U.S. Department of Justice
Office of Justice Programs
Office for Victims of Crime

OVC
Webinar Transcript

Medical Identity Theft

September 17, 2012

Merry O'Brien: Okay, give me 1 second to turn it over to Tiffany. I am going to unmute her phone number here on the list. And I am just going to get, Tiffany, if you can chat me your phone number really quickly and I will go ahead…

Presenters

Tiffany Barrett: Can you hear me, Merry?

Merry O'Brien: Yes, I can, good. Okay.

Tiffany Barrett: I unmuted myself.

Merry O'Brien: You are on it, great.

Tiffany Barrett: So hopefully everyone else can hear me. Okay, great.

Merry O'Brien: Very good.

Tiffany Barrett: Well, thank you so much for this opportunity. We are just so happy to be able to talk to you about National Cyber Security Awareness Month (NCSAM). Just a little bit about the National Cyber Security Alliance (NCSA). We are a public/private partnership and we were started probably about, a little bit over 10 years ago. And our main objective is really to make cyber security simple so that the everyday person can understand what they need to do to stay safe online. Your parents teach you to look both ways before crossing the road, and so our main objective is really to provide those easy-to-remember tips when you go online to keep yourself safe.

National Cyber Security Awareness Month

Tiffany Barrett: And so, October is National Cyber Security Awareness Month. I am just going to advance this slide here. And just to let you know, too, all of these slides and information will be available. I will send it out to you. It has all the links that you need to know to get involved in National Cyber Security Awareness Month. And so, the main objective for National Cyber Security Awareness Month is really to get the message out around the United States about staying safe online. The National Cyber Security Alliance, one of our main objectives is really to help use our platform for all of the other objectives and events and initiatives that other people are doing during the month of October, and help them spread the word about their initiatives as well.

Week 1: October 1-5, 2012. Theme: STOP. THINK. CONNECT.

Tiffany Barrett: So a little bit about what we are doing. The first week is STOP. THINK. CONNECT, which is one of our main messaging platforms. It is basically to stop, think about what you are doing, and then connect online to make sure that you are being conscientious about the actions that you are doing. For example, if you are in doubt about a specific link, no matter who it comes from, throw it out.

Tiffany Barrett: So the Kick-Off Event, we are going to be in Omaha, Nebraska. And the event will be streamed live on Facebook, which we are very excited about. And then we are launching a Small Business Security Summit in Omaha. We will be releasing NCSA/McAfee Home Users

Study. And we will also have the STOP. THINK. CONNECT. Twitter Chat. And at the end of the slides you will be able to see how you can register and get more information about these.

Week 2: October 8-12, 2012. Theme: Cybercrime

Tiffany Barrett: Week 2 is about cybercrime with the Department of Homeland Security and the Secret Service. We have an event in Miami. And there is also going to be a State of Cybercrime Twitter Chat.

Week 3: October 15-19, 2012. Theme: Online Safety for Businesses

Tiffany Barrett: Week 3 is Online Safety For Businesses, and we are going to be ringing the opening bell for the NASDAQ. We will also have a panel discussion in New York City. We will be releasing another study with Symantec about small business. And we will also have a Small Businesses and Online Safety Twitter Chat.

Week 4: October 22-26, 2012. Theme: Cyber Security Education

Tiffany Barrett: And then the final week is Cyber Security Education. We will have events taking place in Washington, DC, and California, and Cyber Education and Digital Literacy Twitter Chat.

How to Get Involved in NCSAM

Tiffany Barrett: And so how to get involved. Anybody and everybody can get involved in National Cyber Security Awareness Month. We want to make it as easy as possible for anybody to get the word out. You can make the events that work for your company, that work for your organization, that work for you as an individual. You do not have to do events. You can just send a Tweet out. You can be considered a Champion of your organization. If you want to be a Champion, what we will do is post your logo and link online and just kind of promote all of the initiatives that you are doing to show your support for National Cyber Security Awareness Month. You can download "Get Involved" sheets, tip sheets, post tip sheets around your organization so that people can remember to keep a clean machine, "When in doubt, throw it out," own your online presence, and other tips that we have about staying safe online. You can follow some of these links to participate and register for our Twitter Chats as well.

NCSAM and Social Media

Tiffany Barrett: And we also provide easy ways to send out Tweets and Facebook and kind of spread the he word on your behalf. But, like I mentioned before, one of the things that we are more than happy to do, any of your initiatives in regards to identity theft, anything that you would like to get out, we would be more than happy to use our platform to help disseminate your message. We have over 350,000 fans on Facebook. We also post things online. So to help sort of bring your initiatives forward and have them be online and have us promote them for you, we are more than happy to do that. And you can just...They will send you my contact information. You can reach out to me if you are interested. And we are definitely more than happy to get your message out because we know that so many people are doing so many wonderful things and we want to make sure that we help you in any way that we can. So that is October.

Tiffany Barrett: I also wanted to give a quick mention about Data Privacy Day, which is held on January 28 every year. And it is a celebration of the Convention 108 in Europe as the signing of Privacy as a Fundamental Human Right. And so, in 2007, they asked the United States to take it

over. So what we do is we celebrate Data Privacy Day in a similar way as National Cyber Security Awareness Month. But it is also another opportunity for your organizations to get the word out about what you are doing in regards to identity theft, and use our platform as an opportunity to get your word out as well. So if anybody has any questions, I am more than happy to answer.

Merry O'Brien: Okay, thank you Tiffany. I do not see any in the chat now, but feel free, anyone, to ask some later and I can...If you want to stick around for the presentation, we will do Q & A as well at the end. And I can also e-mail those questions on to you if people think of them later, too.

Tiffany Barrett: Great. Thank you so much. I really appreciate it.

Merry O'Brien: Oh, yes, thank you for coming. We will definitely be re-Tweeting you on our site throughout the month as well, too, so.

Merry O'Brien: Okay, I am going to now pass it over to Pam Dixon. And Pam, can you unmute yourself, please? We will give Pam a second here. All right. And, Pam, you can also chat me your number and I can unmute you manually, too, if you are having trouble with that.

Merry O'Brien: Okay, and while we wait – while we wait for Pam, we do have a question for Tiffany here. Do you highlight startpage.com to avoid having a tracking mechanism when doing searches on the Internet? Okay, and Tiffany might have to unmute herself.

Tiffany Barrett: There we go, great. One thing, we do not promote any products or services. But if a company like startpage.com wanted to become a Champion, one thing we are more than happy to do is highlight them on our page to promote, you know, what they are doing in regards to having kind of the Do Not Track mechanism. Because there is definitely a lot of companies and organizations that do things like that that are planning on being Champions as well.

Merry O'Brien: Thanks, Tiffany. And I think, Pam, we have you up and Adam now with the audio as well, so you can go ahead.

Pam Dixon: Hi, this is Pam. Can you hear me?

Merry O'Brien: Yes.

World Privacy Forum

Pam Dixon: Okay, great. Hi, I am Pam Dixon. I am Executive Director of the World Privacy Forum. Thank you all for joining me today, and thank you so much to the Network for your kind invitation. I really appreciate the opportunity. I met everyone when I gave a presentation in Colorado and it was really a nice experience for me. I learned a lot and I really – I was just incredibly impressed with the quality of the folks there. So if you attended my talk in Denver, some of this might be a little bit repetitious. However, there is also some new information. If you did not attend that, I hope that this is all very fresh and new for you and that this information is helpful for you. I am happy to take questions as we go along. So, Merry, please feel free to interject at any time, any questions that start coming through on the chat.

