ASPEN TECH POLICY HUB

POLICY

GINNY FAHS

Protecting Seniors Via Technology & Design Policy

The number of online scams targeting older Americans has increased by more than 400 percent during the past five years and amount to $650 million in annual losses for seniors. To cut down on scams, government agencies like the Federal Bureau of Investigations (FBI) and the Federal Trade Commission (FTC) use scam data contributed by victims and private companies to investigate incidents, analyze criminal patterns, and prevent future crimes. Unfortunately, fewer than one in thirty victims report scams to the government.[1] Moreover, operators of large online platforms where scams proliferate do not contribute information on incidents to federal databases.[2]

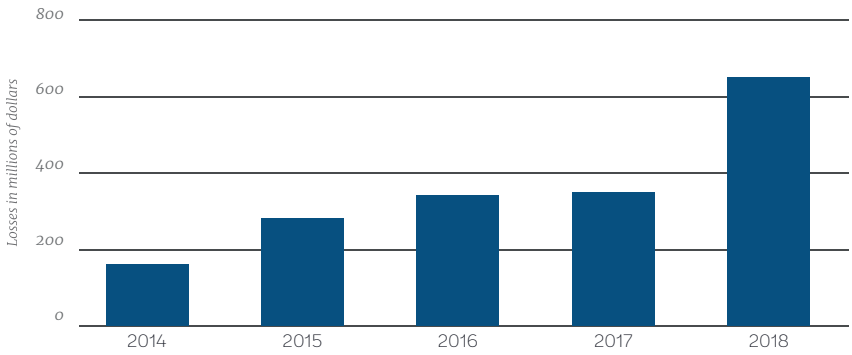
To build and develop scam data sets, the federal government needs to solicit information about and from major online platforms where scams proliferate and improve digital reporting forms such that they are broadly usable by older adults. Beyond scams, legislators and government technology teams should analyze and incorporate older adults' online interaction needs as they craft policy and extend digital services.

BACKGROUND

The $650 million that older Americans lose to online scams every year[3] is a drastic underrepresentation of the effect scams have on our nation's elderly.[4] The reporting of online scams enables officials to perform investigations into past crimes and take preventative measures to inhibit future incidents. Yet many Americans do not know that reporting scams to the federal government is important, nor they do know how to submit a report. Moreover, our user research with older adults shows many who do try to report these crimes to the government cannot do so due to the design of the online reporting form. Without sufficient information about the nature of scams that target the elderly, government officials are not informed about what actions to take, and scams continue to multiply.

This problem is worsened by the fact that scam tactics have evolved, while federal databases, reporting forms, and scam prevention efforts have not kept pace. Half of scams against the elderly now happen online,[5] whereas in the past, the majority transpired over the phone. Scam working groups and government officials continue to focus on robocalls, collecting far less information about the online platforms where scams often occur. Meanwhile, the technology used to perpetrate fraud is evolving quickly, and scams are already starting to penetrate voice assistants and IoT products. The failure to adapt reporting systems and engage corporate actors in fighting the problem feeds the growing scam epidemic and makes future scams even harder to prevent.

Five Years of Losses for Online Scam Victims Age 60+



The U.S. has seen a 400% increase in online crime against adults age 60+ since 2014

RECOMMENDATIONS

We met with officials across multiple government agencies and scam working groups to understand the state of existing federal databases and online scam reporting services. We also conducted scam-themed design thinking workshops and reporting form user testing with older adults in local senior centers in San Francisco. Three key recommendations emerged from these activities:

1. Agencies should solicit information about and from major digital platforms to bolster scam databases;
2. Government should understand barriers to scam reporting and improve digital reporting forms; and
3. Legislators and government technology teams should incorporate the interaction needs of older adult users in policy initiatives and digital service design.

ASPEN TECH POLICY HUB

POLICY

1

Agencies Should Solicit Information From Major Digital Platforms to Bolster Scam Databases

It is an unfortunate truth that avoiding cybersecurity investment boosts profits for corporations, who sometimes even run scams on their own users.[6,7] Self-reported scam data from the past five years shows that romance scams (scams on dating platforms) resulted in $473 million in losses for older adults, more than any other scam type; social media scams saw the fourth-most losses, with $162 million stolen.[8] Online dating and social media platforms currently contribute no data to government on the issue. What's more, current scam reporting forms do not ask victims to list the online platform where their scam began, so government agencies do not know which private companies are most commonly involved.

The government should make scam data transparent and engage industry directly on the issue. In addition to receiving information about scams from victim reports, government agencies should require private corporations to contribute data on the topic. The Sentinel Database is a secure online database of consumer fraud reports maintained by the FTC and available to law enforcement; soon it will also be shared with the FBI.[9] Select state offices, corporations, and nonprofits contribute their fraud data to Sentinel.[10] No online dating services or social media platforms contribute currently.

