FTC Identity Theft: Planning for the Future Conference
May 25, 2017
Segment 1
Transcript

JOHN KREBS: Hi everyone. Welcome. Thank you for coming. Thank you for those who are participating on our webcast my name's John Krebs. I'm with Division of Privacy and Identity Protection. I just want do some quick general information. So if you leave the building, please be aware you're going to have to go through security again. Lunch is at 1:00, and there's a great cafeteria out to the left. If you haven't seen them, restrooms are located just outside of the hallway.

Going to ask everybody, if you can, if you'd silence your cell phones. This event is being webcast. So please be aware of that. If anybody does see any suspicious activity, please let our security force know. In the event of emergency, take a second to read this. But the key thing I want everyone to know is that please follow the directions of FTC staff. We have different procedures if we need to leave the building or if we have to evacuate. If we do need to evacuate, the 7th Street exit-- we'll leave through the 7st Street exit and head down 7th Street towards E Street and congregate. There's a church. We'll meet there. Hopefully none of this will be necessary.

There are question cards during the panel presentations. If you have a question, please write it on the card and hold it up. FTC staff will come and pick it up. We're cognizant of the fact that we might not get through all of the questions. And if you have a question, either on the webcast or here live and we're not able to get to it, we would really like people to go to the event page and to the public comments section and fill in those comments. If you think of something afterwards, we want this to be a continuing conversation. So please go with any questions, any thoughts, any additional information that you feel wasn't presented here.

As I said, this begins a conversation about all of these issues. And we want to work with you to address these. So here's my contact information. Following the event, please feel free to reach out to me. We're happy to get your perspective and your thoughts on all these issues. And with that, I'm going to welcome the Chairman of the Federal Trade Commission, Maureen Ohlhausen.

[APPLAUSE]

MAUREEN OHLHAUSEN: Well, thank you, John, for that nice introduction. And thank you everyone for being here today. We've an important and timely agenda planned. And I'd like to take a moment to recognize the hard work put in by the FTC staff who organized this workshop, with a special thanks to Ryan [INAUDIBLE] and John Krebs for leading the effort.

I also want to thank Amy Wang, an identity theft victim who's traveled here today to share her story. We're grateful to Amy for taking the time and allowing us to put a face to the problem we're here to address. So often we discuss identity theft in the aggregate, at an impersonal level. Amy's voice at this workshop reminds us that our ultimate goal of combating identity theft is a

deeply personal one for millions of victims. And I hope Amy's story will inspire us to redouble our efforts in achieving that goal.

Now in Hollywood, identity theft is often depicted in humorous or glamorous ways. So from Robin Williams' lovable Mrs. Doubtfire to Melissa McCarthy's down on her luck character in the movie Identity Theft-- which I was just mentioning I did watch on an airplane once-- identity thieves are often portrayed as bumbling but lovable people. In other instances, like the Oceans 11 and Mission Impossible movies, we are expected to root for heroes who routinely steal other people's identities.

But in reality, identity theft is a serious crime that can seriously harm its victims. Victims have their money stolen out of their bank accounts, have their good names and good credit ruined, and can even suffer improper medical treatment if a fraudster has stolen and used their medical identity. Such crimes affect millions of Americans every year. The Department of Justice estimates that in 2014, 7% of US citizens aged 16 or older were victims of identity theft, suffering over $15 billion in financial losses.

And the harms of identity theft are not limited to just those consumers whose identities are stolen. It also affects, for example, small businesses that are defrauded, as well as state and federal governments that pay out fraudulent benefits. Today's workshop is a unique opportunity to develop a greater understanding of the problems associated with identity theft, the impact on particular populations, and potential solutions.

The FTC has a long history of dealing with these complex issues. And to kick off our workshop, let me briefly share with you some of the work the FTC has done to protect consumers from identity theft, as well as some of the current and future challenges in this area that we'll discuss today. Now the FTC has been at the forefront of the fight against identity theft going back to 1998-- I was actually here at the Commission then-- when Congress made it a federal crime.

Since then, the FTC has implemented a comprehensive program to combat identity theft. We've collected over 4.5 million identity theft complaints, made them available to our criminal law enforcement colleagues, and used them to publish a yearly report to inform policymakers. We've issued rules and guidance under the Fair Credit Reporting Act to provide additional safeguards for sensitive information about consumers. We continue to provide businesses and consumers with educational materials that help them understand identity theft and protect themselves from it.

And through our enforcement actions, we work to ensure that businesses take reasonable measures to protect consumers' personal information so it doesn't fall into the hands of identity thieves in the first place. In 2006, we began taking a broader look at the problem. At that time, President Bush established the Identity Theft Task Force, a multi-agency effort that the FTC co-chaired with the Department of Justice. The task force's report had recommendations for both the public and private sectors.

For example, the report prompted a review at all levels of government to reduce the unnecessary use of Social Security numbers and proposed changes to criminal laws in the US to make it

easier to prosecute identity thieves. The report also emphasized the importance of educating businesses to safeguard consumer data and recommended that government agencies continue to investigate, and where appropriate, take enforcement action against entities that violate data security laws. And the report recommended the development of a model identity theft report form to make it easier for victims to recover.

The FTC's work to combat identity theft has continued in the decade or so since the Identity Theft Task Force report. We've hosted workshops on child identity theft and senior ID theft, testified before Congress on related issues, and most recently launched the new and improved identity theft website. Now, this website is a free one stop resource for consumers that they can use to report and recover from identity theft. As part of the site, identity theft victims obtain personalized recovery plans based on their specific experience and get customized letters and forms to send to credit bureaus, debt collectors, and other businesses.

Now I'm pleased to note that the team that created this website is a finalist for a 2007 Service to America Medal, also known as the Sammie, which has been called the Oscars of government service. And I've also heard, as I've been out and about visiting folks around the country, about how this site has really helped individual consumers and how incredibly useful they find it in an hour when they're confused, when they feel very at sea, to have this kind of step-by-step process available to them.

Now, in our efforts to fight identity theft, some challenges are persistent, such as the difficulty of holding hackers located in other countries accountable. But in our two decades of experience combating identity theft, we've certainly seen an evolution in the nature of the crime and the challenges it raises. Now first the scope of the problem has changed. We've witnessed dramatic changes in technology, that while making our lives significantly better, have also facilitated fraud on a grander scale.

Fraudsters are using new and increasingly complex technologies to steal sensitive information about consumers. To be successful in fighting back against identity thieves, we must understand how technology not only facilitates identity theft, but how it can also be a tool to protect against it. So indeed, our challenge is to leverage technology to stay one step ahead of identity thieves. And today's workshop provides a forum to discuss just how to do that.

Now a second challenge that we'll discuss today is the rise of tax identity theft. And this occurs when someone uses your personal information to file a tax return and claim a fraudulent refund. In 2008, the IRS identified less than 50,000 tax related identity theft incidents. By 2015, the IRS had identified over 1.8 million fraudulent returns, through which identity thieves had attempted to obtain over $14 billion in refunds.

Now, while the IRS has made huge strides detecting fraudulent returns, tax identity theft remains a multibillion dollar problem. And since many low income consumers rely on tax refunds to make ends meet, tax identity theft can have painful consequences for victims when refunds are delayed.

Changes in technology have also increased the risks for consumers of medical identity theft. Now less than a decade ago, consumers' medical information was kept in paper files. Now that information is typically maintained in electronic form, and there may be a greater likelihood that bad actors could gain access to it. So indeed one recent report suggested that in 2016 there was on average one health care sector breach per day, resulting in the potential exposure of 27 million patient records.

Now, the information contained in electronic health records is extremely lucrative for hackers. A complete EHR database can be sold for as much as $500,000 on the dark web. The information used by identity thieves to, for example, procure prescription medications that can then be resold for a profit is just one example of how this information can be used. Now medical identity theft poses several vexing challenges.