Medical Identity Theft: Surprises the Newest Research Reveals About Detecting, Preventing, and Curing Medical ID Theft

Pam Dixon: The presentation today is divided up into a couple of segments. And basically, what we will be doing is we will be defining what medical identity theft is. Then we will be talking about the harms from medical identity theft. And, Merry, if you could, please advance the slide to number 3. There you go.

Overview: What We Will Be Discussing

Pam Dixon: We will be talking about how the crime operates with a real focus on kind of methodologies, the, you know, how does this get [rooted? routed?] into the system, and what it looks like geographically. And look at those patterns and see what those patterns tell us about detecting the crime and preventing the crime. And then finally, we will close with a discussion about: Can medical identity theft be cured? What are the right things to focus on? Including dealing with some of the really thorny HIPAA issues in relationship to that.

Pam Dixon: And before we start, I just wanted to let you know that I am available after the presentation to ask any questions that you have. If you go to our website, www.worldprivacyforum.org, we have a lot of medical identity theft materials that you are very welcome to look at. We touch these a lot. We just recently, within the last month, republished our entire Medical Identity Theft Victims Frequently Asked Questions. And we update it sometimes twice a year, sometimes once a year. But we put all of our current knowledge into that. So please – please take a look at those materials and use them as you wish. Our contact phone number and e-mail is on the website. And those are good. We actually have a person who answers all of that. We also have a Twitter stream and a Facebook page, I think like everyone else now. And we are happy to work with you via those methods as well. So let us go ahead and begin.

Overview: What is Happening Right Now

Pam Dixon: So, what is happening right now with medical identity theft? This – this crime really came into the fore, at least for us, in 2005. And what happened is, actually, I was asked to testify before the National Committee on Vital and Health Statistics. It is a really wonderful Congressional subcommittee. They are very thoughtful. And I was asked to look at what are the risks in electronic health records and in what was then called the National Health Information Network. And the Chairman gave me way too much time to prepare for the testimony. So I did too much. I did too much research. And the outcome was, as I was sitting there one day going, "What is another risk I can talk about? What else is there?" And it just came into my mind that, "I wonder if there is such a thing as identity theft within the medical sphere." And I Googled the term, "medical identity theft," and nothing came up. It was one of those things where there were zero results. It was amazing. And I thought, it has got to be there.

Pam Dixon: So I went onto PACER, which is the online resource for looking at court documents. And I immediately found a couple of cases dealing with medical identity theft. And I thought, "Okay, I am going to write about this and really start to talk about this in terms of, you know, a risk in electronic healthcare records because it really looks like that is the case." It was all quite preliminary and very early, but I testified and the Chairman of the committee said, "Look, you have got to do more research on this. No one knows about this. No one has ever talked about it." So I spent a very long time actually researching the very first report, published it in 2006, and there was only one goal of that first report in 2006. It was to really say, "Hey, there is something called medical identity theft, and it exists." But that was then and this is now.

Pam Dixon: Right now, I think that many people know that medical identity theft exists. And what is happening right now is that we are learning a lot about the crime and we are having to

look at little pieces of the crime in order to look at the bigger picture of it. So that is kind of my theme of this talk is, by learning small things, we can often learn something bigger. And that is what I hope to do with you today.

Pam Dixon: So one of the things that I have really learned about this crime is that there are four primary viewpoints of this crime. The victims have a view. Healthcare providers have a view. Law enforcement has a view. And insurance companies have a view. And these views often overlap in very beneficial ways. It is just a matter of learning to talk to one another. Next slide, please.

Section 1: Defining Medical ID Theft

Pam Dixon: So, what is medical identity theft? Next slide, please. Medical identity theft in our definition that we have developed, it is, "Medical identity theft is when an individual uses a person's name and sometimes other parts of their identity without consent or knowledge to obtain medical services or goods, or to make false claims for medical services or goods. Medical identity theft frequently results in erroneous entries being put into the existing medical records, and can even involve the creation of fictitious medical records in the victim's name." Now, that was an early definition. It has held up very nicely. This is the key definition and core definition of medical identity theft. And I know that some other folks do include other parts of identity theft. So, for example...If you could advance to the next slide, please. So, for example, we do not say that if someone takes, for example, a person's health file and goes to a local mall and has a shopping spree, we actually do not consider that a form of medical identity theft. We think of that as financial identity theft. And I will explain why in a moment.

Pam Dixon: Basically, though, the rule of thumb is this. Think medical files, not shopping sprees. And here is really, for us, the watershed defining line of medical versus financial identity theft. In medical identity theft, the remedies that a victim has available to them are completely different than the remedies a victim of financial forms of the crime have available to them. So, for example, if a person has their identity stolen and it is used at a healthcare provider to provide services or goods in their name, that individual is going to have to use HIPAA, to some degree at least, to work with getting their files and finding other remedies to correct the errors that were introduced into their healthcare file. They may use the Fair Credit Reporting Act a little bit if that – that theft also has a financial aspect to it. But the – the harm is primarily going to be residing under HIPAA, a little bit under the Fair Credit Reporting Act. If a person had gone on a shopping spree and, for example, had used that information to open credit cards, to open, you know, lines of credit at the various stores, the remedies are all under the Fair Credit Reporting Act, and the various identity theft prevention acts, freezing of a credit would be helpful in that situation. So there are just very, very different remedies.

Pam Dixon: Having said that, something that has become quite apparent from looking at the victim kind of methodology of this crime is that people who are victims of medical identity theft are also often victims of financial forms of the same crime. So it is a – it is a combinatory crime and it has a lot of working parts. Next slide, please.

Pam Dixon: I am often asked, "How is medical identity theft different from healthcare fraud?" The individuals who usually ask me that question are people who work at insurance companies or people who work within the healthcare professions. And they have seen this for a long time, but they just have not called it this. And here is the truth. Medical identity theft is definitely a subset of healthcare fraud. The only thing that is different is there – is there are a couple of key differentiators in the crime. The harm to the victim is profound and it is protracted. It lasts a long

time. The recourse for the victim is quite limited in scope, and the legal remedies are thorny, at best, for the victim. Now, for healthcare providers it is a completely different set of issues. But medical identity theft is really, it is just a subset. And we primarily look at it from the victim's point of view. And most of our research has been in the area of trying to find remedies for victims, and also for healthcare providers in cleaning up the folders, the file folders. Okay, if you could advance the slide, please.

Pam Dixon: There we go. So one of the things that we do each year is that we make requests to the Federal Trade Commission (FTC) and to other federal agencies for raw data. And what we are looking for is we are looking for consumer data about the crime. And we are trying to figure the crime out. And the Federal Trade Commission has been extremely generous with us, and they give us literally tens of thousands of pages of consumer complaints. They spend a lot of time redacting them so that we do not see personally identifiable information, but we get the narrative comments so we can really look at the methodology of the crime. And they are also...They retain the city and state and the providence of the complaints. So it is incredibly helpful for us in both seeing the methodology of the crimes and also mapping the crimes. So this consumer complaint that you are looking at is an older complaint. I did not include any of the newer ones because we are actively going through them right now. But basically, this is an extremely standard complaint and I wanted to give everyone a flavor of the kind of complaints that consumers make.

Pam Dixon: So in the comment field what you will see is the consumer reports incidents involving medical care. Consumer states that there is a suspect and that the suspect relationship is unknown. In other words, in this particular case, they knew someone had done this, but they just, they did not know who they were. The consumer has not yet contacted any of the credit reporting agencies. That is very typical. Consumer has not contacted law enforcement. That is also typical. The consumer reports non-monetary harm. The method of obtainment was that they had access through a relative with the consumer, and the Internet was not used. But this is – this is a typical kind of complaint. The consumer will kind of be befuddled. They think something has happened. They have not gotten a bill yet but they are a bit befuddled. They are starting to get contacted. They are starting to have some negative consequences. And they come in various forms of negative consequences. I am going to move on to the next slide and it will kind of show you the progression of the crime.

