FTC SENIOR ID THEFT WORKSHOP
MAY 7, 2013
TRANSCRIPT
SEGMENT 1

MARK: Good morning, everyone. Thank you all for coming to the forum today. And for those of you viewing the webcast from your office or home, thanks for tuning in.

Before we get started, we need to make some security and safety announcements. So please bear with me.

First, anyone who goes outside the building without an FTC badge will be required to go through the magnetometer and x-ray machine prior to reentry.

In the event of a fire or evacuation of the building, please leave the building in an orderly fashion. I crossed out panic. So once outside of the building, you need to orient yourself to New Jersey Avenue. So go across the street to Georgetown Law Center. And on the right front sidewalk there, that's the rallying point for the first floor conference center. So you'll need to check-in there.

If it's safer to remain inside during an emergency, you'll be told where to go inside the building.

If you spot suspicious activity, please alert security.

Bathrooms. Located in the first floor lobby, there are signs. But you basically cross the lobby.

This event is open to the public and may be photographed, videotaped, webcast, or otherwise recorded. In fact, it is being webcast.

By participating in this event, you're agreeing that your image and anything you say or submit may be posted indefinitely at ftc.gov, or on one of the Commission's publicly available social media sites.

Now, going from the ridiculous to the sublime, we're going to be talking today about identity theft issues that affect seniors and the particular challenges seniors face, and caregivers face, and loved ones face.

We've assembled an impressive group of experts on these issues. But to start us off, it's my honor and pleasure to introduce FTC chairwoman Edith Ramirez.

The chairwoman joined the Commission as a commissioner in April 2010, and President Obama called upon her to lead the agency in March.

For many years, Chairwoman Ramirez has had a strong interest in the intersection of technology, law, and policy. Before joining the Commission, she handled a broad range of complex business

litigation matters, including intellectual property, antitrust, unfair competition, and Lanham Act matters as a partner in the Quinn Emanuel law firm.

As both a commissioner and as chairwoman, she's been particularly involved in data security and privacy issues. As the commissioner, she led the Commission's activities to implement the Asian Pacific process, the cross-border privacy rules, and testified before Congress on behalf of the Commission on both privacy and data security issues.

When she became chairwoman, she made clear that privacy, data security, and identity theft, particularly involving children and seniors, would continue as areas of focus for the agency. So it's very appropriate that she get us started here today. And now, Chairwoman Ramirez.

EDITH RAMIREZ: Thank you, Mark. It really is a pleasure for me to be here with all of you. And I really do want to tell you that I really appreciate welcoming all of our partners from federal and state agencies, private industry, legal services, and other nonprofit organizations.

As Mark mentioned, today we are focusing on one of the most prevalent types of fraud that affect seniors-- identity theft.

I'd like all of you to consider the following scenarios. A 75-year-old retired teacher receives an IRS notice that he owes taxes on income that he earned working at a restaurant in Texas.

In fact, he never worked in a restaurant. In fact, he never even set foot in Texas.

A 65-year-old woman uses her laptop to store all of her electronic health records. The laptop is stolen and the thief uses her health insurance information to pay for his own medical services.

A 95-year-old woman with Alzheimer's disease lives in a nursing home. Someone at the home takes her purse, and then uses her credit cards to make unauthorized purchases.

Unfortunately, as we all know, these disturbing stories are all too common. Many seniors spend lifetimes building credit and saving money for their golden years, but then identity thieves steal their hard-earned savings or ruin their good reputations.

Our goal today is to explore potential solutions to this problem. So we're going to be asking the following questions-- how can we ensure that the people in businesses we trust with seniors' personal information, like tax preparers, hospitals, and nursing homes, do a better job of protecting it? What should seniors and their loved ones do when they discover they have become victims of identity theft? And what is the best way to reach and educate seniors on this issue?

Today's forum will include panels on different types of senior identity theft, specifically those involving tax and governmental benefits, health care, and long-term care. And we're also going to explore the best consumer education and outreach techniques for reaching seniors.

We're very fortunate today to have gathered together the best and brightest minds on these subjects. And I'm confident that we're going to be working together to develop better solutions.

But before we talk about possibilities for future action, I'd like to say a few words about the most effective strategies that the FTC has used in the past.

At the FTC, we employ a multi-pronged approach to combating identity theft-- consumer education and outreach, law enforcement, and complaint tracking and analysis. I'll start with education and research.

At the FTC, we've longed believed that an ounce of prevention is worth a pound of cure. So we have an extensive program for educating and empowering consumers, both on how to protect themselves from ID theft and how to mitigate the consequences of being victimized.

The FTC has published a wide variety of educational materials on this issue. For instance, we created a victim recovery guide called Taking Charge: Fighting Back Against Identity Theft, which provides a practical guide on what to do if your identity has been stolen.

We've distributed over 5.4 million copies of this guide and have recorded over 4.3 million visits to the online version.

The FTC also partners with local state and federal organizations to distribute our materials. With our partners, which include the American Bar Association, we created a guide for pro bono attorneys on how to advise and assist identity theft victims. And using that guide, we've trained hundreds of legal services attorneys and victim assistance advocates.

The FTC and our partners have also conducted 44 identity theft seminars for more than 5,700 law enforcement officers for more than 1,900 different agencies. And as part of our outreach mission, we also provide targeted educational assistance to victims of particular breaches.

For example, our attorneys recently participated in an AARP interactive tele-town hall on ID theft in South Carolina to help potential victims of a major security breach of millions of social security numbers and tax records.

Let me also say a few words about law enforcement. By suing companies that fail to maintain reasonable security measures, we work to prevent identity thieves from getting consumer-sensitive information in the first place.

Since 2001, the Commission has brought over 40 cases against businesses that we allege failed to reasonably protect sensitive consumer information. In one egregious example, we reached settlements with two pharmacy chains, CVS Caremark and Rite Aid, for their alleged failure to protect sensitive financial and medical information collected from customers and employees.

Among other things, we alleged that these companies employment records and pharmacy labels were left in open trash dumpsters. And our settlements with the two companies required them to establish comprehensive information security programs.

In support of these law enforcement efforts and consumer education programs, the Commission uses a third tool to help combat identity theft-- complaint tracking and analysis. As most of you

know, the FTC operates a consumer hotline and website where we receive thousands of complaints each day directly from consumers. We then input this information into our Consumer Sentinel Database, which combines complaint data from multiple sources.

The Sentinel database gives us insight as to where we and our partners should focus our efforts. For example, although seniors are not necessarily victimized more than the rest of the population, the most common complaint we receive from them is ID theft. And those complaints appear to be increasing.

Further, our complaint database reveals that ID theft is prevalent in states and metropolitan areas with high numbers of retirees. This type of data is crucial for helping us target the problem.

In short, ID thieves pose an unfortunate but very real threat to older Americans. And your efforts, as public servants, consumer advocates, and private sector partners are what make the difference in helping to prevent potentially vulnerable seniors from becoming victims.

Thank you for taking the time out of your schedules to attend today's workshop.

And I'd also like to take a moment to thank Steven Toporoff, Lisa Schifferle, Megan Cox, Cheryl Thomas, and Jennifer Leach for organizing today's event. I look forward to working with all of you to implement the ideas and innovations that we hope will result from today's gathering. Thank you very much.

STEVEN TOPOROFF: So we're going to begin in a minute with our first panel, but I want to thank Chairwoman Ramirez for her opening remarks, and really setting the tone for what today is all about.

While everybody is getting ready, I'd like to put the first panel into context. We OK?

CHRISTOPHER LEE: Sure.

STEVEN TOPOROFF: So to put the first panel into context. And we're going to be talking about tax and government benefits identity theft.

So tax and benefit identity theft typically involves the misuse of social security numbers, financial information, and other personal information in order to obtain a tax refund or government benefits such as social security payments or workers' compensation.

And I'll give you a few examples of how this may happen. First, there could be a phony tax preparer who steals clients' social security numbers and other personal information and gives it to criminal gangs, who then, in turn, either use it themselves or sell it to others in order to get tax refunds.