One, it is difficult to detect. Months and sometimes years can pass before a consumer realizes his medical identity has been stolen, if he realizes it at all. Two, it is extremely difficult to remediate. Victims are left with a host of problems to untangle, such as disputing unauthorized charges with their doctors and insurers, as well as trying to remove inaccurate information polluting their medical histories. And three, medical identity theft can lead to serious physical injury to consumers if their health information is co-mingled with that of identity thieves.

So with the challenges of identity theft in mind, let's turn to our goals for. Today in the midst of this changing landscape, we want to take a fresh look at what identity theft looks like in 2017 and begin planning for the future. The FTC and our stakeholder partners have been in the identity theft trenches for a long time, but there is always more to do. My hope is that today's workshop will inspire a call to action to improve all of our efforts to tackle identity theft head on.

In particular, I'd like to issue a call to action in three areas. First, a call for more research. The FTC will focus its resources on data driven policy initiatives aimed at identifying and laying a foundation to address harmful conduct. Our Office of Technology, Research, and Investigations will present later today on some research that they've already conducted. But today's workshop is just the beginning.

One of my major priorities over the next several months is to deepen the FTC's understanding of the economics of privacy and substantial injury in the context of information exposure. While we continue to actively enforce the law to protect consumers from harm, we will also be studying in greater detail the types of harm that consumers suffer when their sensitive information is compromised. By harnessing the research functions of the agency, we can better prepare ourselves to protect consumers from the harms of identity theft in the future.

But we can't do it alone. I call on academics, researchers, technologists, industry, government, consumer advocates, and others to improve our understanding of identity theft by conducting additional research. For example, how can we quantify the magnitude of harms from identity theft? What is the social cost of identity theft? What is the impact of identity theft on certain populations, such as veterans and their families? More research is sure to lead to better policy making.

Second, I issue a call for more cooperation and coordination across the federal government, as well as with our state partners. As identity theft experts and the primary cop on the beat when it comes to privacy and data security, I intend to continue the FTC's leadership in this area. For example, the FTC recently joined forces with the Small Business Administration to announce new education initiatives for small businesses.

And for our part, we launched ftc.gov/smallbusiness, a site to help companies stay ahead with the latest scams, reduce the risk of cyber threats, and respond in the case of a data breach. We've also worked with federal partners over the last several years to host Tax Identity Theft Awareness Week, to raise awareness of tax identity theft and provide consumers tips on how to protect themselves and what to do if they become victims.

And this year, the FTC will chair the cyber security forum for independent and executive branch regulators, a forum for independent agencies to share information, coordinate, and ensure consistency in approaches about ongoing cybersecurity efforts. Now we're ready to take the lead, and we have no intention of slowing down. And we're anxious to work more closely with other agencies with related missions. So the Department of Justice, IRS, HHS, to name just a few. By working together, we can avoid duplication, streamline projects and investigations, and most importantly, provide better protection to the American public.

So third, I call for more public private partnerships. For example, the Commission is working currently with Experian, Equifax, and TransUnion to make it easier for consumers using identitytheft.gov to obtain their free credit reports. We welcome additional partnerships that will help identitytheft.gov become the one stop shop to help consumers recover from identity theft. And we need more efforts, like the Security Summit Initiative, a unique partnership we'll hear more about today between the IRS, state revenue departments, and private sector tax industry leaders to combat identity theft and tax refund fraud.

Now, identity theft is a scourge for both public and private institutions. And success in our fight against it will require cooperation on all fronts. So given the current identity theft landscape, we've got a lot to do. The Commission has a long history of cooperation with stakeholders on identity theft issues. And we look forward to continuing those efforts. So thank you again for being here today. And let's get to work. [APPLAUSE]

JOHN KREBS: Thank you, Chairman Ohlhausen, for those great opening remarks. We're going to get to work by setting the stage for today's conference with presentations from three people-- Keith Anderson, Sean McCleskey, and Alana Benson. And so we'll get started with Keith.

KEITH ANDERSON: [INAUDIBLE] Good morning. I am Keith Anderson, an economist in the Bureau of Economics at the FTC. Because I work for the FTC, I need to provide you with a standard government disclaimer. The views I will express here are mine alone, and do not necessarily reflect the views of the Federal Trade Commission or any of its commissioners.

What I'm going to try to do is to provide a lightning speed overview of the current state of the problem of ID theft. But my approach is going to be the inverse of Amy's forthcoming approach, because I'm going to be basing my remarks on the data obtained in 2014, when the Bureau of

Justice Statistics in the Department of Justice conducted a survey on ID theft as a supplement to their National Crime Victimization Survey.

As you may know, the National Crime Victimization Survey is a large scale survey whose traditional focus is crimes like assaults, burglaries, et cetera. However in recent years, BJS has expanded the range of items covered by adding periodic supplements. The 2014 ID theft supplement collected data from more than 64,000 individuals aged 16 and over. I would note that BJS did another ID theft supplement in 2016, and the results of that survey we hope will be available later this year.

The NCVS is a survey of a random sample of US adults, and therefore relies on the ability of crime victims to describe their experiences. While this should not be a problem when we are talking about crimes like theft or assault, it can be a bit more of a challenge in the context of ID theft, where some victims may not be aware that their information has been stolen. This can be particularly a problem if we are talking about a synthetic ID theft, something you will hear more about today.

In synthetic ID theft, the thief constructs a new pseudoindividual using some information about one person and some about another, possibly even making up some of the information. As a result, the victims may be less likely to discover that their information has been misused. As Chairman Ohlhausen noted, the 2014 BJS survey found that 7% of US adults had been victims of some form of ID theft during the 12-month period before they were interviewed. The vast majority of these were limited to the misuse of an existing account, such as an existing credit card account or an existing bank account.

An estimated 0.7% of adults were victims of a more serious type of ID theft, sometimes referred to as ID fraud. In these cases, new accounts were opened using the victim's personal information, or their personal information was misused in other ways, such as to file a fraudulent tax return, to provide false information to the police, or to obtain medical treatment. To place this in a bit of context, though I would not want to claim that the crimes were really comparable, the number of Americans who reported being a victim of an assault in 2014 was only about 40% greater than the number who reported being victims of identity fraud.

Before talking about the magnitude of financial costs that result from identity theft, I would first note that the BJS questions ask whether someone misused or attempted to misuse the personal information of the person being interviewed. That is, the questions are not seeking just information about the misuses that actually resulted in a financial loss. Indeed, about 35% of those who report that their personal information was misused report that there was no financial cost associated with their experience.

This may suggest that around 35% of those reporting a misuse of their information only experienced an attempt at misuse, which in turn may suggest that about 4 and 1/2% of US adults were victims of successful misuses. I find this interesting because it is very close to the 4.6% prevalence figure we found in a 2003 survey on ID theft conducted for the FTC, which only asked about successful misuses. While only a rough indicator, given various other differences

between the two surveys, this may suggest that the overall prevalence of ID theft has not changed a whole lot in the last 10 years.

Turning now to the costs that were incurred in those instances where there was a financial loss, I note that the median social cost resulting from an incident of ID theft was about $300. That is, not counting those cases where a zero social cost was reported. Half of the ID theft incidents involved an amount less than $300, and half involved an amount greater than $300. When I talk about the social cost of ID theft, I'm including both victims' estimates of the value of what ID thieves were able to obtain using their personal information and any other expenses that were incurred by the victims.

Of course, not all of these expenses were borne by the victim themselves. For example, think about a case in which an existing credit card is used to purchase something. In most cases, the direct cost of misuse is covered by the credit card system, not the individual whose card was misused. While the median cost here was $300, it's important to note that these costs are heavily skewed, with a limited number of incidents involving much greater social costs.

In 10% of incidents, the social cost was at least $2,000. Indeed, almost 3/4 of the total social cost reported was accounted for by these 10% of incidents. As I noted, not all costs that result from ID theft are paid out of the victim's pocket. Indeed, less than 14% of ID theft victims reported that they personally incurred any expenses. Of those who did incur an out-of-pocket loss, the median amount was $100. And again, the figures are highly skewed. In 10% of cases, the victim paid at least $1,500.