Pam Dixon: In fall, 2003, my purse was stolen out of my car and my license, SSN, and some ATM cards were in the purse. I filed a police report—good—after the incident, and another one after checking my credit. I just found out that they are still using my SSN even though it has a fraud alert. So this was in fall, 2003. Now, an update in 2007, years later, the consumer states that the suspect has created eight medical accounts using her information at an unknown hospital. This is absolutely a very typical methodology for medical identity theft.

Pam Dixon: In the credit card world something that has happened is that we have these automated programs, like, for example, at Fair Isaac, they have an automated anti-fraud program. And these anti-fraud programs are made up of massive algorithms and computer systems, and they reduce fraud to an extraordinary degree with this smart machine learning. I believe the last time I talked to Fair Isaac about this program, they told me that the fraud rate was .02 percent. It was right in that neighborhood. That is a very, very low fraud rate. And it is in near real time. I know that all of us have probably had the experience of going shopping, maybe in a foreign country, or maybe for a birthday and maybe you buy a little bit more, whatever you have done, it is out of your habitual purchasing pattern. And you get a call on your mobile phone from the credit card saying, "Hey, is this really, you know, okay?" That is amazing. And it is quick. So a lot of us have been

trained to think, oh, you know, if something negative or deleterious is happening in my fiscal transactions, I am going to be notified of it.

Pam Dixon: Well, in healthcare, just the opposite tends to be true for a number of reasons. And it is not any one particular, you know, stakeholder's fault. But what tends to happen is that the consumer will get their identity taken or massaged or, you know, sometimes there are synthetic forms of identity theft in this area where just pieces of their identity are stolen. But no matter what, it usually involves an insurance number or an SSN. Sometimes it can involve just a name and home address. It is amazing how this crime has been committed, but no matter what, the crime, the person's information gets leaked out in some way. And then years later, usually over 2 years, the victim will discover that somehow there are multiple accounts in one or more hospitals. And sometimes even in one or more states in their name. Many victims have contacted us and have stated that they found out after seeking medical care and having a little surprise in that area. One woman, a very well-known victim who has been interviewed frequently in the media, was literally on a surgical table and found out in this way that she had erroneous medical information entered into her material. So this is a crime that has a very long incubation period.

Pam Dixon: So the bad part about that is, is that the consumer goes a long time without knowing they are a victim. And it is our conjecture that many existing victims are victims and still do not know it. And because of that, it puts a burden on all the other stakeholders, such as healthcare providers and insurers, to really work hard to prevent this crime from occurring. So we have touched on this already. Next slide, please.

Section 2: Harms from Medical ID Theft

Pam Dixon: So I want to edge more into what are the harms from medical identity theft. I think that you can already guess. One of the very first ones that we talk a lot about...Next slide, please.

Harms to Individuals

Pam Dixon: And that is that the key harm, above all, of this crime is that individuals' healthcare files are typically, and I can almost say always altered, but I cannot quite say it. But 99 percent of the time, the victim's health file is altered with improper or incorrect information. And this has an extremely negative consequence. Certainly one of the negative consequences is that victims really have a very tough time removing the improper information from their healthcare files due to a lot of complicating factors from the law. There currently—and I am asked this a lot and I can tell you definitively—there is absolutely no law which requires a healthcare provider or insurer to remove information from a medical file, even if that information is fraudulent. And there are a lot of reasons for this. And I will explain this as we go along.

Pam Dixon: Another thing that has happened to a number of people, and this is all from people that we have either interviewed, found the court cases for, or have found through...They have called us. What happens is also they have had changes to their insurance billing codes, which then populate health information exchanges without their knowledge. Some of them have their insurance caps reached. A number, a smaller percentage, but certainly a number of victims are contacted by collection agencies who are working off their credit report where they have medical collections. This can be from – just for a very small amount of money, under $100, or for staggering amounts in excess of $100,000. And, of course, this results sometimes in changes to insurance rates.

Pam Dixon: And then one of the problems that usually comes to us is problems of employment and also insurance. Sometimes law enforcement because there will be a record of drug-seeking behavior that the perpetrator has added to the victim's record. A number of people will go for employment, have a pre-employment background check, and get really surprised at items on their credit or items that are found even in their health file check for employers who do that. So it is a real...It can be a real life-altering experience for victims of medical identity theft.

Pam Dixon: People who are victims of financial forms of identity theft—and I actually have had that happen, actually on a few occasions. It is just simple stuff where I think, you know, someone in a restaurant once pilfered my credit card. It has all been kind of credit card based. These are…We have some really good laws that protect us from this, and also the credit card and bank systems are pretty alert at this point, too, you know, tagging with fraud and, you know, fraud alerts and red flag alerts and whatnot. So we are pretty used to having some good recourse. But medical identity theft victims, by the time they come to us, they have really experienced the problems of not having good recourse. The next slide please.

Harms to Individual Health Care Providers

Pam Dixon: So patients are not the only ones who are victims here. It is important to understand that healthcare providers, and insurers as well, can be real victims here. In this particular slide, though, I am talking about harms to individual healthcare providers. Doctors, we have found, especially in the last year, we found a number of cases where physicians have had their identity and TEA number stolen as part of this crime. And, of course, this – this puts them in a real ball of yarn that needs to be untangled and that usually takes a lot of time. They tend to be investigated for actually committing the crime, and it is just really tangly and difficult. And at the end of the ball of yarn, unbelievably, there are usually two ways that the healthcare provider has had their identity compromised. And one is just from a person, especially those with drug-seeking behavior, taking their prescription, a prescription, a legitimate prescription they got, and then duplicating that and then printing it, and then signing it and whatnot. It is just amazing some of the counterfeit that is out there. But this is an important thing to be aware of because it is definitely on the rise. And then…Next slide, please.

Harms to Institutional Providers

Pam Dixon: Now, there are also harms to institutional providers. And it is just...In the first report it was interesting. Some of the media called after the first report and they said, "Oh well, this kind of is a payback to the insurance companies for their prices and, you know, their bad attitudes." I had to really spend a lot of time talking with people and saying, "Look, this is not good for anyone. And we have got to really get beyond those attitudes that lead us to think that this is somehow okay to, you know, let an institutional provider suffer with this crime." It is not okay to pass the buck. And institutional providers, both healthcare providers and insurers, they suffer a lot of harm from this crime. There is reputational harm, legal feels, relational harms, and then the costs of what I call under-reaction and over-reaction. And it is really difficult for providers right now to find a balance in responding to the crime of medical identity theft. And I think that people are really grappling with that right now. And institutional providers are...I think there is a range of responses, but there are some just shining examples of providers and institutions that have just done an amazing job and more and more are really at it each day. But it is important to note that prior to instituting a harm reduction program, there is a lot of harm.

Pam Dixon: I wanted to talk about individual harms from medical identity theft and talk about what I call a tale of two victims. Next slide, please.

A Tale of Two Victims

Pam Dixon: Now, these particular...Oh, one more slide, please. These particular individuals are from the same geographic area. Those of you who were at the Colorado presentation will remember these. One person is from Boulder, Colorado. And it says, they report an incident involving medical care. Consumer is not sure where they are getting treatment using her information. Consumer states there is no suspect. The consumer has not contacted any of the credit reporting agencies or law enforcement. She reports, or they report no, non-monetary harm. They do not know anything. Basically, this is very typical. You see a consumer who is going, "Wait, wait, wait, there is something going on." And basically, I found out and was able to research what happened here. This was a hospital incident and it was happening to this victim in Boulder. So…Next slide, please.