Identity thieves may also comb obituaries or the government's listing of deceased individuals called the Death Master File to identify people who have recently passed away in order to, again, file a tax refund in their name.

We're also aware of instances where employees at medical offices or hospitals gain access to patient files, including social security numbers, medicare numbers, which typically are social security numbers, and other information, again, to file either for tax refunds. Or again, social security payments or some other kind of government benefit.

Commissioner Ramirez mentioned the Sentinel Database. That's the database of complaints that we have at the Commission. And the government fraud or government identity theft component of that database is the largest of the different categories that we have.

So for example, in 2010, government type of identity theft, government benefit identity theft, comprised just less than 20% of the total of the identity theft complaints that we received.

In 2011, that went up to 27%. And most recently, it hit 46%, close to 47%. So the complaint data that we get shows that this is a growing problem.

And not surprisingly, Florida, where we have a lot of seniors and retirees, is the number one state for this kind of problem. Losses from identity theft, involving taxes, in particular, total about a billion dollars annually. And losses in South Florida, in particular, are estimated to be at least $100 million annually.

So to address this problem, and we'll hear more from the IRS in a second, the IRS has instituted a number of fixes, including filters to better handle tax returns that are filed. The IRS and Justice Department have worked and are continuing to work on criminal prosecutions of identity thieves. And so in this panel, we're going to discuss the scope of the problem and some of the solutions.

And I want to introduce, very quickly, our panelists. To my left is Amber Smith from the IRS. Then we have Christopher Lee from the IRS Office of Taxpayer Advocate Service, David Lindner from Social Security Administration, Susan Morgenstern from Legal Aid Society of Cleveland. Bob Kerr is from the National Association of Enrolled Agents, and John Morton is from Green Dot Corporation.

I want to welcome all of them here. And more information about them is available in the bios that you have in the packet of information that you were given when you signed in earlier. So I want to begin by discussing the scope of the problem specifically.

And that is, how big of a problem is this? And what are the different agencies finding?

So I'm going to start with Chris Lee from Taxpayer Advocate Service. Chris, in your work in that division, what are you seeing as far as how prevalent might tax identity theft be? And in particular, as it may impact seniors?

CHRISTOPHER LEE: Thank you, Steve. Just to begin, I wanted to explain what my organization does. I'm with the Taxpayer Advocate Service. We're an independent organization within the IRS that helps taxpayers resolve problems with the IRS.

We serve kind of as a backstop. So if the IRS is not able to resolve the taxpayer issues timely or as intended, then we can step in and try to achieve resolution more quickly than the IRS would have otherwise.

We're headed by the National Taxpayer Advocate who's in DC. She reports to the Commissioner. And we have at least one office in each state and in Puerto Rico.

So we help taxpayers, again, that have not been able to resolve their identity theft issues with the IRS. Or, they have an economic-- they're about to suffer economic hardship and they're able to come to us.

We've been working on ID theft with the IRS for as long as I've been with TAS-- since 2004. And each year, we've noticed that our ID theft cases have been rising pretty significantly since 2008.

From 2008 to 2012, our ID theft inventory has risen 666%. From 2011 to 2012, the last full fiscal year, our ID theft caseload has increased 61%. So it's still growing pretty quickly. Or sorry, pretty significantly.

And through March of this year, our caseload has increased another 60% from the same time last year. So we understand the IRS is doing a lot of things to both prevent ID theft and also to better assist the victims of ID theft. But I think the sheer volume of incidents makes it difficult for the IRS to do so.

That's the impact that we're seeing in our office. About 25% of our cases now are ID theft-related. So we have a vested interest in working with the IRS to improve processes.

TIGTA, the Treasury Inspector General for Tax Administration, they've done a number of-- they've issues a number of reports on ID theft. And the latest one, I believe, scoped out the problem. And they estimated that there were 940,000 ID theft incidents last year, which led to $6.5 billion in fraudulent refunds being issued. So it's definitely costing the government money. It's causing taxpayers additional burden because they're not able to receive their refunds timely.

And also, it impacts other aspects of their lives outside of the tax system, like government benefits they may receive or eligibility for other programs. So I can safely say that it's a problem that's already large and seems to be getting more and more significant.

STEVEN TOPOROFF: Thanks, Chris.

Amber, from your perspective at the IRS, again, how would you describe the scope of the problem?

AMBER SMITH: Thanks. Well, I think Chris has done a very good job of laying out the picture for you that we're faced with at the IRS.

I've been with the Office of Privacy and Information Protection since 2008. And I can see just by the way our office has grown, certainly that we've had to dedicate significant resources to this problem. It grows tremendously every year.

Fortunately, we're getting better at identifying identity theft before money goes out the door. It's something that we're very committed to doing. I don't want to get too hung up on numbers, but just to give you an idea of the sort of growth we're seeing--

In 2012, we protected $20 billion of revenue related to fraudulent returns. Actually, over $20 billion in revenue. And what that means is that's money that would have gone out the door. Money that would have gone into the hands of fraudsters, many of whom are identity thieves. A lot of this revenue was related to identity theft. And we were able to protect that revenue.

That's up from $14 billion in 2011. So considerable growth. So what that represents, of course, is an uptick in the amount of fraud that we're seeing and the amount of identity theft that we're seeing.

Fortunately, it also represents that our ability to stop money from going out the door and to make sure that refunds are going into the proper hands, the people who should actually be getting them, is improving all the time.

We are dedicating significant resources. And again, indicative of the growth of this problem, we now have over 3,000 employees working identity theft cases at the IRS. That's a huge rise over the past few years. And this is a trend, of course, that we probably do not see stopping anytime soon.

In terms of the types of identity theft cases that we're seeing-- I know we're going to get into specifics a little bit more later. But just to give you all an idea, I mean this is-- we find through the victims that we help, that the case analyses, the information that we gather through our partnerships with states and with advocacy organizations that this is just such a widespread problem. There's really nobody who's exempt from being affected by identity theft.

So when we're talking about scope, that's certainly something that we pay attention to. And it presents, of course, a special challenge for us because the way we process returns, the way we ensure people get their refunds, within our systems it's very complicated. So we're looking at primary taxpayers. We're looking at identity theft related to children, deceased individuals, now businesses. So clearly, a multifaceted issue, very widespread, and one that we're committed to addressing.

STEVEN TOPOROFF: I'm going to turn to Susan Morgenstern, who's with legal services in Cleveland. But she's on the ground. She has been helping victims of tax issues and tax identity Theft. So Susan, what kind of problems are you seeing specifically when it comes to seniors and tax identity theft issues?

SUSAN MORGENSTERN: These cases never come in as a client identifying, I think I'm the victim of identity theft, could you please help me solve my identity theft problem? They generally come in because there's a downstream consequence.

One case I just closed, for instance, involved a woman who was receiving what looked like court summonses from a payday lender. And she had taken out payday loans to pay the tax debt, who genesis it turned out, was identity theft. Somebody had used her social security number to file tax returns. It generated balances due eventually because these returns were examined by the IRS. They then, because the liabilities were associated with my client's social security number, the liabilities followed her. She started getting these notices. She was terrified. She thought she had to pay. These notices say, you have to pay the IRS. And so being the dutiful citizen that she was, she tried to figure out how to pay the IRS.

This woman had some mental cognition issues. She lived in a nursing home. These debts arose when she lived in Georgia. And whether she fully understood what was going on or not, to this day I don't know. But what I do know was we got the payday lender off her back, and we unraveled the identity theft so that the consequence to her public benefits, which were the social security retirement benefits, was undone. And we were able to secure some refunds for her.

So financially, she ends up in a better place because of it. But you have to think about the consequences to her emotionally of having gone through this identity theft, of living alone in a nursing home environment and not really having anybody to turn to or persons that she could trust. She had a caretaker come in. She starts looking at this caretaker, can I trust this person?

We've had other nursing home cases where before going to a nursing home, the person has sort of no issues on their social security number. They come out of the nursing home and all of a sudden there are issues on their social security number. They find their number has been used.

