling friends and family was the most likely. No steps were noted as being too daunting.
- Words or phrases that stood out to respondents included "anything that asks you to pay money is a scam" and "how you can be a Fraud Fighter," but this respondent noted that it stood out due to the color/font not due to the language used.
- When asked if anything was confusing about the brochure, one respondent said that the USPIS was not spelled out. After being informed that it was spelled out in the first sentence, they said that it was not capturing their attention.
- Respondents felt the material was easy to read, noting that the font size and color scheme was good. In terms of the length and "density" of the brochure, most respondents felt that it had the right amount of information and was not too long.

- When asked if they learned anything new from the flyer, two respondents said they did, noting that they learned how they can help and what to do if they get a scam letter.
- When asked if it made them feel more connected to other Fraud Fighters, three respondents said that it did not, with one adding that they had no interest in being connected to the postal service. Another suggested that the flyer would benefit from a personal slant or a celebrity spokesperson to make people feel connected. One respondent noted that if the flyer is designed for us to "meet your team," they would expect to see more than a toll-free voicemail line (including maybe identifying some of the inspectors by name).
- Reactions to the image were mixed:
 - One respondent stated that this was their favorite item, adding that they know there are real people with badges who are inspectors for the USPIS (rather than just sitting behind a desk/taking phone calls).
 - One respondent felt that having three agents holding their badges out was "overkill" and suggested maybe having just one.
 - One respondent said that the image "looks like the FBI or police are coming to get me, scary" but also added that it was nice to see diversity in the picture.
 - One respondent noted that he liked the badges but did not like the image overall.
- Respondents suggested several improvements, such as having a local number to call instead of the 877 number; using the flyer to hang up in public spaces or places that seniors frequent; and making sure the flyer could be read and understood by high school graduates (to reach the greatest number of people). One respondent suggested putting this information in a brochure rather than this "odd-sized" (legal size) handout; another suggested making it standard 8.5" x 11" size.

Newspaper Tabloid



- Participants (14) were divided on the newsletter. Some, self-professed "newspaper and crossword lovers" loved the idea of the newsletter. They said it was engaging and they would absolutely do the crossword (participants did not differ by victimization but tended to be respondents aged 65 years or older). These participants were also more likely to like the "Uncle Sam" image on the back.
- Others (6) thought the newsletter was "gimmicky" or too long and said they would toss it. They said they would not do the crossword and did not like "Uncle Sam" pointing his finger at them on the back.
- In general, participants found the stories to be engaging, realistic, believable, and relevant to their life. A few participants noted the "sensationalized" heading, but these individuals were in the minority.
- Several participants said that having something like this placed in senior centers, community centers, and other places where seniors gather would be very effective outreach.
- Most participants said they would send the materials back to the USPIS. Participants noted having a pre-paid envelope would help encourage them.
- A few participants noted the size of the newsletter was too large. They suggested paring it down to something smaller. One participant noted, "If it was this size, I would toss it right away. It looks to me like something I would get from somebody like Target. It doesn't look real. I would rather get a newsletter half this size, I would look at it closer than this size. It looks too much like a weekly ad than an informational newsletter."

Scammer Brochure

Front



Back



- In general, participants were able to understand the intent of the brochure, citing "crime" and "criminal activity." Some participants said that they thought the money just went to the scammers' pockets but instead went to crime: "People think it's just somebody who wants to take your money and buy a big TV or something, most people don't know that it goes toward human trafficking or things like that."
- In general, participants liked this brochure and only had a few minor suggestions. One participant asked for statistics to be included. He wanted to know the number of criminal scammers who had been caught and convicted. He said other statistics would make it more believable and engaging.
- Although participants often felt they learned something new from the brochure, not everyone liked the images. One participant thought the images looked like something off of *Dateline* and they would probably just throw this away; interestingly, another participant liked the images, citing a "true crime podcast" as inspiration. Participants who mentioned learning something new, most commonly cited learning about the criminal component and that scammers keep lists and share the lists with other scammers. However, when prompted, no participants suggested alternative images over the ones presented.
- One participant did not like the image with the teddy bear and did not know what it was trying to communicate.
- Some participants (9) mentioned the color scheme as being too dark (participants who mentioned this feedback tended to be female respondents aged 65 years or older). Note: the printed version of the map seemed to show up much darker than the PDF version.
- Two participants also mentioned not liking the quad-fold format. They said they did not know which side to read first (i.e., which was the front or back).
- Participants differed slightly in terms of who would read the brochure versus just throw it away upon receipt. Victims were more likely than non-victims to say they appreciated the brochure, and non-victims were more likely to say they might just throw it away without reading it.