- Consumer complaints data within the FTC Sentinel Database should be made public with offending companies named. Public data is the best way to force a business case for corporations to invest in their own cybersecurity, as companies will seek to maintain good reputations and prove their safety over competitors. A public database strategy has already been successful with the Consumer Financial Protection Bureau's Consumer Complaint Database, for which 97% of complaints sent to companies get timely responses;[11] public data would similarly serve the FTC's charter of reducing consumer fraud.

1

- The FTC should conduct a 6(b) study soliciting data about scams and fraud from the largest online dating and social media platforms and publish the findings publicly. Section 6(b) authorizes the FTC to get "special reports" from companies about certain aspects of their business.[12] Companies are already detecting and monitoring fraud in their systems; sharing this data would inform the government and the public on the scale, scope, and nature of existing scams — as well as which platforms are the worst offenders.
- The FTC should require major online dating and social media companies to contribute data to the Sentinel Database. Contributions to Sentinel can be made by sharing CSV spreadsheet files; contributing to Sentinel does not require technical work or integrating external APIs. The results of the aforementioned 6(b) study would make clear which platforms should be approached for contributions most urgently.
- State Attorney Generals in all 50 states should contribute to the FTC Sentinel Database. State Attorney Generals are able to offer more comprehensive support to victims of scams than the federal government can, making them a good option for victims seeking to report. However, only 16 State Attorney Generals Offices currently contribute data to Sentinel.[13] Complete participation from State Attorney Generals would maximize support for scam victims while enabling the federal government to receive the data they need to investigate cases and understand scams on a national scale.
- The FBI and FTC should extend current scam reporting forms to ask victims to disclose social media platforms, dating platforms, voice platforms, and IoT platforms involved in scams. Requesting this information will enable government officials to better understand where romance scams and social media scams are coming from, as well as the rising threat of cybercrime conducted via voice assistants and smart-home IoT products.

ASPEN TECH POLICY HUB

POLICY

2

Government Should Understand Barriers To Scam Reporting And Improve Digital Reporting Forms

The existing government reporting system puzzles many older adults, their families, and professionals in elder services and elder fraud prevention. The FBI, FTC, and law enforcement each have their own reporting forms, and data submitted through these forms is not shared between the three groups. The design of many reporting forms is not intuitive for older adults; in our workshops, we saw seniors give up halfway through filling out reporting forms due to their difficulty in interacting with the form's design and comprehending the form's content. The efforts of different federal divisions need to be centralized and the design of digital reporting forms should be updated so that officials can capture more and better information about the nature of scams affecting Americans.

- The FBI, FTC, and law enforcement should collaborate to design a single scam reporting system, complete with a shared user-facing reporting form and a joined backend database to pool submitted information for cross-agency sharing.
- The design of all reporting forms should specifically cater to older adults, the age group most affected by online scams and fraud. Features like reveal logic, automatic caching, large text, interaction instructions, print capabilities, mobile and tablet adaptiveness, and a phone reporting alternative[14] will help ensure that scam victims who begin the reporting process are able to complete it.
- Advisory councils working on senior scams should engage seniors who have been scammed so that first-hand accounts help drive solutions. For example, the new Senior Scams Prevention Advisory Council authorized in S.149 - Stop Senior Scams Act[15] should include among its members at least one senior who has been scammed.
- The Senate Special Committee on Aging should host a hearing about reporting senior scams to better understand the crucial reporting angle of the problem. Fighting scams is one of the Committee's priorities. Yet none of their 22 hearings on scams has emphasized reporting, despite widespread recognition of underreporting as a cause of inaction.

3

Incorporate the Unique Needs of Older Adults into the Design of Policy Initiatives And Digital Services

How older adults make decisions is affected by changes in the ways they process emotions, a positivity effect (seeing the upside but not the downside of decisions), and gaps in short-term memory compared to other age cohorts,[16] making it easier for scammers to use online platforms to manipulate and deceive them. Designers of government services are not often aware of the unique needs of seniors, nor do they consider develop in lockstep with elderly users' input. Legislators are increasingly addressing digital design in policy initiatives, and they too are uninformed about seniors' decision-making patterns and how they translate to digital interactions.

- Agencies working on scam reporting should follow the guidelines of the Digital Services Playbook developed within the Office of Management and Budget[17] and the U.S. Web Design Standards developed by the General Services Administration[18] as they build and improve upon online scam reporting systems. The Digital Services Playbook outlines best practices that will help agencies deliver products and services more quickly and effectively by continuously involving real users of the services in the development process. The U.S. Web Design Standards provides a set of common UI components and visual styles for government websites that make it easier to create digital services that are elegant and usable by all, including people with accessibility and digital literacy constraints.
- Product designers within government agencies should complete training about seniors' design preferences, and they should be required to periodically test their products with older adult users. Designers within the U.S. Digital Service and 18F should pilot these trainings and ongoing user tests, as their frequent cross-agency collaboration will help these practices spread throughout government.