Those are very hard cases. Because again, you're dealing not only with the restoration of their benefits, but you're also dealing with these trust issues. What does it mean to trust a caretaker. Can you trust a caretaker?

The other downstream consequence we see is, as I said earlier, the reduction of benefits. So people come in to see our social security attorneys because their social security is being reduced or because their food stamps are being reduced. Or they're having a community Medicaid issue and so they're losing Medicaid benefits. Because all of a sudden, there's income that's being imputed to them that's not theirs.

So for me, as the tax attorney, it can take me up to a year to unravel these cases. And it's a long year for my clients and it requires them to be steadfast in paying attention to me and helping with their case. But often, there's this fear of, well, they took my social security number. What are they going to take next? And that's really the hardest part of these cases.

STEVEN TOPOROFF: Thank Susan. I want to turn to Bob Kerr. We're very fortunate to have Bob today. He is with the National Association of Enrolled Agents. Typically, at the Federal Trade Commission when we do outreach and law enforcement, we tend to deal with analysts and

lawyers. But bob is an accountant. And it might be interesting for me, in particular, to learn from an accountant's perspective and from that industry's perspective, what are they seeing in terms of their clients, their older clients, and tax identity theft issues? So Bob.

ROBERT KERR: Thank you for the flowery introduction, I appreciate that.

Enrolled agents are tax experts who are licensed by IRS. And so that's the enrolled agent's niche in the tax universe.

The question you ask is, well, what kind of identity theft are we seeing? And I typically start this by saying there are a million tales in the naked city. This is but one of them. They're all different, but I just pulled one because I thought it might be interesting.

From earlier this year, a long-time married couple, mid/late 70s. The husband passes away at the end of January. The return, because they're a fairly high net worth couple is complicated and they never file until the end of the filing season. So widow files on April 15. The return rejects. They try again, return rejects again with the ID theft reject code on it from IRS.

So the enrolled agent goes and calls IRS. And as it turns out, the other return was filed early in the year and was in IRS parlance unpostable. IRS didn't process it because the husband's social security number was used with another man to file a return, which IRS thought was a little suspicious amongst many other problems with the return.

Widow has to file the form 14039, which, yes-- thank you, Susan. Here. The identity theft affidavit. And is in the position-- well, a number of unpleasant positions. One of which is her husband of many, many, many years just died. Number two, all she's trying to do is file the married filing joint return for last year, which she can't do. She owes $10,000, which she wants to pay and prevent IRS from donning her for penalties and interest. And so this is one flavor of what we see, although these stories change all the time.

STEVEN TOPOROFF: Another way that some seniors are experiencing tax identity theft is through the use of downloadable debit cards or prepaid debit cards. And we have John Morton from Green Dot Corporation, which is one of the major suppliers of prepaid debit cards. John, in your practice, as part of Green Dot Corporation, I'm sure you must see or hear about instances of misuse of the prepaid cards. What kind of problems are you seeing in your work, in particular as it may pertain to senior citizens?

JOHN MORTON: Well, Green Dot Corporation-- let me start to put some context around this-- is a bank holding company. We're a financial services company, no different than any other bank in the land.

The individuals perpetrating this fraud, their ultimate goal is to get the funds. And in order to do that, in all likelihood, those funds are going to have to pass through the banking system and financial institutions. And so we on the back end, as a banking institution, do see some of these fraudulent proceeds process through our products.

In the case of Green Dot Corporation, the majority of our products are prepaid cards that you can either acquire online or you can acquire in any one of 60,000 retail locations. So typically, what we see from our end is just kind of the back end of what's already been described up here.

We see an individual that is activating or applying for a prepaid debit card. The activation process is no different than what you'd go through if you were opening up a bank account online from your nearest bank. We're going to ask for your name, address, social security number, date of birth, phone number, all the Patriot Act required elements. And we're going to verify that. But these individuals have stolen your identity, so unfortunately they have access to all of that information.

They open up the prepaid card. And then, with the prepaid card, just like with your checking account that we probably all have, they can designate that account as a receiving account for direct deposits, either in the form of a tax refund coming from the IRS or a federal benefits payments, something coming from social security or VA. And so after they've opened up the prepaid card, they're filing the fraudulent tax return and/or contacting the federal benefits agency and rerouting the federal benefit. And so we see these fraudulent funds flow onto the card.

And then, they're as quick as possible, the good ones at, least, visiting the nearest ATM, doing cash back at the point of sale, and trying to get the cash off the card as quickly as possible. So we're seeing both the activation or the application and the opening of a fraudulent account, and then the fraudulent proceeds flow through to-- in some cases, to our products.

It's a small percentage, but it is something we're very concerned about. We've been working with the industry, law enforcement, the IRS, treasury, et cetera, and dealing with this problem for, really, the last three or four years.

STEVEN TOPOROFF: Thanks, John. I want to turn to David Lindner, who's with the Social Security Administration. We've been talking primarily about tax refund identity theft. But as I mentioned, it could also be other kinds of benefits as well. So David, could you fill us in about what you're seeing at the Social Security Administration in terms of identity theft involving seniors' benefits?

DAVID LINDNER: ROBERT KERR: Yeah. Thank you.

Well, we really feel like it's hard to quantify the whole scope of the government benefit identity theft issue that we're facing at the moment. SSA's Office of Inspector General, they investigate allegations of fraud, waste, and abuse in our programs. And a big part of that is the SSN misuse.

Some people label it as identity theft. We label it more as an SSN misuse in how it works for our programs. Because the SSN is obviously vital to how we administer our programs.

And just some numbers to throw out there, in fiscal year 2012, 8,000-some cases were opened by our OIG. And only about 3.51% were SSN misuse-related. Those are just some numbers. So I mean, it's obviously an issue. However, it's only about 3% that we've seen in the past fiscal year having to do with government benefits themselves.

One particular problem, however, is that we're seeing a lot of the redirection of benefits from direct deposit accounts. Criminals and identity thieves are able to gain so much personal information from various sources, whether it's social engineering tactics where they have telemarketing and lottery schemes, where they'll call up a senior and say, look, you've just won millions of dollars. And they get really excited and they say, well, what do I have to do? And they say, well, just to get the process rolling, if you could just send us a little bit of money up front. And then if you give us your social security number and your bank account information, we can just have it all sent right into your bank account. And you don't have to do anything.

And so they go for it. Many individuals have gone for it and it's cost them greatly.

As soon as they get enough information, they can go to the beneficiary's financial institution and switch over the direct deposit information and reroute it to a fraudulent bank account where they can collect the funds.

And another issue we have is something call lead lists, which are lists that are found on the internet, commonly found in forums, things like that where identity thieves just post lists of information. Could be names, dates of birth, SSNs, addresses, credit card numbers of all these different individuals. It's almost like it's being put out there for you to play with. It's the information they've been able to gather. And you can go out and try and do some of your own malicious acts by doing things such as redirecting payments from the direct deposit. Or, obviously, you can do much worse if you have complete access to someone's bank account.

So clearly, we think that the amount of PII that individuals-- or Personal Identifiable Information, sorry for the acronym. But the amount of personal information that's out there in the public, wherever it is-- it's Facebook, it's Twitter, it's all these different things. And that's not just in a senior sense, but I just mean in general for anyone, there's so much information out there that people can gather on you without you knowing it.

Pictures of your house. They know where you address is all of a sudden if you put it up on Facebook. And it doesn't take too much more. They can answer these security questions and get to your SSN. And really, that's where you're going to see your social security benefit frauds the most for seniors.

STEVEN TOPOROFF: Thanks. One of the issues that comes up periodically at the Commission is the issue of the Death Master File. And I hinted at that before, and that's the government's official listing of deceased individuals. And it's my understanding that what some thieves do is they comb obituaries or have access to the Death Master File and they quickly try to file a tax return in the hopes of getting a tax refund for that deceased individual. Because there may be a gap in time before IRS and others know that this person or that social security number associated with that person has-- that person, in fact is deceased.