Pam Dixon: So here you find kind of the conclusion of this and kind of the other side of this, and this was fascinating because we found this from checking through thousands and thousands of pages of FTC complaints. This whole situation unfolded in front of our eyes because of the way the complaints cross-referenced. Now, we, with our teeny tiny staff here, did this kind of human cross-referencing. I do not know of any program or procedure anywhere that is doing this kind of human cross-referencing of victims and – and healthcare providers. I do not believe it exists. I think we are the only ones kind of doing this thing. But here is what we found.

Pam Dixon: So, in Boulder, the caller was the admissions manager of a particular hospital, and reported an incident involving medical care. And, basically, this admissions officer reported that although they were located in Boulder, the person who wanted to get medical care was in Grand Rapids, Michigan. So really, you have a consumer who had been—a Boulder-based consumer—impacted by a medical identity theft in this region reporting. And then you have an admissions officer reporting. And it all links back to high activity in this region. And there – this is not the only complaint like this. There are many healthcare providers, many entities. And, basically, to untangle this ball of thread, all we had to do was make a few phone calls and we found out that Colorado, in fact, has a lot of medical identity theft complaints related to drug-seeking behavior. And we untangled it because enough people had made complaints to the Federal Trade Commission. Now, if people had not made these complaints, we could never have put this trend together. And in this particular case, this tale of two consumers, you can see how they are linked by the same pattern of crime. And I think that this exists in a lot of different places in the US. But because there is real no reporting methodology or procedure or standard in this area of crime, it is really difficult to track statistics and to track victim patterns. So, let us move into a little bit of the methodologies. Next slide, please.

Section 3: Methodologies: How it Happens

Pam Dixon: So I want to talk about, okay, how does this crime operate and what can we learn about it from what we know? Next slide, please.

Pam Dixon: So as I mentioned, we have requested literally tens of thousands of consumer complaints to the Federal Consumer...The FTC's Consumer Sentinel Database. And we have gone through them literally line by line and created a gigantic database of them. And we are working on the more recent years right now, and it has been made much easier by a very nice statistician we have brought onboard. What we have found is something we would not have expected. But the data has revealed that medical identity theft has some victim patterns that really did not trend with what we thought we were going to find, which surprised us. So, basically, many of the victim patterns is that you see over and over again people did not know the person

who had taken their data. Now, anecdotally we have heard from healthcare providers over and over again that most people who, you know, were coming into the emergency room were relatives and had given their license or healthcare card to a friend or a relative. That is what we had heard anecdotally. We also had heard that it was a lot of individuals who really needed healthcare and who had just stolen a purse or had committed a crime like that to commit the crime. That is really what we thought we were going to find.

Pam Dixon: We found a lot of the stolen purse in the FTC complaints. We did find also some of the roommate, relative, and acquaintance complaints, but mostly it was unknown, unknown, and unknown. And what we discovered is that the crime is, by and large, an insider process. It is not an outside or a familial process. And it is – the big numbers that you see in this crime, while healthcare providers definitely can see the kind of what I call the "one-offs" that are associated with this crime, it is much difficult to penetrate to the deeper layers to the crime which are more systemic. Can you advance one slide, please?

Section 1: Defining Medical ID Theft

Pam Dixon: Okay, so this is a slide I pulled from Section 1. I wanted to talk about the geography of where this happens. Basically, it happens in very clear, distinguishable geographies. Urban areas, the mountain west, and where Medicare and Medicaid hubs are. Next slide, please.

Pam Dixon: So in the next slide, this is actually an interactive map we have on our website, and if you hover, if you have JavaScript enabled and you hover over any of the dots, you will get a listing of the cities where medical identity theft has occurred, and the number. And you can see that Florida is just a gigantic hub of medical identity theft. That big red dot on Florida is the size of the crime. And that is particularly in South Florida, but as you can see, Florida is just a hotbed. And then you can see Chicago is a hub. And the eastern corridor. There is a strange large dot in Colorado/Denver/Boulder area relative to its population. Very large. And then, of course, Texas, Arizona, and Southern and Northern California are also big hubs. And this really corresponds to large areas of Medicare/Medicaid payment processing and those kind of centers. So this is, to people who work at CMS (Centers for Medicare and Medicaid Services), this is not a surprise to them I do not think. And I also think that this is not a surprise to law enforcement. If you look through the Department of Justice filings in the area of healthcare fraud, these are the areas that come up again and again. And what we found from really doing a long analysis of the DOJ (Department of Justice) records in combination with the FTC filings, and also in combination with some of the HHS (Health and Human Services) complaints, this is really a systemic crime that is committed in a more organized fashion. It is not random. And the people committing this crime tend to be well-trained, smart, and well, well-organized.

Pam Dixon: But this map, when we put it together, I have to tell you, we kind of looked at it and we were really surprised. We were not aware of how it would look before we put the data in it. And we have done a regression of the data based on the actual complaints year-by-year. And then we have a decade-by-decade regression and progression. And the data is remarkably stable, except it shows this same geography [unclear] by growing by about 3 to 7 percent a year. And the geography of the crime is remarkably stable in that these are the areas that are growing. It does not really, you know, you do not see, for example, a spot coming, then going, and then coming, then going. It just pretty much stays like this and then just grows in a very kind of stable pattern. Next slide, please.

Section 3: Methodologies

Pam Dixon: Those of you who have heard me present before know that I categorize medical identity theft operations into three categories, what I call insider, outsider, and takeover. And I will discuss those now. Next slide, please.

Section 3: Methodologies: How it Happens - Healthcare Perspective

Insider

Pam Dixon: So an insider, I am going to discuss this from the healthcare perspective, not the victim perspective right now. It is a lot easier to talk about it because so much of this is happening within the healthcare sector. So an insider would be...The prime example is the Cleveland Clinic, the Isis Machado case. So in this case, which probably everyone on the phone knows, is Isis Machado was a billing clerk who worked inside the Cleveland Clinic and she regularly exceeded her browsing limits. And what she did is she systemically downloaded a whole bunch of patient data electronically and passed it off to her gang member boyfriend who then sold it within his identity theft network. Both of them were caught, and Isis Machado allocuted and admitted quite a bit, and it is a fascinating case to read regarding medical identity theft methodology. And for those of you who are within the healthcare sector or law enforcement, it is an incredibly useful case study. We have done a very intensive analysis of the case study to see how she got access, to see how it could have been made better.

Pam Dixon: And, of course, Cleveland Clinic has done a lot to change their system. And I do not know, I do not work there. I have not consulted with them. So I do not know all that they have done. But it is my understanding that they have done quite a bit to improve the situation. And it was well over 1,000 people who had their records stolen in this particular case. So because the average crime payout for improper billing and for fraud in this area can be very high, the real criminals like to commit this crime to scale. They do not want one or two victims. They want 1,000. They want 100. Better yet, 5,000. So it is kind of a greed scenario. And the greediest get caught. The smartest, it takes a little bit longer and sometimes they can evade the law by, you know, doing various other techniques. One of them is what I call a clinic takeover. We will talk about that third.

Outsider

Pam Dixon: But for now, let us talk about another way this happens—next slide, please—which is an outsider. So there are what I call "one-off" situations. There are so many of these. When you go and talk to a healthcare provider, they will really talk a lot about these. And you can find a lot of good examples very quickly. So this is a one-off situation for how this happens. This is where you are going to have a direct list from the victim. And it might be with some consent involved, too. So, for example, we have a situation where you have a family member who steals a, or borrows, an insurance card. Or you will have, you will have, you know, someone break into someone's computer and get the information. But it is just one person involved.