Not surprisingly, the cost of ID theft-- both the social cost and the cost directly borne by the victim-- differ by the type of misuse experienced. While the median social cost from the misuse of an existing credit card is only $300-- and that's only in those cases where there actually is a cost-- the median social cost from the creation of a new account is almost $700. And for other misuses, the median social cost is $1,000.

Therefore, for my remaining couple of minutes, I will focus on what occurred in those instances where there was identity fraud. That is, new accounts were opened or other misuses were made of the victim's personal information. Consider first the kinds of misuses that were most prevalent. Not surprisingly, the most common misuse was the opening of a new credit card account, which occurred in 30% of identity frauds.

The second most prevalent problem was filing a fraudulent tax return, which occurred in almost 15% of these cases. Filling out the top five misuses experienced by victims were opening new telephone accounts, obtaining new loans or mortgages, and presenting the victim's identity information to police. In addition to direct out-of-pocket financial costs resulting from their ID theft experiences, some victims of ID theft incurred other types of financial problems. 14% of ID theft fraud victims, ID fraud victims, reported that as a result of the theft of their information, they had had problems with debt collectors. 13% said that they had experienced credit related problems. Almost 7% indicated that they had experienced banking problems.

Victims of ID theft often also incur problems in addition to direct financial loss. One of these is the amount of time victims must spend trying to resolve the problems that result from being victimized. At the time they were interviewed, over a quarter of ID fraud victims indicated they had not yet succeeded in resolving all of the problems that resulted from their victimization. Of those who believed that they had resolved all of their problems, almost a quarter said that it had taken them a month or longer to do so.

Many victims also incurred emotional distress as a result of their victimization. Indeed, 55% of ID fraud victims said that they had experienced either moderate or severe emotional distress as a result. These In fact, these numbers are comparable to what was reported by those who had been a victim of assault. Finally, let us take a quick look at whether the risk of being a victim of ID fraud varies across different demographic groups.

Looking first at age, we find that while 0.8% of those between 25 and 64 were a victim of identity fraud, the figure was lower, 0.5%, for those who were between 18 and 24 or were 65 and over. Consider next race and ethnicity. And here I need to note that the figure for non-Hispanic whites on my slide is incorrect. 0.6% of non-Hispanic whites report being a victim of identity fraud. The prevalence among blacks or African Americans was significantly higher, 1%. The rate for Hispanics or Latinos was 0.8%, slightly higher than the rate for non-Hispanic whites. Finally-- and again, my slide here is correct-- those with lower incomes-- i.e., those with incomes of less than $25,000-- were more likely to be a victim than were those with greater incomes. It's 1.1% versus 0.7%.

In sum ID theft continues to be a serious problem. While the prevalence of ID theft may not have increased a lot in the past 10 years, it also does not appear to have declined. And while many victims of ID theft, particularly those who only experience the misuse of an existing account such as a credit card account, may incur only limited expenses and problems, the problems are quite substantial for many of those who experience the more severe types of ID theft, having new accounts opened with their personal information or having their information misused in other ways, such as to file a tax return and provide a false ID to the police. Thank you. How did I do that?

JOHN KREBS: Thank you, Keith. [APPLAUSE]

SEAN MCCLESKEY: Good morning, everybody. Hear me all right? Hi, my name is Sean McCleskey. I work for the University of Texas at Austin for the Center for Identity And prior to that, I served 17 years with the Secret Service before I retired from the San Antonio field office, where I ran an identity theft and cyber crimes unit. So that's sort of my background as I provide this presentation.

Identity theft today. So we're going to do a very quick overall dive on the issues confounding us with identity theft today, sort of looking at what is identity theft, what are the problems that we're facing, and maybe what are some solutions. And I'm going to give you some things that I did in my neck of the woods in San Antonio with my task force that we had some fairly good success with identity theft. Didn't eradicate it by any means, but we really had a good program that definitely reduced some of our issues in our backyard.

So identity theft is the fraudulent acquisition or the use of a person's personally identifiable information. Usually we think of that as name, date of birth, social security number, anything that ties-- bank account number, credit card number. That definition is growing fairly rapidly as we start looking at what is identity. Some of the things that we have identified obviously is your-- besides your social security number, it is your email. Maybe your token to get into work. That identifies you as well and gives you access.

So the things that we delineate as an identity is growing and growing. And therefore, we have to start looking at those different things as well as some of the more standard PII that we've looked at in the past. So we typically have financial fraud, which usually everybody is fairly aware of. Checks, credit cards, bank accounts, and so forth. That's generally what people associate with identity theft, right? Credit card being stolen, bank account being stolen.

We have tax identity theft, which we talked about. Should you ever get a call from the IRS about your taxes, no. Hopefully that's one of the things that we keep spreading the word out. You should never receive a phone call from anybody saying you owe money, and you're going to be sued, or you're going to be arrested for that. Hopefully that's a message that we are still getting out. We're working at UT Austin. And I know the Secret Service is doing that as well.

We have medical identity theft, which we talked about, which is a major problem because not only is your information in there, what else is in there? Probably your spouse's information. Probably your children's information. Plus it has information which is very sensitive, which is what your health information. I purchased at one point in a case about 10,000 medical files from a member of the Aryan Brotherhood in San Antonio who had stolen those from a doctor's office. Doctor's office had no idea that those records were in fact stolen.

And there was a lot of information in there. I could have gone to town making a lot of different identity documents and completely creating identities based off the information that I had within those files that they'd given me as well. Obviously cyber intrusions is a very large topic today. We hear that quite a bit about information being stolen, sort of these large breaches. Ghosting which is using somebody who is deceased, their information, which is a problem.

But one of the things I really want to talk about is synthetic identity. We touched on it a little bit. That's one of the biggest issues we're being confronted with right now in law enforcement, as well as academia. Because synthetic identity is obviously you're taking bits and pieces, maybe a fake date of birth, but a real social, a real address or fake address, and then a real social security number. So you're kind of merging all of that together.

So what does that do? It makes it harder for the victim of it to be notified of it. It makes it harder for the institution that's being provided the documents and issuing out either credit or opening a bank account to notice that as well. And so what we have found is a criminal will figure out, OK, I've got this blend of different things. And I'm going to fire it out to these different organizations using, for example, a good social security number, maybe a fake name, and so forth.

What that is doing, we see, is creating a credit file. Not necessarily a credit history. But maybe a credit file. And there are institutions that will issue credit based off you having a credit file and

not necessarily a credit history. So that becomes also problematic. And then you've got-- it's just much harder to dive down and figure out who is doing what in that scenario. It also makes it harder for some of the laws we have if you are in fact switching some of those identifiers around.

The last statistics that I saw on this was they thought 80% of credit card fraud now was related to synthetic identity. And they also said they thought proximately 50% of the social security numbers being used in synthetic identity belong to children. So obviously that's a real issue. And the hard part, I can say as an investigator, is sort of tracking it down. It's hard enough to sort of track down the real victim sometimes on a case. If you've got transposed dates of birth with somebody else's social security number with a fake address, it makes doing what we do much more difficult. Because we're going down a lot of different trails to locate who we need to locate and figure out who's involved in this.

What's going to have to happen with institutions is they're going to have to start, I think, looking at more as far as computer learning on their writing algorithms, when folks supply their information to open up an account to see if those numbers match with each other. As opposed to just kind of doing a very quick cursory look and then checking it off. But what's made that even more difficult is what? Most Very few people go up to their bank anymore and deal directly with their banker, right? Most of this is online.

It's mobile. And so that's part of the problem, is that you're doing this from a distance. So nobody's actually seeing when you come in and looking at sometimes the date of birth or looking to see if these things match or if these numbers correspond. So again, that's why synthetic identity is something we're going to have to really start looking at and working on and understanding how it works and how we defeat that type of crime when we're up against it.