So Chris Lee, what is your position about some of the issues involving the Death Master File? Do you have any recommendations? I mean, what would you like to see in terms of protecting it so that deceased individuals-- again, their information isn't compromised?

CHRISTOPHER LEE: Yeah, sure. The Death Master File, as you may have mentioned, it's a database maintained by the Social Security Administration. And it contains the full name, social security number, date of birth, date of death, and the county, state, and zip code of the last address of record, which is all good information to have if you're an identity thief and want to file a fraudulent refund.

We've seen some fraudsters use the Death Master File information to file fraudulent returns. And these deceased individuals are, in some ways, the best victim because the objective of these identity thieves are to file a refund claim before the legitimate taxpayer. And if the legitimate taxpayer is dead, they don't have to worry about a second return being filed and the victim being notified that their SSN has been compromised.

So young children and elderly are also good victims because if these taxpayers don't ever file, then the chance of them being discovered is not as good as a taxpayer with the filing requirement.

So we've seen reports in the news of, say, some parents that have lost their infant child to sudden-- to death. And next thing they know, they file their return. They file their final return with claiming their deceased child and come to find out that someone has been using their child's social security number to file a return. And so it's an additional emotional turmoil that they've had to face.

And while I don't think Death Master File misuse is all that prevalent, it is something that we should be able to stop and it doesn't really make sense for one arm of the government to kind of arm the identity thieves with information that is harming another part of the government.

The National Taxpayer Advocate has made a number of recommendations. In her 2011 report to Congress, she recommended that Congress limit access to Death Master File information in one of two ways. One is limiting the release of the information until after three years of the date of death.

Taxpayers that are deceased have a filing requirement. Their state needs to file and if they have a surviving spouse that wishes to file as a surviving widow, then it needs to be open for at least a couple years. But after three years, there's really no legitimate reason for the SSN to be active in the system. So we've also recommended that the IRS retire the number after three years, which I believe the IRS is doing now.

But during that three-year gap, we recommend that the Death Master File information be released to companies and institutions that have a legitimate need. And I think there's been a couple of bills proposed in Congress that kind of make the same recommendations that the National Taxpayer Advocate has argued for.

Again, it's not something that's quite all that prevalent, but it seems to be low-hanging fruit that we should be able to close this loophole.

STEVEN TOPOROFF: Amber, any thoughts on the Death Master File from the IRS's perspective?

AMBER SMITH: Absolutely. So this is clearly an area where I think we all stand together. And the IRS has been working with SSA as well on proposed legislation. As Chris mentioned, there are a couple of bills in Congress right now that would limit the availability of that information.

The trouble there is that there are valid uses for this information. So I think that at least two of the bills would have the Secretary of Commerce establishing a certification program, so that entities that have a real need for that access would be able to come in through this program and become certified to obtain it.

I think right now we're in a tough position because we are relying on-- and when I say we, I mean all of us. We are relying on private businesses to do the right thing. And in some cases, they are, which is fantastic. I think we had ancestry.com, which a lot of people use for genealogy research had been routinely releasing this information and they stopped. So that's great, cutting off the flow at least in one area. But we would really like to see that the availability of that information certainly limited.

We see a lot of identity theft. And again, growing using the information of deceased individuals. Presumably-- and it's incredibly sad because you see the high-profile news reports of tragedies, and then you see returns coming in using the information of these people. And what you have is a situation where their loved ones are being victimized over and over and over again. So the way that we've been dealing with that, and Chris referred to this, is by making that information unavailable for use. Making those numbers unavailable for use after a certain period of time.

Obviously, it has to be kept open so that final returns can be filed. But one thing that we do now is we are locking accounts as soon as the final return comes in. So that will prevent parents' children from being victimized again in subsequent years by the use of their loved one's information and having to deal with those sorts of hassles. Once the final return's in, the information can't be used any longer.

But again, limiting the availability of that information would certainly go a long way to stopping that.

STEVEN TOPOROFF: Thanks. David, any thoughts from the Social Security Administration's perspective?

DAVID LINDNER: I mean, we obviously agree that there are things that can get better. Just as a background, SSA receives approximately two and a half million death reports each year, coming from funeral homes, to family members, to state agencies, federal agencies, you name it-- financial institutions. And we need this information to administer our programs.

We need to make sure that when somebody's deceased, that we're able to take that beneficiary off our roles. And then it also alerts us to, say, if that beneficiary had a surviving spouse and children, that we need to be able, if they qualify, to provide them with the benefits that they

deserve. So that's really why it's so important to make sure that these death records are correct from a program purpose for SSA.

It basically came to be, as Chris was saying, there was a FOIA lawsuit in 1978. Freedom of Information Act, in case anybody doesn't know what FOIA is, lawsuit. And basically, as a part of the settlement in that lawsuit, SSA agreed to release the last name, SSN, and date of death for any individuals they had in their death records. And release them to the public because under the Privacy Act, we generally treat deceased individuals as if they have no privacy rights except for a few exceptions. And we then provide the Death Master File to the Department of Commerce's National Technical Information Service, who then sends it out to other government agencies and private companies that use it themselves to verify deaths and to hopefully prevent fraud themselves.

So the idea of it is really to prevent fraud in the first place, which is what makes it somewhat ironic. There's been other instances that have come up regarding erroneously placing a living person on the Death Master File, either something was reported wrong to SSA. There's a number of ways that this could have happened. Obviously, don't want it to ever happen. But unfortunately, there's been instances where that has occurred. And that can be a real pain for somebody that's trying to live their life and they're showing up on the Death Master File.

So we do contract with ID Analytics, which is a leading identity risk management firm. And they review all these cases of any living persons that were ever put on the DMF. And they look for things like account openings, account changes, account closures, anything that could be a symbol of identity fraud or theft.

We usually review these quarterly for a period about three years because we like to keep track of these individuals for extended period of time. And so far, based on what ID Analytics has came to us with, they've not identified any patterns of misuse from the SSN, from the Death Master File, from somebody that was placed on the Death Master File who was still living.

But of course, if they were to come to us and find these patterns of misuse for these individuals, we would properly notify them and offer credit monitoring and anything else we can try and do to resolve the issues as quick as possible.

STEVEN TOPOROFF: Thanks. One of the issues that comes up all the time at the Federal Trade Commission is people call us and will ask us when it comes to tax issues or government benefits issues, well, what do I do? How can I avoid the problem?

And it's a difficult one because a lot of times you're not necessarily in the position of control. If somebody steals your social security number or a senior's social security number because they have access to files at, let's say, a hospital or a doctor's office. There's not much that you can tell the senior on what they can do.

But what we sometimes recommend, certainly is that seniors-- anybody for that matter-- try to file early. Don't put your tax return in the mailbox, like your mailbox outside on the street with the little red handle. Go to the post office and place it in there where it's more secure.

But are there other measures that seniors can take? In particular, some of the questions that we have gotten are, can you adjust withholdings to avoid having to pay taxes in the first place? Are there other procedures within the accounting system that seniors might be able to take advantage of in order to limit the risk of identity theft?

So I'd like to start with Bob, our accountant here. Are there procedures within the preparation of taxes, the tax code, from your perspective, that might enable seniors to somewhat limit their risk of being identity theft victims?

ROBERT KERR: I think there are certain things that folks can do to help prevent problems. But let's sort of scoop it up high first to start on this.

One of the things that we see is that phishing, P-H-I-S-H-I-N-G, is a real problem. It's a really cheap way for fraudsters to go out and hit a gazillion plus or minus email accounts.

And these efforts are in varying degrees of sophistication. Some of them are really amateurish. Some of them are really not bad. You need to keep in mind a couple of fundamentals.

IRS doesn't ask for taxpayer information by email. IRS doesn't have any address that says @rocketmail.com. So don't fall for that one. IRS doesn't make outgoing calls asking for PII, period.

So if any of those happen, then you can put down the phone because it's not IRS. So those are sort of common sense issues. And particularly in this day and age, when everyone has email accounts it's not an age-specific thing. But I think that, perhaps, seniors might be a little more vulnerable and may, perhaps, a little less skeptical of something coming in with an IRS eagle on it. Oh, it looks official. So that's my high-level observation.