Pam Dixon: And there are some very well-known examples. The Juliet Sample case. She was a roommate. She stole an ID. She went all over the place, you know, getting drugs in her roommate's name. Gave the roommate a lot of troubles. Joe Ryan, his identity was stolen in a work-related incident, and his coworker went and had all sorts of surgeries in his name. It was a huge problem for this guy and it took him years to get it cleaned up. In Utah, there is also a very famous case of a woman who, in another case, a woman she knew stole her identity and with such a drug-seeking problem. This woman's children were taken away from her and she finally had to go to the Attorney General's Office and do a DNA test to prove that this person who had done all

this drug-seeking behavior was not her. It was an incredible situation and it took a long time for her to get healed and cured. And, meanwhile, she had time, very traumatic time away from her children.

Clinic Takeover

Pam Dixon: And then finally, another major methodology—next slide please—is what I call the clinic takeover. There is a lot of these that occur and it is shocking when you first start to read about them. So one of the best case studies that I really like to study is the Dzugha case in Northern California. In this case, these were Russian Mafia and they had so much money and made so much money from this crime, they just simply would pick up and purchase a clinic and then offer free exams and free food and free rides to the clinic. They would pull in a whole bunch of Medicare and Medicaid patients, photocopy their IDs, and then bill in small amounts over the course of a couple of months. But they did it with a lot of people. So they made a lot of money in a lot of little places over time. And they made quite a bit of money. It was several million dollars. These guys got caught by a real savvy woman who noticed that her son's breathing treatments, all of a sudden she had 60 small payouts for these breathing treatments that he never got. So that untangled the ball of yarn. But other than that, these guys probably would have gotten away with it. And this is not terribly rare at this point. It is just hard to find because sometimes you have real doctors and real nurses taking part of it. Sometimes, as in this case, it was a blend of real doctors and people just pretending to be real doctors. It is an awful thing to even think about.

Risk to Note

Pam Dixon: In almost all of these cases, there is a risk I wanted to point out. And it is a really challenging issue to talk about because I understand both sides of it. So one of the things that happens in this crime, okay, so let us say that you are a healthcare provider and you have patients coming to you. What will happen is that healthcare providers can ask to see an ID to make sure the ID matches the patient. That is not a problem. But what has happened in a number of cases that have come to us is that some hospitals will take a palm scan and even have some DNA association with the actual perpetrator of the crime. So, for example, let us say—not mentioning any names of any healthcare providers—but let us say that a person has gone in and they have a stolen license or they have made a license from a person's identity. It is a really fantastic fake. And they are out there, trust me. What happens is that that ID gets associated with a biometric, with the photo, with the perpetrator. And then what happens is that when the victim, the real person comes along, it makes it enormously challenging for them to untangle the crime.

Pam Dixon: And the biggest risk that we have found with this is driver's license scanning. So if a healthcare provider is taking an ID and just scanning it, lock, stock, and barrel, what that is is really a criminal honeypot. It allows the individuals committing the crime and stealing the data to have a readymade driver's license scan complete with the biometric. And it is a real problem. I wanted to mention that risk because it is something that is under...I think under-evaluated, particularly at healthcare providers, and it is a very important thing to start considering. I think it is great to look at a driver's license, but scanning it really introduces some problems.

Pam Dixon: So I wanted to talk a little bit about forging identity credentials. Next slide, please. This is just a case, and there are many, many cases in the FTC data. And the case is about a person who is having an enormous amount of troubles because someone forged their driver's license and then went around and did all sorts of harm. And we are running just a wee bit short of time, so I am going to skip reading it. But this is, I just wanted to point out that if you have forged driver's license that becomes associated with a perpetrator and it is actually a victim's identity, it

is so hard for that victim to then go and correct their identity. And we have had to work with victims that are in this situation and it is just very challenging because it really gets at the core issue of, okay, how do you prove you are who you say you are? And it is actually very difficult when your identity has been calibrated to a criminal's. And especially your medical identity, with your blood type, and your allergies, and this sort of thing. And a lot of times, of course, the victim ends up looking like the criminal. So it is really a great idea for healthcare providers and insurers to have procedures on how to clear things up when this happens. And some hospitals have just incredibly positive procedures in this area. Next slide, please.

What Methodologies Tell Us About Detecting and Preventing for Healthcare Providers

Pam Dixon: So this is just some of where the—oh, sorry about that, I am on a Mac and this did not export correctly. But I have a better slide I can supply for you, Merry. There is a couple of key little edges where this crime can be detected and prevented. ID scanning is a risk, but if you can check an ID without the scan, it can really help; at least some of the one-off outsider kind of attack. Internal access controls is a really great place to assist in detecting and preventing this crime. And a risk assessment specifically for medical identity theft that really looks at some of the unique operations and methodologies of these crimes, it is incredibly helpful. Not many people know how to do this yet, but it is a growing area of specialty. Looking at any kind of third-party billing scenarios is especially important for this crime because that is where a lot of this occurs.

Pam Dixon: And then I think that it is really important to understand that certain geographies have a higher risk. So if you are in North Dakota, your risk is so substantially less than if you are in Florida. So if you are in a high-risk state, definitely you are going to need a different approach than someone in a very low-risk state. And even within some states, there is much less risk between cities. So if you look, for example, back at that map, the State of Washington is, in general, a very low-risk state with a couple of hubs for the Seattle area and the Bellevue area. But, in general, that state is pretty low risk, there are almost no complaints in that state. So you have to know your geography and really take a consideration based upon that. It can really help. And again, as you are looking at medical identity theft, and I know it is difficult, but you really need to look at any inside risks and really focus there because a lot of what has happened, that has comprised a lot of case studies, is there was an insider problem.

Pam Dixon: Now, I think a lot of us heard about this amazing hacking in Utah. And there are other huge medical database breaches now. Reporting is really key on this and I think that is under control. And I think that most healthcare providers and others have really good reporting policies now. But this outside hacking thing has become more of an issue as thieves have realized that this is a real, you know, it is a very cost-effective crime. And I see every indication that this – this trend will continue. Next slide, please.

What Methodologies Tell Us About Detecting and Preventing for Law Enforcement

Pam Dixon: Now, we know from the statistics and the kind of methodology here that this crime is happening in three categories. Polished criminals, or desperate kind of individual families, and then a lot of it drug-seeking. These are really the key areas. So those are the key areas to look at when you are creating a prevention regime. Of course, the polished criminals are the hardest to catch, and the easiest to catch are the most desperate people, which is just, you know, it is an awful situation, but that is the truth of it. We are finding that it is extremely common for – for us to get presented with victims who are having a multistate problem and a 1- to 2-year maturity

cycle is quite common. We have had...The longest running person we have had is 7 years and it took them 7 years to find their crime. I mentioned strong geographical patterns. This follows through all the literature. It follows through the Department of Justice cases, the FTC complaints, it even follows through the calls that we get from victims.

Pam Dixon: And then something that is very...Something that I think that all of us can really start to do some consumer education on is what victims can do for prevention, which is to have their documentation. Because a lot of victims, they will present to the healthcare provider with very little documentation of their own health histories. And if there is one thing I could change right now, if I could change just one thing for victims, it would be that everyone would have a copy of their current health file going back about 10 years. And if they have a chronic disease, just the highlights. Because, you know what? That would help everyone involved so much because there would be a real good baseline to help fix the file, and a whole lot of other very good things. But this is a very good area to look at for, you know, working with detecting and preventing. And then just very quickly, next slide, please.