So the impact of identity theft, it's big, it's real, and it's diverse. Not only do we have the financial loss which we look at. We have-- it's an increase in other crimes. Identity theft is usually ancillary to a lot of other offenses. We have national security risks. We have your personal security risks. We have reputational damage. Most people don't realize-- there's a number of identity theft cases that we investigate involving where it's sort of-- you've heard of the revenge porn, or you've heard people getting online and pretending to be somebody else, particularly in a relationship that breaks up.

And then they're inviting people to come meet them and putting out information you would not want. I've worked a number of those cases. I had the honor-- I don't know if you would call it that-- to work one of the very first impersonation cases on Myspace. And it was a nightmare for the victim in that case. And so that's one of the things we sort of forget about as well when we deal with identity theft.

Why is identity theft so popular? It's very simple. Economics. Much higher level, you get a better bang for your buck. You get a lot of money potentially. Jail time is pretty minimal. And it's also easier to launder. It's much more easier to do that than drugs sometimes. And the biggest problem is a lot of businesses are willing to accept those losses. We hear that constantly, constantly, constantly. It's just part of doing business. We're going to accept it and move on.

These crimes are typically detected well after they are committed, often unreported. And due to jurisdictional issues and scarce resources, often never investigated. This is one of the biggest issues. Some people are just embarrassed because they handed over information they shouldn't have. They got a phone call from somebody. They gave it to them. And then they went, whoops. That's probably a bad idea. I shouldn't have done that. And so they're embarrassed to report that.

A lot of times I hear a lot of people say they'll go into a local police department, and the local police department's like, we don't have the resources to do this. We just simply don't have the manpower. It's You're coming here to Texas. It's out in California. We just can't really do much for you. So a lot of frustration. So people, if they're usually the victim one time, if they're victimized again, I found sometimes they don't want to come back because they're like, I know the song and dance I'm going to get from the agency. So I'm not even going to bother going in there.

And most people think, well, if they get caught, get arrested, nothing's really going to happen to them anyway. They're going to get a slap on the wrist. They're going to get probation. So why bother? But the thing that we are seeing, particularly in law enforcement, is these crimes are increasingly becoming part of other criminal organizations. A lot of many of which are transnational.

There was a number of credit card cases I worked out of San Antonio in which the credit card scheme was being orchestrated by a cartel or a criminal organization out of Mexico. Why? It made good business. It was sort of they had a credit card division. It was easy to get numbers out of Mexico. It was easy to put them on counterfeit credit cards. And it was easy to go in there and have people buy things and bring it back across the border. And it just supplemented their income.

And also, again, less likely to be prosecuted. Less likely to be investigated. Less likely to draw attention to what they were up to. So we saw that multiple, multiple times. We're dealing somewhat with the attorney general's office in Texas right now on human trafficking. One of the things they're saying is identity theft is very prevalent in human trafficking because they're using the victim's identity to purchase hotel rooms, to purchase cars, to rent cars, to lease things, to open up lines of credit.

So not only is this person who gets-- if they get pulled out of this life, are they have the physical damage, the emotional damage, they now have an identity that's completely destroyed and in tatters. So there's lots of other reasons that identity theft is a real issue for us, other than sort of that financial loss which we've talked about.

Again, here's some illicit crimes. Most of these I've come across in some form or fashion. Obviously, narcotics, drug trafficking, organized crime, mail fraud. Mail theft is a huge crime that is tied into identity theft. It's probably one of the biggest issues right now in San Antonio that we are facing as far as a law enforcement agency, is still the theft of mail out of mailboxes. We keep thinking that's a really low tech crime, particularly we talk about cyber a lot. They're stealing mail left and right right now, probably right now as we speak.

Weapons trafficking, homicide, obviously national security, right? Using an identity to get into the country. Or again, even a synthetic identity. One of the big issues there. Wire fraud. We talked about human trafficking. Online impersonation, revenge porn, and extortion blackmail. These cases, these bottom cases, are very hard to prosecute sometimes. They sound like it would be very easy. I have found some of the US attorney's offices sort of reluctant in that because they're saying, well, maybe there's a consent issue there. May they shouldn't have-- it's not as easy a crime to prosecute and investigate as you would necessarily think. In some cases there are, but most of the times we've had issues with that.

So how is identity stolen? So one of the things we've started to do at UT is start looking at the actual statistics related to identity. What is actually being stolen? And one of the things we do is we've got the ITAP. And the ITAP is the Identity Threat Assessment and Prediction program. And it's a-- we model identity theft breach cases and figure out what are the real statistics behind the theft of this data.

One of the interesting things that we've come up with, particularly in today when we talk about cyber so much, is almost 50% of the cases that we modeled-- and these are open source cases that are provided to us through open sources, a lot of it through law enforcement. 50% of these cases do not deal with a computer. So it's the physical theft of data. So what does that tell me as either a policeman and/or an academic and/or business manager?

That if you're putting all your resources into your cyber-- which again, you should be-- but if you're putting everything into there, you're still leaving what? A huge gap. If you're not dealing with your people, if you're not dealing with your policies within your organization. Most people are pretty surprised by that number. I, quite frankly, was surprised when we did the research on that.

So we looked at most of the things that came through on these cases that we modeled. Again, probably no big surprise here. Physical theft was still a very large part of it. Stolen wallets, purses, mail. The phone and mail scams are still very prevalent. I think people forget about that. Dumpster diving, shoulder surfing, those are still things that are very active right now. Credit card skimming, the email phishing, social engineering, using unprotected WiFi networks. And then, of course, obviously the computer breaches, which gets a lot of media press and is a little bit more sexy.

But those other things are still happening. And anybody you talk to that's dealing with identity theft or particularly at a local department or in an identity theft task force, they're going to be just as covered up in these things as some of the other computer breaches or network intrusions. Again, still [INAUDIBLE]. We still have a lot of this going on. One of our big things was to push people to stop putting it in the mailbox and take it to the post office and put it in there.

And what are they stealing for the most part? Outgoing mail. Outgoing mail has checks in it. It has account numbers in it. You can wash a check pretty fast and go out and reprint it again. Or print it, fill it in, whatever you want to do. So that's still-- or I've seen them where they actually just steal the mailbox. Just rip it off the ground and take it behind them. Literally, police officers

have caught them driving down the street dragging a big mailbox behind it as it's bouncing, throwing up sparks.

So some of the research that we have done-- and these are some of the statistics on what we found. Insider theft was 10%. Third party vendors, 15%. Physical theft, 12%. Data on the move, 7%. Axonal exposure, 10. Employee negligence, 10. And hacking, 29%. So again, it's a fairly wide variety of things that are going. So if you focus on just one of them, you're going to get hit. There's no question about it. So that's something you need to think about when you're coming up with your policies and procedures within your organization dealing with data, security of data, and how that data is handled and what happens when it gets in fact disclosed without authorization.

One of the things that we are trying to also do is come up with a big picture for identity. It's not about just replacing your driver's license or your credit card. That may be replaceable. But the journey you got to get those things is not necessarily. I have a retired badge from Secret Service. If I lose that, they may or may not replace it. But if somebody goes out and steals my identity and pretends to be me, and also pretends that I'm a retired Secret Service agent, I can't replace the damage that's done to that.

I can't replace if somebody is out there pretending to be me as a UT employee. I may be able to replace that card, but I can't replace sort of the things I've done up to my life to be able to be in those positions. And that's one of the things we're really trying to get out there to people, is your identity is your story, your life story. And it got you to where you are today. And it's not really replaceable as some of the documents are.

And again, going on this again. We really need to think of, is it replaceable? And what is the value of your identity.? And that's one of the things we're really working hard. Because that's a big question. What is the value of your identity? What is your identity worth? What is your social security number? I could show you what it's worth for sale on the dark web. But what is it really worth to you over the span of your life?

And again, that's one of the things that we're doing, is looking at the value of identity, the liability. So we look and see OK if you steal a social security number, what else can that give you access to? How can you build an identity off of that one piece of data? If you steal a email address, an IP address, what will that lead you to to get to other pieces of information? And then what is the value of that if in fact it is disclosed?