STEVEN TOPOROFF: Susan, any thoughts from your practice on steps that seniors might be able to take to minimize the risk?

SUSAN MORGENSTERN: I would start by urging, and I do urge my clients to work through a trusted return preparer if they need to file a return. And the question is really, do they need to file the return?

Often, our clients don't have a filing requirement because their incomes are so low and that makes them especially vulnerable to identity theft. But in the event that they do have a filing requirement, we urge them to file through a VITA site or a tax counseling for the elderly AARP site.

They get those same phone calls that other panelists have been discussing with regard to sharing information. All of the communication that goes out, if you initiate the phone call, then maybe you could share your social. But if somebody calls you and says, well, by the way, what's your bank and social information? Don't share it. And we can say it time and time again and clients are still resistant to that. They think, well, this is a friendly conversation. I'll just share that information.

We urge them to order their credit reports. They're allowed the three free credit reports per year. Every client of mine walks out with that information, even if they're not an identity theft client. It's a free service. Why not take advantage of it, find out what's going on with your credit report?

And the fourth thing, and it seems sort of silly to say it, but it's not really. And that is open your mail. A lot of our clients come in with these-- by the time their problem is big enough that they need to see an attorney, they have those plastic bags, those blue crinkly plastic bags loaded with letters that they haven't opened from IRS or from other creditors. And the problem could have been averted altogether or maybe stopped in its tracks much sooner had they opened their mail.

I always say to my clients, even if you're afraid to open your mail, bring me your mail and we'll open it together. I give them self-addressed stamped envelopes. I can't stress enough how serious this is, especially with the elderly clients. They just don't-- they can't read it. The language is incomprehensible. The type is small. And it's maybe sort of one of those fake letters, but it looks official and they just don't want to open it.

An example is when the IRS files a lien, these creepy companies come out and start sending notices to the taxpayer saying, well, we can help you? They send out documents that look like official IRS letters or that look like government letters. And the clients come in with these letters and their hands are trembling and they'll say, well, now they want all my money, or now they want my house, or now they want this or that. And it's so important to explain to clients that you have to open mail and you have to figure out, is this legitimate mail or not?

STEVEN TOPOROFF: One question that we get is the paper or electronic filing question. And that is, which is safer, in particular, for seniors? Is it better to file in paper? Is that more secure? Or electronically? And I suppose that there are advantages and disadvantages with each.

Susan, do you have any sense from working with your clients? Do you advise them one way or the other, paper or electronic filing?

SUSAN MORGENSTERN: It's a really hard question to answer because I am the first one to rail against electronic filing. I think electronic filing as a general concept, helps to facilitate identity theft. You can file a return from the privacy of your bedroom at 3 o'clock in the morning and nobody knows whose social security number you're using to file that return. And in that regard, I think the issue is, what safeguards do you use with electronic filing to make sure the electronic filing process is safer?

In some instances, I do advise my clients to file electronically. It's a way to find out really early in the system whether your return is going to be rejected because your number's already been used. And clients who wait-- the example of the elderly couple that waited-- will find out that they can't file electronically on April 15 and will need to paper file at that point.

If you're in a hurry for a refund, electronic filing will facilitate-- hopefully, will facilitate the return of the refund pretty quickly.

So I'm not coming down either way on that question, Steve. Only because I think there's so many hazards in the electronic filing process itself.

STEVEN TOPOROFF: Bob, any thoughts? Paper? Electronic?

ROBERT KERR: I've learned that the answer to nearly every tax question under the sun is it depends. And so the answer to this tax question is it depends. As Susan was saying earlier, I think there's some real advantage, and certainly no disadvantage, to filing early. You file early electronically. The IRS either accepts or rejects your return. That's a data point there that's particularly useful, A. And B, the earlier you file, the smaller the window is for someone else to claim your identity and file for you.

So in the main, I think filing earlier is better than filing later. Some people can't. The example that I used to start, they had a significant amount of dividends and they had to wait until later in the year in order to get all the 1099 docs to do the filing. So that wasn't going to work for them.

And I don't want people to leave this-- certainly, seniors leave this to be stress. Because oh my gosh, I have these things that are going to keep me from filing until later and I'm doomed. That's not the case. But I think there's some merit to filing earlier rather than later.

Then e-file versus paper. I think one of the things that we keep in mind, from my perspective, is that recent law requires paid preparers to file electronically. And that taxpayers have the ability to opt out, but it has to be a client affirmative. So client has to request to the enrolled agent, I don't want to file electronically. Otherwise, by default, we're going to file electronically because we're required to.

From my personal perspective, I don't think that electronic filing in and of itself is any more hazardous than putting it on a piece of paper. And Steve, you yourself said earlier it's one of the common sense things. If you live out-- I'm from Ohio and I have friends in rural areas. If your address is RD 2 and you're going to take it out to the end of the lane and put it in the mailbox and put the little red flag up, that's probably a bad idea.

If you're going to take it to Union Station here and drop it in the mailbox, that should be just fine.

STEVEN TOPOROFF: Amber, any thoughts on paper versus electronic from the IRS's perspective?

AMBER SMITH: I think it's been pretty well covered. I mean, obviously we're proponents of e-file, recognizing that the information is encrypted in transmission. It makes it safer, again, than dropping it in the mailbox.

And quite honestly, the earliness of filing where possible can't be stressed enough. I mean, the identity thieves, they're filing early. So as much as you can limit that window, and e-file certainly does help to facilitate that.

STEVEN TOPOROFF: Thanks. Want to move to an area that I touched on when I presented the context in which this arises. And that's the issue of tax preparers and trusted tax preparers. And my understanding is that there's been a case recently, Loving v. IRS. And it's not the loving that everybody's familiar with having to do with marriage, this is a different loving where the court basically threw out the IRS's program to regulate non-attorney, non-CPA tax preparers.

Did I get that right? OK.

So that kind of leaves a gap, especially when it comes to seniors. It is now more difficult, assuming that that court's decision stays. It is more difficult for the IRS to control who tax preparers are. And we, at the Federal Trade Commission, know from our work with Justice Department and others, that there are cases of phony tax preparer services. Either where the tax preparer just hangs out a shingle with the sole purpose of collecting social security numbers and other information or they're a legitimate tax preparer but may do some funny business to either inflate numbers so that the tax return seems to have a larger refund attached to it where they may pocket the difference and give the victim what the true amount would be. So this is a real tough issue.

So in light of the Loving case, what best advice do we have for seniors on how to find a good tax preparation service If they choose to need-- if they need one and they choose to follow that? Amber, any thoughts on that?

AMBER SMITH: Well, I would actually defer, probably to Susan on this. Not to put you on the spot, but I suspect you have some opinions about this.

ROBERT KERR: And IRS probably doesn't really want to make the public opinion on Loving either.

AMBER SMITH: Probably not.

STEVEN TOPOROFF: Fair enough.

ROBERT KERR: But Susan, I'm sure would be pleased-- are you?

SUSAN MORGENSTERN: I mean, I have opinions about everything.

ROBERT KERR: And I do as well. Let's, again, scope up high on Loving. The DC Circuit Court decided in favor of Ms. Loving and her co-plaintiffs. The case is in appeal.

My opinion is that IRS is going to prevail on appeal. So this is the delay in IRS executing what we consider to be a thoughtful and deliberate oversight program in order to bring into the fold hundreds of thousands of return preparers of varying degrees of competence. It sort of sets a floor of return preparers who hire out their services to demonstrate a minimal competency. You have to pass a basic test. And then, you have to take continuing education every year because the tax law changes so much.

If you pass a tax test 10 years ago, you're lost today. If you pass a test a year ago, you could be lost today, but that's a separate issue just because of the tax code being so complicated. So what's in disagreement right now is whether IRS can require folks to be minimally competent, and whether IRS can require folks to take continuing education.

I'd say, Steve, on that one, just to sort of stay tuned. Because ultimately, I think IRS prevails. And we'll see this within the next several months.