Thank You Card

Front



- Several participants did not understand why they might be receiving this letter. Interviewers explained the concept, and they thought it sounded nice. Note: most participants who asked questions about *why* they were receiving this thank you card were non-victims. Victims seemed to appreciate the efforts by the USPIS more.
- Most participants liked the format and the color scheme. One participant did not like the color scheme, and another did not like the logo, but all of the other participants had positive feedback.
- The majority of participants found the bookmark to be helpful information and would tear off and keep the bookmark for later. One participant noted that we could add a scissor icon to denote that it should be cut or torn off.
- Note" a spelling error "Please tear of."

"Swag" Address Labels



Picture Frame Magnet



- Results were mixed in terms of participants reaction to the "Swag" materials. Although some participants thought it was a nice touch and said they would use it, other thought the address labels were useless (they already get too many and almost never send anything via the mail anymore) or odd (one participant mentioned it was odd that the frame magnet where he might put a picture of his grandchildren would say "report mail fraud" on it).
- In general, when participants were asked to choose which item they would liked more, they chose the address labels.

All Mailing Questions/Closing Questions

- Do any of these mailings change the way you think about scams? Which ones? Why?
 - Most participants stated that the information changed how they think about scams, specifically that mail fraud was such a prevalent issue (outside of phone and internet scams), and how to protect themselves. Many of the participants who stated that the information did not change how they thought about scams said that this was because they already considered themselves to be scam-savvy.
 - The participants who reported that the letters did change how they thought about scams reported that the following materials helped:
 - The first letter: "I wasn't aware that when they intercepted something you would get it back."
 - The newspaper: "It was like, 'Hey, you better watch out because fraud is still happening.'" Another participant added that they liked the stories.
 - The scammer brochure/map: "I didn't associate [scams] with human trafficking and drugs, so that really stood out." Another participant added "I thought the money going to scammers was going to luxury things, but it is used for drugs, sex trafficking, and terrorism; I was really shocked."
 - Responses did not differ by age range or by victim/non-victim status.
- What would be a good way to make sure that people who have experienced mail fraud see this information?
 - Participants suggested several ways to inform victims of fraud, including the following:
 - Radio, TV commercials, or billboards
 - Senior centers or senior living facilities common areas and community clubhouses
 - Mailing the information to everyone
 - One participant suggested sending the information just to those who had been identified as having been victims of a mail scam
 - Social media
 - Email or phone calls (but the participant who suggested this noted that it might not be effective given all of the phone calls we get on a daily basis, and sending an email to someone who fell victim to mail, not email, fraud might not be feasible)
 - Magazines, especially AARP, placed in doctor's offices or other places people sit and wait
 - From trusted people in the community, such as community advocates, community organizations, case managers, and even via schools.
 - Have restaurant or local businesses do promotions for fighting mail fraud, similar to teacher appreciation day
 - Posting the information in the local Post Office
- How would you feel if you got these letters from the USPIS right after the fraud?
 - Participants were divided on this issue, with many of them saying they would feel like a fool, would feel terrible for having given money to scammers, or would be mad that the information got to them *after* they fell for a scam. However, the majority of participants, even after citing embarrassment, would feel grateful and happy that someone was on the case, watching out for them and trying to get their money back to them, "Like man I wish I would've known about this before, but glad I know now and hopefully I don't do it

again in the future." "I would feel stupid. But then I would feel like someone is looking out for me."

- Responses did not differ by victim/non-victim status or by age range.
- Would you feel embarrassed to be receiving these letters?
 - Participants were divided on this issue. Some said that they would be embarrassed to talk about it and receive letters, adding that they think many other people would be embarrassed too and that might be why mail fraud goes unreported. Other participants added that they would not necessarily be embarrassed by the letters but would be embarrassed by their own actions of falling for a scam in the first place ("I would be embarrassed that I had done something stupid." "What was I thinking?" "Yeah, like SUCKER is written all over you.").
 - Several victims stated that it may feel embarrassing to receive these, but being protected and informed outweighs those negative feelings.
 - Participants who reported that they would not feel embarrassed added that they would be thankful that they were more aware now. One participant added that if a friend or family members got scammed, they likely would not be embarrassed and would appreciate the help and support the letters would bring.
- Would receiving these letters help you feel like you have more power to fight fraud?
 - Most participants said "yes" to this item, adding that they would feel empowered because they had information on what steps to take, how to help friends and family, and that someone is working to help them.
 - One participant noted that they would not feel like they had more power, per se, but did think that they would feel better having received the information.
 - Additionally, a few participants noted wishing some of these materials came to them together. One participant said she would like the magnet and the thank you letter to be paired together, while another mentioned pairing the Meet Your Team flyer with the standard letter.
- Would you want to continue to receive fraud awareness information?
 - Overall, most participants said "yes" to this item, noting that scams are changing all the time and they would like up-to-date information.
 - One participant said they would only want information on new scams, or annually at most. Other participants added that since scams change often, they would be especially interested in staying connected, particularly if materials were mailed monthly.