And that's the thing that we've tried to also-- we've seen quite a bit-- is often it's tied to a document. It's a document, a credential, or a token. And so that's one of the things that we've tried to push out is, OK, security of those items. Your ID, that's just not something you can throw away or put aside and forget about. It has repercussions in fact if it gets lost or stolen. It can lead to other pieces of information that can in fact-- somebody can impersonate you or get access to something they shouldn't be getting access to.

One of the biggest things I've tried to do in Secret Service and at UT is to protect a thing is to know a thing. What are your assets? What is the value of your assets? Who's looking to steal these assets? And how would these assets be compromised?

More times than not, when I used to go into an organization that had a breach, I would ask, what kind of data do you have? Typically they would go, I don't really know. I know we have data because obviously somebody stole it. I can give you sort of a clue. I don't really know what we have. OK.

Do you know where it's located within your organization, physically, and/or within your network? Maybe. Maybe not. Who's got access to it? I don't really know that either. So those were fundamental questions that I would be asking as an investigator that a lot of organizations couldn't return the answer. So how are they going to protect their data, that entity, if they don't even know what they have, where it is, and who's got access to it?

That's one of the other things we've also done, is come in there and looked and see where are those breach points. Where are they coming in? Where are bad guys-- is it where we think they are, or is it someplace entirely different? And again, those statistics are helping us build tools that we're able to go out and provide assistance to organizations, whether it be a government or private organization.

Again, stress this again. That's why I put it in here twice. What identity assets do you hold? Where are they located? Who has access to them? Are they being monitored? Very few organizations-- you'd be surprised-- have their networks monitored.

I went to a municipal league conversation in Texas dealing with water boards and so forth. To my knowledge, none of them were having their networks monitored. This is water. Water is very important, right? They can go in there and direct-- there was a case I read about once where somebody went in and tried-- they hacked into the system, and they were using different types of chemical-- the normal chemicals they were putting in the water, they went in and tried to disrupt that. So huge issue. Nobody was monitoring. So that was my question. Why not? Nobody had a very good answer on that.

Again, one of the things we talk about is 50% of identity theft or breaches is not related to computer. So you really have got to look at what your people and your policies are doing in relation to how the people react with machines. That's why we say it's a two front fight. We've got to do both. If you have the best system in the world, and somebody walks in with a thumb drive and is able to download all the data from that-- or if, in fact, that thumb drive has a virus on it, doesn't matter. You may have just lost right there.

So we're trying to do more research on this. We're trying to go out and educate the workforce with s research saying, OK, this is what kind of-- this is the value of identity, according to our research. This is how people are trying to compromise it. This is what some of the things you should be looking for. And getting out there and really educating particularly managers and organizations.

The workforce is a big thing. Everyone uses PII to some degree to make decisions. Everyone typically collects some sort of PII. A lot of folks trade in PII, and there's a lot of people that are dealing with PII. Sometimes they don't even know they're dealing with PII, because it's just part of the job. It's part of the motions that they go through. And so we're trying to reach out to all those different organizations because it's just not one stakeholder that's involved in protecting data.

Law enforcement. We've got to do better with training in law enforcement. Particularly on the local level. Local law enforcement gets, in my opinion, not very good training when it comes to identity theft. Most young patrol officers, they go out there. They're looking for drugs and guns. When they walk into a room that's an identity theft organization, they're going to find printers, scanners, thumb drives, cell phones, card readers, embossers, laminators.

That's fairly innocuous stuff. It doesn't look to be overtly criminal, right? Particularly we've had an issue with some of the white hotel keys that are plain. They just have a strip on the back. You can put a lot of information in there. We've seen those tossed away a number of times. Why? Because they didn't know that's what they should be looking for. And so forth.

And this is why one of the things I've done is build a curriculum for law enforcement officers, particularly patrol officers. This is the kind of stuff you need to be looking for. It's not junk. It's not trash. It's potentially evidence. May not look it on its face, but it possibly is once you go in to do some forensics on it. Is this evidence?

You'd be surprised how many times this stuff gets tossed away because it doesn't look-- they just kind of look over real quick. Eh, it's paper, it's junk, it's trash. Move on. When in fact, it was some very valuable evidence. It's not an easy crime to investigate. Because again, it looks innocuous. Very unfamiliar how to collect it. Most folks don't know. They have a very limited knowledge of the laws that are available. And quite frankly, there's a big perception. Who cares? Nobody's going to do anything about it anyway. They're going to get a light sentence. They're going to get probation. Going to be right back on the street again.

So one of the things that we did in San Antonio is in 2004, I got asked to start a task force. I started the South Texas regional task force, which was a combination of local agencies in the San Antonio area, that we're all working the same thing. And guess what we were doing? It's pretty much stepping on each other's toes quite a bit. So we figured, all right, let's maybe work together and go out and try to combat this.

What we found very quickly is that we had a problem bigger than we ever thought we had. So we were going out and arresting a group of folks on a Tuesday, usually filing a state case on them because the state case is a little easier than federal cases to file. And they don't have the loss requirement that the fed cases have to have sometimes. They would go to jail. We'd go back and run another warrant on Thursday. Guess who we would find? Same bad guy again. 400 to 500 more pieces of PII he had in his possession.

We were doing this for about two years, basically chasing our tails to some degree. So I heard about a program out of Virginia that the Postal Inspection Service was using. And it involved the

use of the 1028A statute, which is one of the best statutes I think ever devised by the government to deal with identity theft. So I had that in my back pocket. I started going around. Completely stopped the way we were doing things in San Antonio.

I went out and gathered intelligence on who our bad guys were. They were, in fact, methamphetamine users and the Aryan Brotherhood. Those were our two principal-- and most of those were combined. Most people would not think that would be the group that's targeting this the most. But in fact, it was. So we had to know that.

Most of those folks had a high level of recidivism. So we went in and said, OK. We've got to change the way we do things. We went to the US attorney's office and started saying, hey, we have this very small group of people who are committing a very large number of these crimes. We have a program that we can use to reduce that. But your dollar losses are too high, and we've got to have a concerted effort in that.

We switched our hours. We quit working what I call banker's hours, which is law enforcement hours. We had to start working nights. It was a novel idea. Weekends. We had to start working the hours that our bad guys operated. They were usually out at night or very odd hours, and we had to get out there and be out there with them.

We started working closely with the narcotics units. Because a lot of what was driving the theft of identity was the use of methamphetamines. So we had to start talking to them. And again, we had to cultivate contacts in the hotel and in the motel community because a lot of them were hopping between these hotels. And they were also stealing a lot of the customer information out of these hotels. So that was a two-pronged approach on that, was to get in there and educate those people as well. And also they would let us know when somebody showed up they thought might be involved in all of this.

So the Identity Theft Enhancement Act, the 1028 is the best thing that ever happened to me in my career. Basically what this is in a nutshell is, if you knowingly transfer, possess, or use that lawful authority and means of identification of another person-- and there's a very long list of statutes that are available to this-- in addition to the punishment provided for such felony, daring in relation to any felony violation, be sentenced to a term of imprisonment for two years.

You got to go to jail for two years. There's no probation allowed on that statute. So it could be your first offense. And if you get caught doing this, you're going to prison. On top of whatever else you did. So if you went out and stole a checkbook, opened up an account, and basically committed what we called bank fraud, you would get charged for the bank fraud and receive a sentence for that. You would also receive the two-year sentence on top of that.

So what it did for us in San Antonio was that all of a sudden, this group that was running around and we were seeing all the time, they were getting four to five year sentences. Well, guess who I stopped seeing the next week, the next week, the next week eventually? Those guys. We reduced identity theft crimes, according to the police department, by 60% within our neck of the woods. Which was a pretty good, I think pretty good rate of success for that.