STEVEN TOPOROFF: But in the meantime, if somebody comes to one of the panelists and wants to know what's the best way to find a trusted tax preparer, what is the best advice that we can provide to consumers?

ROBERT KERR: I mean, there's some fundamentals you can do. IRS prints an annual 10 tips, which I think is a decent place to start. Ask for qualifications. Is the person an enrolled agent, like my folks? Is the person a CPA or an attorney? Does the person do VITA or TCE work as well at the other side here? Because such folks have what I consider skin in the game.

My enrolled agents and CPAs and attorneys are licensed. And they're at risk. And I'll let Susan speak to background on her folks, but I think they're bringing a similar back pattern with them that make them trustworthy as well.

I think people need to keep in mind the eternal truth of the statement that if something looks too good to be true, it is too good to be true. And so don't accept promises of big refunds. Come on down to my place. We'll just do it at the kitchen table. We'll have some coffee. And we'll just plug in some numbers on this return I've gotten by TurboTax and I do this for everyone in the neighborhood. That is a problem. If something smells bad, it probably is bad. So sort of common sense still plays a part.

One of the other things that we always stress is that if someone should be proud enough to charge for a return that person should be proud enough to sign it. So don't accept a return from someone who's not going to sign it and put on his or her PTIN, a Personal Tax Identification Number.

And finally, never sign a blank return. Always review a return before you sign it.

STEVEN TOPOROFF: Susan, did you want to add to that?

SUSAN MORGENSTERN: Well, our clients don't pay to have their returns done. They don't go to an enrolled agent. So we-- I guess this is about eight years ago now, seven or eight years ago, formed a coalition of community agencies in my county, which has now spread across Northern Ohio, to provide free tax return preparation year-round to our clientele. And this is both VITA and we also refer to the AARP tax counseling for the elderly sites.

They get quality returns done. What we've done is worked with those preparers so that if there's an issue on the return, the VITA sites can call us and say there's something not right going on. If the return's been rejected, the client will be advised to seek assistance from legal aid, hopefully.

The other thing that happens during filing season is the role of affinity groups. And what happens here is you're at church or you're playing cards or something, you're hanging out with your friends, and they say, oh, well, if you give me your information, I can help. It's an abuse of a friendship. If you give me your information, I can give you the name of somebody who can help you file a return. And so there's no face connection between the taxpayer and the return preparer.

We've seen horrible identity theft cases in that way. And in those situations, the lesson is learned too late. And you can't really sit there and chastise your client for not using common sense. But in the end, that's what it comes down to, as Bob was saying, is common sense. You need to look at the preparer. You need to understand what's going on. Your return ultimately-- it's your signature or your authorized signature in the event that you're filing electronically.

STEVEN TOPOROFF: Thanks.

ROBERT KERR: And if I can just add one more piece? I think that in the situation of folks who are older, I think you want-- for your parents, for instance, looking to a generation ahead of you. You want to check in. Have you done this? How are you going to do your return? Just to check-in to make sure that they're staying between the buoys. because you can reach out and you can help.

STEVEN TOPOROFF: Thanks. So I want to turn to solving the problem. If a senior discovers that they are a victim of tax identity theft, what are the best steps? What's the best advice that we can give to seniors and their advocates? And caregivers?

First, where can older Americans turn generally for advice? So Chris, what is available from the Taxpayer Advocate Service?

CHRISTOPHER LEE: I think the first thing that we advise taxpayers is to, as Susan mentioned, open their mail and respond to the IRS. I think a lot of victims realize that they're victims of ID theft when they get notices from the IRS regarding a collection matter or exam matter. And if they've not filed a return and haven't filed a return for years but get an exam notice from the IRS, they should not ignore it. They should respond to the IRS.

And once the IRS figures out that it's identity theft, they'll move them into these identity theft procedures. And they'll fix their account and put an indicator on the account so that in future years they'll be protected against ID theft. So definitely want to respond to IRS notices.

The IRS also has information on their website about identity theft and about the steps they should take, such as contacting the credit bureaus, contacting the FTC in lodging complaint there.

The Taxpayer Advocate also has a website that kind of consolidates the information that's already out there on the IRS website. But it's basically the same information, just on one page. And the National Taxpayer Advocate has a short video talking about what they could do for identity theft.

If a tax identity theft victim is not able to resolve their issues with the IRS timely, they can always come to the Taxpayer Advocate Service and there's a directory of the local tax-- the closest Taxpayer Advocate Service office on the TAS website. So we would you the IRS to resolve the issue. But if they can't or if they're taking too long, we certainly are there to help them.

STEVEN TOPOROFF: Amber? Here's a question that we frequently get. And that is, sometimes people do not necessarily know that they're victims of identity theft.

For example, they get a breach notification letter from some company that says that their social security number may have been compromised, or they lose their wallet, or something like that. And then there are true victims of identity theft. Is there a difference in process at the IRS if you think that you may become a victim? Is there a procedure, or what's the best advice for those people?

And also, for those who are true victims-- for example, they've received a letter from the IRS that they failed to report income, which is a tip-off for possible identity theft. What are the processes that somebody should go to when they contact the IRS?

AMBER SMITH: Sure. So I would say that those are probably similar processes. There's a continuum there, and so some people would be in the beginning of the process. If they suffer an event, like a stolen wallet or even just a lost wallet, or something's kind of strange-- if they think that they may have inadvertently compromised their own information through phishing or some sort of social engineering, we recommend that they can call us. We have the Identity Protection Specialized Unit in order to be proactive and protecting themselves from negative tax consequences later on in the event that the identity thieve, or anybody who comes into possession of their information would try to get a refund using it.

We have the 14039, which is more commonly referred to by people who don't care for memorizing our numbers as the identity theft affidavit. That actually can be used for multiple purposes. It can be used for people who suspect that they-- or whose information may have been compromised. It can be used for people who know that they're victims of identity theft, but have not yet had any negative implications to their tax account.

When they call the Identity Protection Specialized Unit. And the number's on www.irs.gov. They will most likely be directed to fill out that form and submit it.

And what that does is it allows us to mark their accounts. So if something fishy happens with their tax accounts, or-- we're just going to pay a little bit more attention than we would just through normal processing. So that certainly helps as a proactive measure.

Chris' advice is very sound. If we identify the identity theft and we send out a notice of some sort or an AUR notice, an Automatic Underreporter notice because we've identified income associated with the person's social security number that wasn't reported by them, certainly get in contact. That will help us begin to resolve the case.

It can take a little time, unfortunately. But our goal is to get everybody their refunds, the refunds that they're supposed to get. And the sooner we can get started on that, the better.

STEVEN TOPOROFF: And David, at the Social Security Administration, if somebody who's a senior has a problem and they suspect that their social security number may have been compromised, or in fact, they know that it has been compromised, what are the best steps for them to take when it comes to contacting SSA?

DAVID LINDNER: Well, they have several steps to take, Steve. So I hope you're ready. No, just kidding.

STEVEN TOPOROFF: Go for it

DAVID LINDNER: Basically, if you think you're a victim of identity theft or any type of SSN misuse, the first thing you want to do is go into your local field office and file a report with them. Because most likely, you're missing a payment or your direct deposit has been redirected. So because of that, we're also going to file a report with the Department of Treasury to investigate where the missing payment went and try and track it down that way.

And we're also going to file a report with our Office of Inspector General. And you can even file a report directly with the OIG. They have an OIG hotline number. I can provide it to you, or I don't know if you want it afterwards? You want it now? All right.

STEVEN TOPOROFF: Sure.

DAVID LINDNER: It's 1-800-269-0271.

AUDIENCE: Can you repeat that?

DAVID LINDNER: I'm sorry. Yeah, 1-800-269-0271. And they would go forth with their reports and the field office would put a hold on your bank account because of the missing payment, or possibly redirected payment. And then the investigations are done by Treasury and OIG.

Now, you also move into another area where we also-- if you are a victim of identity theft or SSN misuse, you have a couple options. You can block electronic access to your social security records.