3

- Going forward, legislation related to digital design should make special considerations for seniors taking into account their online interaction needs. For example, the Deceptive Experiences To Online Users Reduction (DETOUR) Act prohibits the use of exploitative and deceptive practices by companies that operate online. Commonly referred to as dark patterns, these practices take the form of manipulative user interfaces designed to intentionally limit understanding and undermine choice.[19] Our research suggests certain dark patterns not identified in the DETOUR Act disproportionately affect seniors because they aim to capitalize on distraction and short-term memory blunders. The DETOUR Act includes special considerations for dark patterns that disproportionately affect children, but does not single out deceptive practices that particularly affect older adults.

Endnotes

1 Martha Deevy, Shoshana Lucich, and Michaela Beals, *Scams, Schemes & Swindles: A Review of Consumer Financial Fraud Research* (Stanford, CA: Financial Fraud Research Center, 2012).

2 Federal Trade Commission, "Consumer Sentinel Network Data Contributors," https://www.ftc.gov/enforcement/consumer-sentinel-network/data-contributors, accessed Aug 16, 2019.

3 Federal Bureau of Investigation: Internet Crime Complaint Center, "2018 Internet Crime Report," 16, https://www.ic3.gov/media/annualreport/2018_IC3Report.pdf, accessed Aug 22, 2019.

4 Numbers in the FBI's Internet Crime Complaint Center are an under-representation of the problem because they only represent self-reported scams. Many individuals who are scammed never realize it, and many individuals who do realize they were scammed never report the scam to the federal government.

5 Nicholas Mastrocinque, "Personal Interview," interview by Ginny Fahs (Aug 12, 2019).

6 Bridget Small, "Office Depot Computer Scans Gave Fake Results," *Federal Trade Commission* (March 27, 2019), https://www.consumer.ftc.gov/blog/2019/03/office-depot-computer-scans-gave-fake-results

7 Nicole Drayton, "FTC Sues Owner of Online Dating Service Match.com for Using Fake Love Interest Ads To Trick Consumers into Paying for a Match.com Subscription," *Federal Trade Commission* (Sept. 25, 2019), https://www.ftc.gov/news-events/press-releases/2019/09/ftc-sues-owner-online-dating-service-matchcom-using-fake-love

8 Federal Bureau of Investigation, *supra* note 3.

9 Federal Trade Commission, "Consumer Sentinel Network," https://www.ftc.gov/enforcement/consumer-sentinel-network, accessed Aug 16, 2019.

10 Federal Trade Commission, *supra* note 2.

11 "Consumer Complaint Database," Consumer Finance Protection Bureau, https://www.consumerfinance.gov/data-research/consumer-complaints/, accessed Nov 8, 2019.

12 Lesley Fair, "6(b) Or Not 6(b): That Is the question," *Federal Trade Commission* (April 23, 2012), https://www.ftc.gov/news-events/blogs/business-blog/2012/04/6b-or-not-6b-question, accessed Nov 8, 2019.

13 Federal Trade Commission, *supra* note 2.

14 The non-profit Cybercrime Support Network has received DHS funding to build a centralized phone reporting line to complement online reporting systems. CSN should receive further executive support to make their phone line a "one stop shop" that can also link up with federal agencies and offices like FBI, FTC, and Consumer Financial Protection Bureau (CFPB).

15 US Congress, Senate, *Stop Senior Scams Act of 2019* S.149, 116th Congress, 1st session, introduced in Senate Jan. 19 2019, https://www.congress.gov/116/bills/s149/BILLS-116s149is.pdf

16 Natalie Denburg, "Personal Interview," interview by Ginny Fahs (Aug 5, 2019).

17 "Digital Services Playbook," U.S. Digital Service, https://playbook.cio.gov/, accessed Nov 8, 2019.

18 "U.S. Web Design System," General Services Administration, Technology Transformation Services, https://designsystem.digital.gov/, accessed Nov 8, 2019.

19 *Deceptive Experiences To Online Users Reduction Act (DETOUR Act) of 2019*, S 1084, 116th Congress, 1st session, introduced in Senate April 9, 2019, https://www.congress.gov/bill/116th-congress/senate-bill/1084/text.

ASPEN TECH POLICY HUB

POLICY

ABOUT THE HUB

The Aspen Tech Policy Hub is a Bay Area policy incubator, training a new generation of tech policy entrepreneurs. We take tech experts, teach them the policy process, and support them in creating outside-the-box solutions to society's problems..

The Aspen Institute
2300 N St. NW, Suite 700
Washington, DC 20037
202 736 5800

THE ASPEN INSTITUTE