And again, a lot of it being on this particular statute. Because most statutes, you're going to-- and particularly with a financial crime, you're going to do what? You're going to get probably probation. You're going to be right back out doing it. This says, nope. You at least got to go to jail for two years. One of the Aryan Brotherhood lieutenants who was one of their executioners, we got for one check, one ID, and one gun, and he got 10 years. Probably would not been able to do that had we not educated the US attorney's office on the 1028 program and then got them to buy off on that.

And a lot of that was, they got rid of the loss-- we didn't have to have $100,000 loss to get the case accepted. Obviously on that case, we had one check, one ID. So they waived the loss factor for us. So again, there was a lot of coordinated effort into that.

A lot of this culminated into a case for me where we had the theft of data from a hotel, a very popular hotel in San Antonio. We started seeing customer portfolios on a lot of the search warrants we were running. We went into the hotel and said hey, are you missing some things? They're like, nope. All good here. Can we take us to the room where you keep it? Sure.

Go down there. Room unlocked. Open the door. Boxes of portfolios everywhere. Guy literally walks up-- the manager walks up, picks up one. He goes look, here, there, not here. Panic, starts looking at other boxes. Empty, empty, empty, empty, empty, empty, empty. Figure they stole about 17,000 customer portfolios. Customer portfolio had credit card number, had the back of the card imprinted on it, had the customer's name, had the customer's address on it.

So the Aryan Brotherhood had figured out where this was. And it's interesting. The toilet paper was more secure than the credit card information. True story. That sucker was locked up tighter than you could get into. That was not. They were going out and basically going on a publicdata.com and building identities off of that using this information.

The hotel was not able to identify or to send out notices to the victims. They had no idea whose information had been stolen. They couldn't comply with some of the state statutory requirements. So they just had a wealth of information to go out there. They were buying large dollar items with counterfeit credit cards using that information. Some of that stuff was being sold back to a cartel in Mexico. Just a huge mess caused by simply not sort of accounting for where your information was.

And so it's kind of a culmination of everything we've done between Secret Service and UT about protecting your data, and in knowing how to deal with it. As a side note to that, I'm almost done. 12 people went to jail in that case. One of them got out. They arrested him a couple of months ago. Guess what he had on him? 3,000 customer portfolios from the hotel eight years ago. It was his bank account, savings account. He just stashed them away and hid them. So that's it. That's a very-- sorry that's a very quick dive into it for 30 minutes. I appreciate your time. Thank you very much. [APPLAUSE]

ALANA BENSON: The green button? Hi everyone. So if you look at your agenda for today, you will see that my name is listed as Alana Benson. And it's also on that nice little piece of paper over there. And it's also on my birth certificate. That's it. I was born in the state of New

Hampshire. And with all of that information, it should be pretty clear that I'm who I say I am. But what if on your agenda, my name actually said something like Allison, for example?

This kind of goes to show just how little information birth certificates have for us. And I want to let you know that all of the birth certificates and the death certificates that you'll see in this presentation are completely real. They've all been obtained legally, and they are all certified copies with nice seals and signatures of people. There will be some fake documents though, don't worry.

Though I also want to really show you the right and wrong ways of obtaining these kinds of documents, because by the end of this presentation, all of you will be able to do it. So I really believe that identity is at the core of these issues. Now, we like to talk about fraud, and it umbrellas out into all kinds of different things. We have tax refund fraud and hacking and cyber security and data breaches.

But when it comes down to it, identity is at the core of everything. It's who we are. And that's three of my central ideas here. So number one, identities are how agencies know us. So I say my name is Alana Benson. It's on the nice little pamphlet. And that's who I am, right?

And number two, agencies and institutions know our identities through documents. So you know that partially because I just showed all of you my birth certificate. And number three, documents breed other documents. So if I have a birth certificate, it makes it easier for me to get a driver's license. And then I can go and get a passport. The other thing too is that death certificates are incredibly helpful when you're trying to steal identities.

So now I live in Wyoming. And say I wanted to go and apply for a driver's license there. There's going to be four things that I'm going to need to get. The first is proof of my identity, which is something like a birth certificate or a passport. The next one is two pieces of Wyoming residency, which is pretty much anything that has my name and my address written on the same piece of paper. So any kind of mail or something.

The next thing is proof of my social security number. And we're going to talk about that more later. But that's something like a social security card or a bank statement or a W2, anything like that. And if I was going to move back to New Hampshire where I was born, I would need pretty much the exact same requirements. And if you'll notice, all of those things are real ID compliant. Now we've been hearing about the Real ID Act since 2005.

And the problem with it is it's supposed to be this bulletproof way of proving our identities. But I don't necessarily think that that's the case. And you might not either by the end of this. So these are what I like to call identity verifying documents, things like driver's licenses, passports, birth certificates, you know, things that have your picture on it. Except some of them don't.

Birth certificates have actually nothing on them to tie the person to the identity. So I show you any random birth certificate, and if the gender and a rough age is kind of close, you could believe that it's me. The other thing is that identity supporting documents prop up your identity. So

utility bills that have your address on it, pieces of mail, and W2s that have your social security number on it.

So how do I steal identities with documents? You've all thought about it, I know. So the first thing you're going to do is you're going to find an appropriate obituary from an open state. And I never thought I'd be talking about appropriate obituaries, but basically what I mean is that obituaries contain all the information you would really ever need to steal an identity. It has a full name. It has both parents' names, mother's maiden name sometimes, city and state where someone was born, all of that. And it's really unfortunate, but obituaries are a great place to start when you're looking for an identity to steal.

And the next thing that you look for is that these come from an open state. And an open state in terms of agencies is just something that is-- they allow certain information to be considered public record. So the problem with open states and birth certificates is that anyone can order anyone else's birth certificate, as long as you can provide the correct information, which you presumably got from your obituary. And we like to think that this is what open and closed states actually look like, but the reality is more like this.

So it's not as clear cut as we like to think. Because Massachusetts is technically a closed state, but I also have a birth certificate from that state. So other states like Illinois and Wyoming, for example, are more closed, but we don't like to put everyone in the fully closed category because you can still probably get a birth certificate from those places.

So your next two steps is that you're going to order the death certificate first. And that also tells you that you are ordering those from deceased people. And the third step is that you will use the death certificate to order the birth certificate. And you might wonder why you would do that. But that's because to order a death certificate actually requires a lot less information. So maybe the obituary doesn't actually list the mother's maiden name. Maybe it's just the full name, death date, and city and state.

So you go ahead, and you order the death certificate. Now, this is a death certificate for a girl who died as an infant in Washington State. She was born in 1990. And she also died in 1990. And that does tell us that she in fact died as an infant. You will also notice that there is a lot of other information that I had to redact on this. This also contains her social security number.

So you order this, and you can then use it because it contains all of the information, such as her mother's name, anything you might want to know. And you use it to order her birth certificate. The problem is that since she died almost 27 years ago is that when you order the birth certificate, it's marked as deceased. And that's because the Office of Vital Records has actually had time to go through and mark her death certificate and her birth certificate and match them together.

So on our second try, this is the death certificate for a young woman who died in Kentucky. And there is her social security number. This is really problematic because it essentially makes social security numbers public record as long as you can order them. Now, this was an interesting case

because I ordered this death certificate a couple days after the young woman died. I found her obituary, and I ordered her death certificate.

And then I waited. And I waited about three weeks. And I finally called them and I said, hey, is that death certificate coming? And they said, oh no. No. You're going to get it in, I don't know, a little while. It takes us three months to actually receive the death certificate.

So that tells me that if I order her birth certificate and maybe hope that they don't need the mother's maiden name perfectly correct-- and in a lot of cases if you make a mistake on your order form, they'll send it to you anyway-- they'll send you the birth certificate. And it will not be marked as deceased. So now I have a birth certificate. It's not marked as deceased. It matches my description. And I also have her social security number. So I'm well on my way.

My next step is to create my identity supporting documents. And this is a lot easier than you'd think. And these are actually fraudulent. So I have a Wi-Fi bill, and it has my actual address on it. And I just uploaded it into my computer, put a white text box over my name, and wrote Heather, which is the name of this identity.