And to do that, you'd have to visit the website at socialsecurity.gov/blockaccess. It's not that difficult, amazingly. Thought it was going to be much worse, right? No.

And you can go there and sign up so that no one can have access electronically to your information in SSA's systems.

The downside of that is that you'll have to go into SSA field offices to conduct all your business. But this is a way that you can physically control who's going in, making changes to bank account, direct deposit information, anything else.

And lastly, if you think you're a member, or victim I should say, of identity theft or SSN misuse, we have what we call the direct deposit auto enrollment fraud block. So basically, what's going on now is, either through your financial institution or the Department of Treasury, a beneficiary can go in and pretty much sign up for this where any time he makes a change to his bank account, or routing numbers, or anything at his financial institution, that financial institution will automatically send the change to Social Security so that he continues to receive his benefit checks. There's no holdover because there's a problem with the routing numbers or the checking account numbers or anything like that. So it's automatically updated through the bank, and then to Social Security.

You can do this through either your financial institution themselves or the Department of Treasury. However, if you become a victim of identity theft and someone has found a way, after collecting enough of your personal information, to reroute these funds, they can easily go in there and it doesn't require authorization to make the change. So they can just say, I'm so and so, change the bank account to-- the benefit funds to go into a fraudulent bank account. And all of a sudden, you've got a huge problem on your hands.

Now, in reply to that, we do have a fraud block that we can put up. So that after that instance occurs, no longer can any changes be made without authorization on your record. If somebody came in and said, hey, I want to change my checking account number or whatever it is, the beneficiary would have to be there in person to authorize the change. So hopefully that cuts down on that type of direct deposit fraud.

But again, we want you to also contact-- like they were saying, contact the FTC, so they can collect the identity theft complaints and give you more resources on what you can do. Because identity theft can really hamper you in various elements of your life, not just these that we're talking about right now. So they'll provide you with more information on what to do.

Also again, the IRS. Because you don't want somebody to file a tax return under your SSN before you get the opportunity to.

There's also the Internet Crime Center. Crime Complaint Center I believe it's called. And basically, that center alerts the authorities to your identity theft claim. And it gets the appropriate law enforcement agencies with jurisdiction involved in the matter.

And lastly, like a lot of us have said up here too, is that you want to contact the three major credit bureaus to alert them to a possible misuse of your SSN. Mostly, Experian, Equifax, and TransUnion. I think you only have to contact one. I think they all contact one another. I'm not sure.

STEVEN TOPOROFF: Right.

AMBER SMITH: Just the one.

DAVID LINDNER: Just the one.

AMBER SMITH: Just one.

STEVEN TOPOROFF: You contact one, they'll contact the other two.

DAVID LINDNER: I mean, that's--

STEVEN TOPOROFF: That's very helpful.

AMBER SMITH: And just to add, if I could add one more thing because I don't think it's been mentioned. File a police report with your local police department. And I think a lot of people may be hesitant to do that. They don't want to be a bother. It seems like maybe a small thing, particularly if it's just a lost wallet, or if you think your information has been compromised, or if you know your information has been compromised. But if you know, file a police report. And that helps us, too.

We have partnerships with local police departments now. We assist them as much as we can. And a lot of these crimes are prosecuted on the state and local levels more so than the federal level.

STEVEN TOPOROFF: I'm going to ask David to address a question that we get all the time. And that is, when should you, if you're a victim of identity theft, in particular a senior, when should you ask to have your social security number changed?

And as a follow-up question to that, it's a little bit different, but we get the question all the time. So if I am a victim of tax and government benefits identity theft, am I, in fact, ultimately going to get my benefits? And I'm going to apologize, but I really need to step out a second. I haven't been feeling well. So if they could answer that, I'll be back in a second. Soon as I can. Thanks.

DAVID LINDNER: OK. Well, I can talk a little bit about the social security number and when you need to change it.

Pretty much, there's a lot-- it's more than just a number, as I think we all know. So the Social Security Administration takes it very seriously whenever we are looking into changing someone's SSN. This is something that not exactly always for the better, but it's followed you through your whole life and it connects you with a number of things you wouldn't even imagine. So if you are looking for a fresh start with a new social security number, it might not be exactly what you're looking for. And that's why we ask you to contact the FTC, and IRS, and Internet Complaint Crime Center, and the credit bureaus first to see if they can resolve the problems of identity theft or SSN misuse that you guys are possibly undergoing. And hopefully, that straightens out the issue.

However, if there's enough of a basis and continual misuse of your own SSN, then we'll definitely look into, after all the steps are taken, to change your SSN and do everything we can to make things better for you.

But the problem is-- this is where the other side comes in. Like I said, it would be easy if we could just change your SSN. But there's a lot of disadvantages to it as well.

As I say, it doesn't necessarily give you a fresh start. You show up and you all of a sudden, all the other government agencies and private companies, they all have you under your old SSN. All your records are under that old SSN. And it's not going to be very easy for you to get those records from those companies and agencies if you keep supplying a different SSN. It's a real headache to explain your situation and why you got this new SSN. It's not something they're probably going to see a lot. And so it's going to be very difficult in that respect to get your SSNs linked so that the old you can link up to the new you, per se.

And credit is another issue. It's important that you get your old credit linked to your new SSN. Because otherwise, you're a senior just starting out. You're going to have zero credit. If you're a senior beneficiary, it's not going to be very easy to apply for anything because they're going to be wondering why you have no credit and you're of senior age. So it makes things a little murky.

And I don't have all the answers in terms of the credit lines and how that works out. We were talking about that a little bit before we started. I don't know if that breaks down into the financial institutions, credit bureaus, or how that works and how that is connected. Because you also got to think that with your own line of credit, if somebody was using that credit, you don't necessarily want all of that old bad credit that somebody ran up on you to go with your new SSN either. Then you really haven't accomplished anything. So we take it very seriously.

And we do do it in severe circumstances, but it's very important that when you are undergoing something like that, that you really document everything extremely well. So that when you present it to us, we can see the continual patterns of misuse and the problems it's causing you on a daily basis.

It's not us just wanting to be hard on you guys. We just really know there's so many implications in changing your SSN that could follow if it's not done correctly.

SPEAKER 1: Thanks very much. And I see we have about 15 minutes left. We do want to get to audience questions. But before doing that, we did want to touch on one more issue, which is the move to plastic. And as the government moves away from paper to plastic distribution of benefit payments, what should seniors look out for? I'll start with the Robert. Should seniors be encouraged to use plastic to obtain tax refunds and benefits, and what are the considerations there?

ROBERT KERR: I think it's important to keep in mind a couple of things here. In some corners of the world, the government agencies are moving in this direction. And Susan, you might know this. In California, aren't unemployment benefits done on cards? I think that they are out there. And so the government is trying to find ways not to use checks anymore.

The other thing is, is that some people don't live in places that they have secure mailboxes, so it makes it hard to get a check from IRS to a person.

And finally, a lot of people aren't banked. And so if you don't have a bank account, then what do you do with this check that comes to you? So there's lots of reasons to use something other than a check or direct deposit.

From our perspective, we're agnostic on whether someone uses plastic or whether someone does a direct deposit or someone asks the check be mailed to them. I think different individuals have different circumstances though.

STEVEN TOPOROFF: Again, I apologize for having to step out. But John, any thoughts on when seniors do use the prepaid cards, what are some of the ways that Green Dot and others in the industry are securing the cards when protecting seniors from possible abuse?

JOHN MORTON: That's a good question and thanks for asking it. Really, we've seen the rise. Prepaid's a fairly new industry in this country. It didn't really exist 10 years ago. And so I think a lot of the federal benefits and tax fraud that we see in relation to prepaid is related to the fact that it's a new industry and fraudsters and scammers are always trying to find the next easiest way to get money in and off in committing these frauds.

Green Dot has invested millions over the last few years in improved fraud detection systems, monitoring, et cetera, to stop and thwart these tax fraudsters and these federal benefit fraudsters.