What Methodologies Tell Us About Detecting and Preventing for Victims

Pam Dixon: What can be done? Oh, quick methodology. Yes, I am going to just skip over this a little bit due to time. The one thing I can say that I have not said already is that a lot of times if you look in newspapers and at advertisements, you will find advertisements for free healthcare clinics. And a lot of fraudulent clinics will actually advertise in this way. I can pretty much go online and pick out the fraudulent clinics, talk to them on the phone, and figure them out very quickly. But I do not think that patients are doing that. So those clinics that are legitimate that are doing tests and research and, you know, really acting as safety net clinics, it would be very, very positive for this crime to have a way of differentiating the real from the false. And I do not know all the answers in that area, but it is something that we are very, very actively looking at. Next slide, please.

Section 4: What Can be Done?

Pam Dixon: Okay. What can be done? So, first thing that can be done—next slide, please—is to really focus on the curing of the things that causes the most harm. And one of that is alternation of medical files, and the patient catch-22 of all that that means. Second thing that can be done is to focus—next slide, please…

Key Solution: Risk Assessment

Pam Dixon: Second thing to be done is to do a real robust risk assessment. A lot of people are using mobile devices, mobile apps, and other electronic devices and have a lot of health information exchange pilot projects. It is really important to conduct risk assessments, specifically for medical identity theft in all of these projects. Next slide, please.

Key Solution: Focus Inside

Pam Dixon: Another key solution is to be sure that you are focusing inside with browser controls and expanded accounting of disclosures, and some kind of checks and balances for that. And we have a lot of specific advice in that area. And just to understand that even if you are checking patient identity, it is not going to completely solve the problem. Next slide, please.

Key Solution: Ownership and Leadership are Key

Pam Dixon: Ownership and leadership is probably the most important key solution. We have found over and over again that healthcare providers and insurers and others who have an individual or a team responsible for medical identity theft really do well in solving this crime. And then I am noticing that the time is very short. So, Merry, if we could please get to the next to the last slide.

Merry O'Brien: And actually, Pam, we slated until 3:30, so you are doing okay.

Pam Dixon: Oh, okay.

Merry O'Brien: Yes. I think we have got about 10 left, so you are right on schedule. No problem.

Pam Dixon: Oh, okay. All right, we are good, yes.

Key Solution: Red Flag Fraud Warning

Pam Dixon: Red flag fraud warning, I love. We are actually working on a red flag fraud warning right now with a couple of healthcare providers. It has really eluded a lot of people for a long time because of the internal electronic health records systems. They are not really built for that. There are a couple of other issues with it. We believe we have found a triphasic approach to it. So putting a red flag warning at the – in the various user entries in the Epic systems and some of the other healthcare systems. So I think that we have found a really good workaround for this. But, in general, we think an incredibly important solution is to have a red flag fraud warning for people who have been victims of medical identity theft. And this is something that healthcare providers can do. It takes some workaround. And there is also some HL7 (Health Level 7) stuff that we are working on that will really help, too. So we think that we can put a red flag fraud warning in three areas of the electronic records. A little different with paper, but as people go digital I think we are going to have a nice solution. Next slide, please.

Key Solution: Procedural Checks

Pam Dixon: I think everyone knows about procedural checks and this just should be done as part of a risk assessment. Next slide, please.

Key Solution: Take the Patient's Side

Pam Dixon: Take the patient's side. This is so important with credit collections. There is a real problem that we have encountered in assisting victims. They will come to us and they will say, "You know what? I definitely have been a victim of identity theft. I have got a collector after me and when I call the hospital they tell me to go to the collector. I go to the debt collector and the debt collector tells me to correct it at the hospital." And, basically, the patients are really stuck in an endless catch-22. And what we have found is that in cases where the healthcare provider has had even a single person have responsibility for this issue, a lot of times it just takes a little while for that issue to get resolved. And it usually does take administrative support to resolve that issue. Next slide, please.

Key Solution: Control Anti-fraud Issues

Pam Dixon: Okay, so anti-fraud, and this is, for those who are on the line who are insurers and who really understand this, it is important to have really good anti-fraud controls that use the minimum necessary identity information. Basically, whenever you build an anti-fraud database,

just imagine that this database will be breached at some point. And then go from there and create the information in there. So much can be protected. So, for example, you can have access level controls. You can hash the data, encrypt it. You can do all sorts of things that really help this kind of data stay safe. And then next slide, please.

Key Solution: Attend to Networking Issues

Pam Dixon: Another key solution is being very careful of the networking issues. There is a trio, if you look at it, it will really help. Information integrity. Is everything correct? Access controls. Who can get this information? And then authentication. How do we know they are who they say they are? And then next slide, please.

Key Solution: Jane and John Doe File Extractions

Pam Dixon: The John and Jane Doe file extraction is a really great way. We just heard about this in 2007 in California. And since then, we have talked to a lot of healthcare providers who have, after the fact, instituted it. It works really well. Basically, what is done is that people will, if they have errors in their healthcare file, the hospital or healthcare provider will take that information out of the file and cross-reference it with the identity of the perpetrator. Or if they do not know the identity, they will give that perpetrator a John or Jane Doe unique file number. And that way the individual who is the victim has a clean healthcare file, and the perpetrator has a clean healthcare file of their self, and the healthcare provider has a way to map the data, which is something that they need. I have been asked a number of times if, you know, people should have the right to delete their data from a healthcare provider. And, you know, it is not that simple. Healthcare providers need to have a mapping of that data for their own auditing and quality control purposes. So this is a solution that keeps everyone happy and meets everyone's needs. It is a very good solution. Next slide, please.

Key Solution: Reporting Coordination

Pam Dixon: A lot of times there is a lot or reporting issues with this crime. Folks will not – victims will not report the crime. Healthcare providers and insurance will not report the crime. So it is a really helpful tool to set up a procedure and a policy. How is this crime going to be handled by us? If you are a law enforcement agency, how are we going to accept these complaints, and what is the followup? How do we work with other healthcare providers to map all of this to trends? These are all things that need to be hashed out over time. Next slide, please.

Pam Dixon: This is just an extraordinary victim story. And this is a situation where there was medical care involved at Palmer Hospital. There is a debt collector involved. There was financial service involved. They contacted their credit reporting agencies, but they did not contact law enforcement. This is just a mess of a crime. And this person shows up a couple of times in the FTC complaints. It just went on and on. And this kind of situation is just overwhelming for a victim. Next slide, please. And this slide was specific to Colorado, so I am just going to go ahead to the checklist for healthcare providers.

Section 4: Methodologies: How it Happens

Checklist for Healthcare Providers

Pam Dixon: So I really focused on healthcare providers here, but I think that this law is also really helpful for law enforcement as well. So the checklist would be, okay, do you have a risk

assessment specifically for medical identity theft in place? Do you look at IDs or do you scan them and save them in a database? What kind of protection is in that database? Is it hashed? Is it encrypted? Is there access level controls? Do you have tiered access and encryption to healthcare files? This is medical identity theft 101.

Pam Dixon: Who handles medical identity theft reports? And what information is taken from the victim? How is it coordinated within your institution? Who handles the curing of the healthcare file, and how are you going to do that? Are you going to do a John and Jane Doe file extraction? Are you going to give the victim an old copy of the healthcare file or a new copy? How are you going to handle the HIPAA requirement? It is pretty thorny.

Pam Dixon: Who handles follow-on record issues? So, for example, this – this could have spread through health information exchanges or just through the course of daily, you know, doing your job, to labs, to pharmaceuticals, pharmacies. It could have spread to other healthcare providers, surgeons, anesthesiology groups, and even – even further than that, especially if a person has a disease requiring a lot of assistance. Like, for example, a chronic illness of some sort or kind of a high maintenance or a critical disease. So these follow-on issues are issues that most victims really need a lot of help with and also most, actually, healthcare institutions.