I also used my actual lease, and I hadn't signed it. So I just wrote her name. And that is my second piece of proof of residency. That, and the Wi-Fi bill. And then the last thing is that I downloaded a W2 form. I filled in her social security number, my address, her name, and a matching EIN number and employer. And that's all of a sudden a couple steps towards tax refund fraud.

So you can start to see how document fraud can really affect every single agency. And it's not just documents. It goes out into every silo that we're going to be talking about today. Though, is anyone actually doing this? Yes, they are.

So this is an Amazon screengrab for a book called The Paper Trip 4. It is pretty much a guide on how to commit this kind of fraud. It has all kinds of information on ordering social security cards, each state that you can order a birth certificate for and what number to call to do it. So it pretty much outlines every single step you would need to take. And that's on Amazon, if you would like to order it.

We also have so many examples of this actually occurring. But one of the most recent that we've heard about is in May there was a man in Massachusetts who was wanted for drug charges. And he fled to New Hampshire, where he ordered a birth certificate of a man who died back in 1994. And he then used the birth certificate to get a driver's license, and then used that driver's license to get a job, where he worked on the Portsmouth Naval shipyard, where they repair nuclear submarines. Now, he didn't actually do anything. He just wanted a job. But at the same time, you can see what kind of access and enablement comes from having a false identity. It can pretty much open doors for you wherever you want to go.

And as with all fraud, as we talked about with statistics, we never really know how much is happening simply because we only know how much is reported. And usually infants, the deceased, and the elderly are not reporting. But isn't someone checking on any of this? Though

you may have heard of the CSI effect where we talk about in courtrooms how after watching CSI, a lot of the juries will demand a ton of DNA evidence that doesn't necessarily exist.

And a lot of that happens here. We like to think that if you go and apply for a driver's license, that someone is actually checking. And the way that they would do that is by checking the partial Death Master File, which we'll get to. But oftentimes the verification doesn't actually happen. So we have it in our minds that it's going on, but it doesn't necessarily actually happen.

So we really have to thank the SSA. And this might sound like an aside, but essentially the way that we're going to understand death data is to go all the way back to the social security number. So socials were invented to keep track of all of the SSAs' beneficiaries. And that's all it was. It was just a tracking system.

And then suddenly people come in, and they start using it for other purposes. They say, hey, this works great for my agency. But the problem is, that was never the case. Social security cards used to be labeled not for identification. And now they've pretty much just given up because everyone does label it. It would be like if you went to your neighbor and you asked to borrow a muffin tin because you wanted to bake muffins and then got mad at them when you didn't end up with bread. It's the same thing. You can't get upset with them because it was never that intended purpose.

So the same exact thing that happened with social security numbers is happening with the Numident. And the Numident is the SSA's record of death data. It's pretty much a big list of everyone's name, social, and whether or not they've died. Now that file was extracted due to Freedom of Information Act request into the full Death Master File, which is what six federal benefits giving agencies use to check death data to see if people who they're paying are actually deceased or not.

Now this was extracted into what's called the partial Death Master File. And because of the Social Security Act, it forbids sharing state reported data. So a new database was created which excludes roughly 11 million deaths. Now, why does any of that matter? Why does the partial Death Master File matter?

Well, aside from the six federal benefits paying agencies that you see in red, there are a whole bunch in blue and more that have to check this kind of subpar database full of death data. So things like Homeland Security and the Justice Department, and even the Treasury's do not pay list. They're all checking the Death Master File that doesn't actually include all the deaths. And we can't even verify how incomplete it is because a lot of it is not getting verified.

Again, we really see how this affects every single agency. Now a way to easily understand this, because it is a little nebulous, is we're going to use benefits to track data. Now, this is a true story. It's about my grandmother. She was born in New Jersey, and she died in New Hampshire.

Now, New Hampshire vital statistics reported her death to the Social Security Administration. They say, OK. We have her death. Records it on the Numident. And then stops her payments. Now her death was extracted from the Numident and then recorded on the full Death Master

File, the one that those six agencies get to use. But because it was reported by New Hampshire, which is a state, it is not included on the partial Death Master File.

And we see this come around as a problem because the New Jersey Department of Pensions continued to send her checks because they don't have access to her death data. So when they go to check and see if they should stop sending her payments, her death data isn't there. This trickle down is really problematic because we can immediately start to imagine how many improper payments are being sent out.

Now, this is all very depressing, I know. But there is good news. So there is legislation going on as we speak. It is going through the Vermont governor's office right now. Today, actually. I checked this morning. Vermont's H111. Now this is a bill that would move Vermont over from being a fully open state where anyone can order anyone else's birth certificate to a state where you'd have to use identification.

And no, it's not perfect. It is not bulletproof. But it's certainly a step in the right direction. And it shows that in 2017, as Sean was talking about, documents are very, very important. This is a letter from the Social Security Administration-- the ones who continually get blamed for all these problems-- not only stating that under current law, we are not authorized to share state reported data, which despite maybe wanting to, their hands are pretty much tied.

They do call out that in the president's fiscal year of 2017, there's a proposal that would grant them the authority to share all the death information, including data from the states. Now, we don't necessarily know what's going to happen this year. But it is also a huge step in the right direction to see that Social Security is standing up for themselves saying, hey, we really can't do this by law. But also, we know it's important, and we're lobbying for it. So that's a good sign to us.

And the way this all connects back to documents is because if we can't share death data, especially state reported death data, which is predicted to increase in the coming years, then how can we possibly verify identities with any real certainty? How can someone know if I take Heather's death information that I'm not her? If I present any number one of the birth certificates that I have, that I'm not any of them? And that's where we see this affecting identity theft in general.

So I have a whole bunch of really scary birth certificates and other documents. If any of you would like to see them, it's much more powerful to see them in person, non-redacted, than on a screen. Then please come and see me afterwards, and I'll show you. So thank you so much.

[APPLAUSE]

JOHN KREBS: So we're going to keep moving, and we're going to welcome up our next panelist from our Office of Technology, Research, and Investigation.

DAN SALSBURG: Hi everyone. I'm Dan Salsburg from the Office of Technology, Research, and Investigation at the FTC. And this is Tina Yeung, who is the lead technologist on a study

we're going to talk about. So late last month, a database of sensitive consumer information appeared on a site frequented by identity thieves. But this wasn't the typical data dump of sensitive data. In fact, I have a surprise for the ID thieves out there who attempted to use this data. The FTC created and posted the database, and we tracked how you used the data. That's right, ID thieves. You were part of a study.

So what did we do? We created a database of about 100 consumer accounts. We posted the data publicly, and we tracked the use of the data. I'm going to briefly describe the setup of the study. And then Tina, the lead technologist on the study, will discuss the findings.

First, we created a realistic looking customer database containing six types of information. Names. These names were based on common first and last names found in the US census data. Addresses that were geographically distributed across the United States. Phone numbers that had area codes aligning with the addresses. Email addresses at four popular web-based email services. And we used common naming conventions for the email addresses.

Passwords. Two things to note about the passwords. The first is, in the dataset, we did not identify what the passwords were for. We didn't identify that they were for the email accounts or payment accounts or just passwords for something else. Second, most of the passwords were incorrect. Meaning if someone tried to log on to either our payment accounts or our email accounts using these passwords, they wouldn't get anywhere.

But for a subset of the accounts, the passwords were real. But for those accounts, we activated two-factor authentication. And so each email and payment account was protected by either a wrong password or two-factor authentication. The last piece of information included in the dataset was payment mechanism. For each fake customer, we assigned a credit card number, an online payment account, or a Bitcoin account. We set up all these payment mechanisms in a way that limited the ability of the identity thieves to actually make any purchases.

After creating our database of fake consumers, we posted the database on a website that hackers and others use to make customer credentials public. This sort of data can be found in a variety of places, such as the dark web, hacker forums. But we posted it on a publicly viewable pay site. And we posted the data twice, first from April 27, and then one week later on May 4. And we ended our data collection on May 10.