I'm not, for some very legitimate reasons, going to sit here and list all of our controls. A, we don't have enough time. And B, it actually puts people at risk if I start discussing all of our controls and detail. But we do look at when you're opening an account, who are you? We verify you. We go out to those credit reporting agencies that you've heard mentioned and verify you. We ask you additional questions, what is known as knowledge-based authentication or out-of-wallet questions.

If you've ever ordered your own credit report, you know what those look like. We ask you questions that you should only know about. And tools like that have done a great deal to drive tax and federal benefits fraud off of our portfolios at Green Dot Corporation.

We've enhanced our monitoring. We're looking at every single thing you do much like a bank would. We are a bank. From the time you open the account until the time you close your account, as funds flow on and funds flow off. And that monitoring and those edit controls have allowed us to be the blocker return in the last few years, over three quarters of a billion dollars worth of suspicious deposit activity back to the federal government. So there's a lot of controls in place and a lot more being put into place by banks, by prepaid companies, et cetera, to deal with this problem.

If you're an elderly or senior citizen and you're opening up a prepaid card, that might be the right product for you. You'll see these controls. We're going to ask you for this information. We're

going to ask you questions about yourself. Just know that that's there to protect you. It can be a little bit of a pain. We acknowledge that, but it is a tool there to protect you.

STEVEN TOPOROFF: And if seniors do have problems, if they suspect that there's been misuse of their card, what should they do? What are some of the steps that they should follow?

JOHN MORTON: So most of the fraud that we see in this area isn't misuse of a senior's existing prepaid card. This is where someone's stolen a senior's identity and has opened up a prepaid card that the senior never authorized. So I'm going to answer it more from that perspective. And really, that's already been talked about here. I'll, at the end, come back to if your account that you actually have has been compromised.

But if you think you're a victim of identity theft and it's been used to perpetrate federal benefits fraud or tax fraud, please, by all means, contact the agency directly. Contact the IRS. Contact the Federal Benefit Agency. File the police report, et cetera. Those agencies all have processes worked out with the banks to notify us in those instances. And we work very closely with those agencies and treasury to repatriate the money that we still have on the account back.

In some cases, we will hear directly from the victim, more in the case of federal benefits fraud than tax fraud. In some cases, because when the victim's contacting the Federal Benefits Agency, not everybody has connected the dots yet that this is actually fraud. The victim's contacting the benefits agency saying, hey, I didn't get my direct deposit, which comes very routinely, as everybody knows. And the benefits agency is, in some cases, saying, well, we sent it here to Green Dot Corporation. And here's their phone number. And they'll call us and we'll say, well, did you specifically ask for it to be sent here? The answer becomes no.

So if we get contact from the victim directly and the victim notifies us that they think that they're a victim of identity theft and we're able to find an account matching that victim, we'll block that account to secure the funds and ensure that no other funds leave that account. And then what we typically will do is we will get on the phone with the victim and call back to the benefits agency to help begin that process of filing that claim and repatriating those funds.

If, on the other hand, you already have an existing account, whether it's a bank account, a checking account, a prepaid account, et cetera, and you feel that your account at that bank has been compromised. By all means, immediately get on the phone, notify that banking institution that you feel that your account's been compromised. And they all have processes and steps to deal with that, including the blocking of the account. Depending on what the compromise may be, they may reissue your account number, your route number, your account number, your checks if it's a checking account, or they may block and reissue the plastic that's linked to that account, the debit card that's linked to the account.

STEVEN TOPOROFF: Any of our other panelists have any words about the use of plastic for-- that's my term by the way. It's a Toporoff term-- the pre-loaded and downloadable cards? Any other comments on that?

DAVID LINDNER: Just if you think you're a victim of this prepaid card identity theft, the same steps that I discussed earlier for direct deposit are the same as how you should treat it. Come in or call your local office immediately, so we can get investigations started with Treasury and our Inspector General. And of course, as he was saying, call your FTC, the IRS, the Internet Crime Complaint Centers, and all the credit bureaus.

You can never do too much in these instances. And I think it's important to just really protect that card as much as you can. The card doesn't have much value unless it's in your possession. So it's important to hold onto that and not do anything-- I don't want to say stupid. But don't put your pin and password on the actual card itself and tape it on the back or anything like that. So that as soon as they find a card, they can withdraw the money right out of the card as well. I mean, just simple things like that. But protect it like it's your own debit card.

STEVEN TOPOROFF: OK. In the time that we have, which is just a few minutes, I'd like to open it up to questions from the audience. And we've also had some questions that have come in remotely, either through Twitter, Facebook, or through our inbox. And one of the questions that I'd like to ask the panel is, do we see any particular issues in the older population among Hispanics? Is there a particular problem there?

From the FTC's perspective, I'm not sure that we do, that we're informed that there's specific issues in the Hispanic population. But is anybody else seeing that as a particular concern?

SUSAN MORGENSTERN: I think identity theft is an equal opportunity-- finds its victims whatever their language.

STEVEN TOPOROFF: Another question that we had remotely is there's some studies that suggest that seniors have a low rate of identity theft. And the question is, are we overstating the problem? And I'll answer it first, but then I'll open it up.

To us, it's not necessarily a question of numbers, it's a question of impact. And that is any amount of identity theft involving seniors is something that we should all be concerned about. Because seniors, as we're going to discuss later in the day, have particular issues-- maybe. It depends upon the senior, but could have issues in terms of mental capacity, mobility, isolation. So even if you look at the numbers whether seniors are particularly vulnerable or not, maybe the studies are correct that they're no more vulnerable than other people, which is what Chairman Ramirez actually said in her opening remarks.

But again, the impact to the individuals involved can be great. Think of your parents, if they came home and received a letter from the IRS that they didn't report income or they couldn't get their social security benefit that months, and they don't necessarily understand why. So again, from my perspective, as somebody who does this work at the Federal Trade Commission, is involved in identity theft issues on a daily basis, any amount of identity theft that impacts a group, whether it's children, which we focused on a few years ago, or seniors, is something worthy of our attention. Any thoughts from the panelists?

AMBER SMITH: Yeah. I would absolutely agree with that. And I think that it's an area that is just ripe for growth. Especially as technology becomes more complicated. I don't know about you all, but I have trouble keeping up with technological developments, not being the most savvy person. But I think as those developments increase at an exponential rate, it's going to be just easier and easier and easier to lose track of all the different ways you need to be protecting your information. And that could particularly be a problem for seniors.

But even so, any amount is too much. And it's important to recognize that identity theft is relatively easy. It's one of those crimes that it's huge because it's fairly easy. And so it's something that, regardless of the numbers, we should be very, very aggressive about addressing.

CHRISTOPHER LEE: I don't the IRS has done any demographic analysis on the victims of ID theft. But as you said, impact on the elderly is significant. And also, it can be undetected for years. And so that's why we think the senior population is exceptionally vulnerable.

And one thing that I wanted to mention is we talked about alerting the credit bureaus of your ID theft. But also, you can order a free transcript of your IRS account. And it's worthwhile doing once every few years, if not every year, just to make sure that your account-- especially if you know you shouldn't have filed for the last five years, but there's been returns filed every year, then you should definitely alert the IRS.

I don't like getting correspondence from the IRS. I hate getting mail. But I did order a transcript a few weeks ago. There's an app for iPhone called IRS2Go and you can order it through that, or you can call the IRS at the regular toll-free number and make sure you account is clean.

SUSAN MORGENSTERN: In fact, there are several transcripts and we order those transcripts when we first get an identity theft case in. You can see the returns that were filed on your social security number, the wages and other income that was reported on your social security number. And then you could also get a third transcript that shows the journey of your tax return through the IRS. So all three types of transcripts are very useful to taxpayers or to victims of identity theft.

STEVEN TOPOROFF: Great advice. And with that, we're going to conclude this panel. I want to thank all the panelists for coming here today. I know I learned a lot. And again, I appreciate their willingness to come out and participate in this forum. So thanks.

STEVEN TOPOROFF: And with that, we're going to take a short break. And the next panel will tackle issues involving medical identity theft.