Pam Dixon: Who interfaces with law enforcement, and how does that get worked out? To whom are you going to report this crime? Are you going to report it to the FTC? You know, who gets this? Are you going to report all of your cases in a batch to the law enforcement? Are you going to go to FBI? You need to kind of make those public. Are you going to...? Some hospitals work in tandem with other hospitals and insurance companies to report like crime sprees or trends. These are all choices.

Pam Dixon: Do you have training for collections in a way to help victims after a collection is made by a collection company? And then, how do you handle identity proofing after a problem has happened? It is very difficult when you have two people claiming to be John or Jane Doe. How are you going to handle that situation when it arises? Because it is kind of a matter of when, not if. So that is a checklist. And next slide, please.

Section 5: More Info

Contact Info

Pam Dixon: If you have questions or would like more information, we are based in San Diego. We are right downtown if you happen to be in the area, we are happy to meet with you or talk with you or e-mail you. We are consistently and pretty constantly looking at research in this area. So our information changes from time and we update. You are welcome to stay in touch with us on our Web page or our Twitter feed or Facebook. Any of those methods work. We update a lot. And I am very happy to take any questions. Thank you so much.

Q & A

Merry O'Brien: Okay, Pam, we do have a few questions here, and for those that might have some more, feel free to chat as we ask these ones. Okay, so the first question. Is it difficult to get the medical service providers onboard with the red flag warning when they are the ones who may have hired the insider?

Pam Dixon: Yes, that is a great, great question. Okay, so here is what we found in a couple of cases. If there is a sole proprietor or a small practice group, small physician practice group of maybe, you know, 12 or less, and they have hired the insider, it tends to be very, very challenging to get anything to happen because there is usually litigation involved. And in order to solve the problem, they have to kind of confess to a crime or at least to negligence. So we tend to find that the situation is greatly exacerbated by that. Certainly, the most famous case in this the Skodnek case in Boston where a physician actually stole his patients' identities. So when they needed their healthcare files to correct them, he was not going to give them their healthcare files. So it required a judge's order and an awful lot of work to get that handled. So, yes, it greatly complicates the problem. However, healthcare entities that are larger, you know, they tend to have a few more rules in place and the red flag...There definitely...I think that there are a number of healthcare providers that either have red flags, internal red flags in place, or are looking at it. We just talked to a healthcare provider in Northern California who has an extraordinary system in place. We just talked actually a couple of months ago to someone in Central California who is putting in a red flag system.

Pam Dixon: So these systems right now are all self-created. There is not a...You cannot go out and buy an off-the-shelf or precreated from a vendor, like a huge vendor like Epic, a red flag solution. There are healthcare kind of vendors that support these kinds of functions. So I think that this is something that is...healthcare providers are open to. And it is definitely growing in popularity. I think, though, that there are those circumstances, especially the smaller providers or the sole proprietors, if there has been a problem, not so willing. You are right.

Merry O'Brien: Okay, good. Okay, somebody is asking about the currently developing healthcare exchanges and how these new laws, you know, may affect victims.

Pam Dixon: Yes. That is a great questions, too. Healthcare exchanges, health information exchanges are really problematic for victims. So, for example, let us say that you are going to Southern California and you are in Long Beach and you are part of the new exchange down there. I believe, I think there is 27 emergency rooms that are hooked up to it. So if you are not watching, your information can be exchanged with 27 other—let us just say, for example, 20—other emergency rooms in the region. Meanwhile, if the person has compromised their identity and they are compromising your healthcare files in 20 other emergency rooms and you walk into any of them, you have got a real problem. There is a push in I know the State of California and some other states to actually weaken privacy laws so that it becomes less burdensome for health information exchanges to exchange data.

Pam Dixon: I think that one of the big problems that we are going to have to tackle is that, you know, we need to retain really good and reasonable privacy protections going forward so that as we go digital in the healthcare sector, and it is definitely happening right now, as we go digital we need to find a way to allow patients to exert control and to have just certain baselines of privacy. So I think that some of the shifts that are happening with health exchanges are challenging. And I do not think enough care has been taken for the problem such as medical identity theft. And, you know, the system is just being built right now and I am really hoping that we are in enough time to get some of these good controls built in as we are building it. The systems are about 20 percent operative in the US, at least, and I think we have some time to still work and get some changes made. So I am hopeful.

Merry O'Brien: Okay, our next question is about prevention. What suggestions do you have for individuals to prevent becoming victimized? And then another person is actually also asking what

would a victim, how should we advise a victim to go forward first? Is there a website that would be helpful to report and that sort of thing?

Pam Dixon: Okay, so let me answer the last question first. On our website, www.worldprivacyforum.org, there is a link to a medical identity theft page. And on that page is an FAQ for victims. It is extremely detailed and it really works for victims. We have sample letters and just a step-by-step of what you need to do to recover from the crime. And it is a really good application of current law. And both myself and Bob Gellman, who is just a remarkable attorney and writer, write it and update it. And it is...To get now back to the first question, what is the best tools for prevention. Right now there are a couple of really good tools for prevention. And the absolute number one best tool is to never interface with the healthcare system. And that is not a reasonable suggestion for most people. But that is how you could really go far to prevent a crime. The people who are at greatest risk for the crime are people who interface the most with the system, or people with kids, because kids are usually getting shots and getting, you know, a broken leg and things like that. So the demographics of the crime tend to be users of the healthcare system. That being said, you do not have to be to, you know, get involved, but it sure increases your odds.

Pam Dixon: Another really important thing is that if you can get a copy of your healthcare files, if every single person you work with can get a copy of their healthcare files before they need it, it would actually...It cannot prevent the crime, but it can prevent a lot of the harms from occurring in the first place. One of the things that is well known in this office is that when identity theft victims call, that are medical identity theft victims, one of the two things they always say to us—almost always—is, "I am not able to get a copy of my healthcare file now." And there are a lot of reasons for that. And, in some cases, it gets resolved without that ever happening. But it would really, really help that victim if they had a clean copy of their healthcare file. And I just cannot even...It is just incredibly important to establish baseline controls. And in cases where the healthcare file is polluted with a lot of misinformation, it is very subtle and really woven in there over years, it is quite challenging to clean out. It is like picking little, teeny, microscopic pieces of lint out of a haystack. But not one needle in a haystack, but, you know, thousands and thousands of pieces of lint. Some of the cases are like that. And they can even spread to other haystacks. So it is really important that a patient has a copy of their healthcare file.

Pam Dixon: Some patients have received benefit in terms of prevention or early detection by having credit monitoring. And it is the kind of credit monitoring that alerts you when -- to any incident when your billing address has been changed. It is very, very broad coverage credit monitoring. This can actually help victims. Sometimes there are reports within the FTC files, and also reports to us, and also reports in a couple of major data breaches as well where there is credit monitoring. People who have had their credit monitored will be alerted to when the billing address changes. And the billing address changing is actually one of the very frequently found modalities of this crime, so it actually can be a really good early detection tool. In terms of preventing, though, somehow shutting off your credit or, you know, keeping your SSN, you know, to yourself, it does not quite work in this area, especially for Medicare/Medicaid patients because their SSN is right on their card, and their card is usually copied when they seek service. So they are very vulnerable populations and very vulnerable to this crime. And I wish I could tell you that there were better prevention tools. But right now there is not. I am really very hopeful about the work we are doing with the red flag. And I am really hoping that that is going to help repeat and...I do not think it will prevent the first time. But I think it really help if we can get it done with the repeat offenses.