The two postings of the data had similarities and differences. First, it was the same data. So posted on April 27 and May 4th, we posted the same customer files. But they're posted using a different format and at different times of the day. A Twitter bot that monitors the paysite for postings of credentials and then tweets about it to followers tweeted about our second posting, the May 4 posting, but did not tweet about the first posting on April 27.

Posting one on April 27, that was viewed 100 times. The second posting was viewed more than 500 times. We then monitored the data for three weeks. The first week was actually monitored before we posted any of the data at all. That was our pre-study control period. Then we monitored the data after the first posting, which we'll refer to week one in subsequent slides. And

we also monitored it after the second posting, which we refer to as week two in the subsequent slides.

We logged email account access attempts, payment account access attempts, credit card attempted charges, and texts and calls received by our phone numbers. And Tina is now going to describe what we saw.

TINA YEUNG: Thank you, Dan. The first thing we looked at is how long it took identity thieves to attempt access to an email, payment [INAUDIBLE], or make a purchase attempt. After the first posting, it took an hour and a half before the first attempt to access an account. While after the second posting, it only took an identity thief nine minutes.

Due to logging methodology, we're fairly certain that the first attempt after the second posting was a direct effect of the second time we posted, not the first. Next, we looked at the total number of unauthorized access attempts over the course of our study. The x-axis shows the pre-study time period, the week leading up to our posting, as well as the time period after our first and second postings. The y-axis shows the number of attempts. Note the spike after the first posting and a much more dramatic increase with over 1,100 access attempts in week two.

We also looked at the percentage of our fake consumer accounts that identity thieves attempted to access. This graph shows that identity thieves attempted to log in to over 97% of our email services, make charges to over 97% of our credit card numbers, and log in to over 90% of our payment accounts, although with our payment account we're fairly sure that it may be an underestimate due to our logging methods.

We also looked at the account activity by day. The x-axis is a timeline starting shortly before our first posting and going right until the end of our study. The y-axis shows the percentage of accounts identity thieves tried to access by day. Email services are shown in blue. Credit card numbers are shown in red. And payment accounts are shown in green.

For instance, by looking at the red bar on May 4th, you could see the identity thieves attempted to access all of our payment accounts on that day. I should also note there our two postings are highlighted in gray. We also wanted to look at the identity thieves' attempts to access our email accounts by entering the passwords that we presented in our fake consumer database.

In total, there were over 500 attempts to access our email accounts over the course of week one and week two. The other thing of note is a single access attempt in the pre-study, which could have resulted from a number of reasons, such as an actual consumer entering a type to more nefarious brute force attempt.

What additional information could we glean about identity thieves from the data? For three of the four email service providers, we were able to get IP addresses of the identity thieves. So this graph underestimates the total number of IP addresses. The x-axis shows the number of attempts, possibly including multiple attempts to the same account, while the y-axis shows the unique number of IP addresses. This graph shows that most identity thieves try four or fewer times, and at that point probably realize that credentials didn't work.

On the right hand side of the graph, there is an outlier where 44 attempts were made from one unique IP address. So basically, this graph shows one of two scenarios. One, either identity thieves only try a few attempts before moving on, implying a relatively manual process of looking at data, or two, identity thieves frequently change IP addresses between attempts.

Speaking of changing IP addresses, we wanted to take a closer look to see if it gave us any information about where identity thieves may be located, as IP address might give us a rough idea of the country. So the x-axis shows the countries these IP addresses are supposedly from, while the y-axis shows the number of unique IP addresses. Ignore color coding for just a moment, it first appears as though most IP addresses come from the US.

However, we used a free service that assigns a probability that the IP comes from a proxy, VPN, or Tor exit node and found that identified over half of the IP addresses in our study as falling into one of those categories. This means that identity thieves often use these services, and that IP addresses reportedly coming from the US might actually be from anywhere in the world.

One thing of note is that just because the free service we use didn't identify the other half of IP addresses as not-- sorry. One thing of note is that though the free service we use did not identify the other half of IP addresses as not coming from VPN or Tor exit node, it does not mean that they did not. It just means that the service that we used failed to identify them as such.

We also looked at the credit card purchase attempts made by identity thieves. Some things we pulled out from the data of note was the maximum an identity theif tried to make in one purchase was $2,697.75. In just two weeks, identity thieves attempted to charge $12,825.53 to our fake customer accounts.

This may both under and overestimate the injury ID thieves cause had our credit cards actually been usable for a couple of reasons. First, it may both under and overestimate the amount because we noticed one identity thief's multiple attempts to purchase the same item for the same value at the same retailer in a relatively short period of time. If the card had worked, it may have emboldened this identity thief to continue making larger purchases, or they may just have stopped. We're not sure which.

Secondly, it also may underestimate the total injury because we saw pre-authorization charges from merchants. Typically these pre-authorization charges are lower than the full cost of the purchase. Other noteworthy attempts we saw our identity thieves attempt to make for purchases include attempts for online dating services, attempts to purchase at pizza places, and purchases attempted for hotels.

Next we looked at the price range of purchases being attempted by identity thieves. Along the x-axis, you could see the buckets that we created. And along the y-axis is the number of charges. This graph shows that most identity thieves make purchases for less than $10. We speculate that the small denomination charges may be attempts to check validity and marketability of the cards. However, as you can see along the right hand side of this graph, there are some outliers, such as the identity thieves who tried to purchase items for over $1,000 and $2,000.

Lastly, we looked at the types of products and services ID thieves attempted to buy with our credit cards. The x-axis is the categories we bucketed the purchases into, and the y-axis is the number of charges. As you could see, the majority of identity thieves made attempted purchases online. Other noteworthy things in this graph. The eight purchases to give to charity may not actually indicate the philanthropic nature of identity thieves.

Panelists at the recent FTC's give and take workshop on charitable giving noted that online travel platforms may be attractive for credit card for a variety of reasons, such as purchases can be made in very small denominations, and feedback is instantaneous, as charges are made immediately. Finally, we found it interesting that identity thieves made attempted purchases to fund their insurance and investment accounts.

DAN SALSBURG: Four additional thoughts. First, ID thieves are looking for consumer credentials and pounce when they find them. We can see this in how quickly they tried to access our accounts, just nine minutes after posting number two. Second, email and payment service providers could be monitoring the same sites that the ID thieves are monitoring and suspend accounts found on those sites. So ID thieves appear to be using a Twitter bot to alert them about the postings of credentials, and providers could use similar automated techniques and be a step ahead.

Third, our accounts with two-factor authentication established had an extra and effective barrier against ID thieves. This isn't to say that two-factor authentication is a cure-all, but certainly in our experience within the study was that it kept ID thieves from accessing our accounts. And fourth, one ID thief attempted to purchase the same item from the same merchant using 22 different payment mechanisms 22 times in a row. This really shouldn't happen. Merchants should have rate limiting programs or other things in place that should prevent this sort of serial purchases. And so we urge merchants to take a look at their policies on this.

In the future, we intend to analyze other data that we collected as part of the study, including email spam, text spam, the phone call data, and text data, and see if we can find anything about how ID thieves are operating through this data. Also, this study looked at ID thieves that troll pay sites for credentials. In the future, we are interested in studying other ways that consumer credentials are obtained by identity thieves.

If you are conducting identity theft research, please share it with us. And if you're interested in collaborating with the FTC on identity theft research, please reach out to us at research@ftc.gov. Finally, this work required the contributions of a number of people at the FTC. Without their contributions, we could not have done this. So we thank them. Thank you all.

[APPLAUSE]

JOHN KREBS: All right. Thanks Dan and Tina. We're going to take a quick break and come back at 11:00 for our panel on the dark web. There is coffee and some granola bars and cereal bars out there. Please help yourselves. If you want something more, there is the caf to the left, and I think we're going to put out some waters. Thank you. We'll see you back in a few minutes.