Merry O'Brien: Thanks, Pam. Okay, we have a few more questions. Would you mind staying for about 5 more minutes?

Pam Dixon: No problem.

Merry O'Brien: And I will attempt to get to all of them as quickly as possible. Somebody is asking if we can also forward the Machado case study. Any information about finding out more about that when we do the slides. So that might be something we can send along, some more information there. Somebody else asks, what is happening, what are other countries doing right now to combat this issue and help victims?

Pam Dixon: Okay. So we actually went and slogged around to a lot of other countries trying to figure out what was going on. And this goes from Japan to Singapore to Thailand to India to Europe and to Canada. And here is some surprising things we discovered. Number one, Canada has this crime. The UK has this crime. And some kind of countries in the Middle East have this crime. And also India has this crime to some degree. But, amazingly enough, this crime does not exist really in any substantive number in Asia, by and large, and in a lot of Europe. And there is a lot of reasons for this. One is there are different identity schemes in these countries. So, for example, in India there is something called an Aadhaar card. An Aadhaar card is a total ID card and it is tied to the fiscal transactions of that individual and the services of that individual. So you have people going in and getting these services and they just do not get the services. There is no need to steal a person's card. You get a little bit of what I call a shame. Shame stealing. So you will get some identity theft based on someone not wanting to appear to have a particular disease.

Pam Dixon: In Japan this crime is negligible. And it is not because they have ID cards in Japan. In Japan it is because there is more of a community function and the responsibility for crimes in the sector are set up so they fall on an individual doctor as opposed to a healthcare entity. So in order for the crime to be committed, the criminal would have to go through different steps and it does not work to scale as nicely. And in Europe, for whatever reason, the crime occurs in the UK, but not in other countries. And I can only assume it has to do with the structure, the payment structure, and some of the other things. But, in general, the North American countries...I do not know much about South America at this point. We have not done enough work there to be able to characterize the crime problem in those countries. But the primary place where this crime is happening right now is really in the North American region and the UK.

Merry O'Brien: Okay, are patient portals increasing the risk of medical identity theft? These will be required for stage 2 of meaningful use.

Pam Dixon: Right.

Merry O'Brien: This might be a specific question that you might need to give a little background for others on.

Pam Dixon: Okay, so I am not even going to get into meaningful use. Basically patients...Maybe I have to. Okay. So, under the American Reinvestment and Recovery Act, ARRA ITAC (Interagency Technical Advisory Committee), they funded...The Obama Administration funded a lot of new electronic, you know, modernization projects. And along these lines it required certain uses in order to qualify for that funding. So there are different stages of reaching the funding and different milestones. It is a very intricately involved system. One of the things is to create patient portals where they can access their various, you know, files. I actually think that this is probably going to end up being more preventive for patients than anything else because I know, for

example, in the financial sector, people checking their, people who have the ability and who do check their online financial statements catch discrepancies much – statistically much more quickly than others do. And I am very interested in seeing patients access their file and look at it. And I think that this is incredibly important because most patients do not take the time to go in and make a written request for their records. So my hope is that the patient portals will actually assist patients in having more and freer access to their files and to find the same kind of information sooner like it is happening in the financial sector, find the problems sooner.

Pam Dixon: That being said, I think that one of the real weak points in the patient portal is always going to be the patient's computer. So I think we are going to have a lot of data on the patient computer. And there is going to be a real need for what I call computer hygiene education in terms of having your files laying around on your computer and leaving your computer or iPad or mobile device around. So I think that is kind of a risk. But I would rather have that risk than have the risk of patients never seeing their – their data.

Pam Dixon: Now, one thing I have not talked about at all is identification really in the patient portals. Identification, in order to really identify a patient online, it takes a lot of data. And there are a couple of really interesting systems that help. I really like systems like the VA system that actually authenticates patients in person, and then gives them the ID and the online ID and allows them to operate online after that. That is kind of a luxury, though. That is certainly my preference. I think that that is actually a great situation. I think the worst case scenario with the patient portal and certainly the most risky scenario is that there is just a single factor authentication for an ID. That could be easily hacked. And I really am hoping that healthcare providers just go for a two-factor authentication and really high security standards.

Merry O'Brien: Great. Okay, oh, I have quite a few questions. Okay, Pam, do you mind hanging in a little bit longer?

Pam Dixon: Sure.

Merry O'Brien: Okay, and for those who do need to go, feel free, of course, to sign off, but it is a very popular hot topic here, so we will take a few more then. Okay, what can victim advocates do to have good policies in their jurisdictions to help victims clear their records?

Pam Dixon: So one of the most important things is to help victims clean up their healthcare file and to help victims clean up their collections, if there are any collections. These are the two most challenging things for victims. The third most challenging thing is if the perpetrator has had a lot of drug-seeking behavior. They are going to need assistance with making sure that law enforcement knows that they are a victim and they are not a perpetrator. And this can really run to everything from arrest records, cleaning up arrest records, to making sure Child Services is not improperly investigating a person for drug-seeking behavior when it is not them. So those are the primary areas this happens.

Pam Dixon: Now, there is a real problem with victims of domestic violence. A lot of those victims...We have worked for a long time with the National Network to End Domestic Violence on healthcare privacy issues. And one of the things that we have found in working with those trainers is that sometimes the abusers will have really excellent access to the system. In that case, what needs to happen for that victim is they really need to work with an excellent, probably right now, a really good nonprofit who can go to the healthcare provider administration and really intercede on their behalf. It is a very thorny, tricky situation and basically what needs to happen is that those, you know, the abuser needs to have highly restricted access to those files. And this has

come up quite a few times. So this is a really important thing to watch over. But other than that, most, barring that special circumstance, most victims really need help with getting their healthcare files cleaned up and getting the fictitious entries, you know, removed or separated from the real entries. Of course, it really helps when you have a healthcare file record. If you do not have that record, sometimes you have to just start from scratch and say, okay, let us find out my blood type. Here is a history. Here is the medications I am on. Sometimes a medical history has to be rebuilt from the ground up.

Merry O'Brien: Thanks. Okay, well, everyone, I am going to ask Pam one more question and then I am going to refer everyone else to her contact info that will be on the slides we will provide after that so I do not keep you too long. But one last question. Have you worked with the Senior Medicare Patrol, SMPs, before? Have you been educating them and that sort of thing?

Pam Dixon: Actually, no, we have not. This is something that we are very interested in doing. We actually are seeking resources and contacts so that we can work with seniors. Because seniors are at a very high risk. We have written material especially for seniors. And we are very good about distributing it in our local area. We are preparing an online bookstore. We actually have a Web design forthcoming that has free materials specifically for seniors. And when that launches, that will be available. But in the meantime, we are also very much interested in making those contacts and moving forward with something like that. I think it is incredibly important. So if someone on the call has those contacts, we would be very interested in partnering with whatever senior programs there are that would really help get this kind of help to seniors; a very important group.

Thank You For Attending Today!

Merry O'Brien: Very good. Well, I hope everybody joins me in virtual clapping here for Pam Dixon. Thank you for taking the time with us today. This was a really fascinating Webinar, very well-attended. And we hope to have you back maybe in the future for more. We certainly know this is a topic that could definitely receive more attention. So we would also like to encourage everyone to, you know, definitely follow us online at the links that will be in the slides because we will have a lot of good upcoming Webinars this fall that may be of interest to folks. Some perhaps on child identity theft and more on cyber awareness and that sort of thing. So please follow us and learn more. And thank you, guys, for attending today.

Pam Dixon: Thanks so much.

Merry O'Brien: Bye, everyone.

[End.]