FTC Identity Theft: Planning for the Future Conference
May 25, 2017
Segment 2
Transcript

JOHN KREBS: Down side of me providing free coffee for this event in an auditorium where nobody can actually bring it in is, yeah, that makes it hard for people to finish their coffee. Rob, why don't you come up.

So we're going to get started with our next panel, and our next panel is-- we've titled it The Identity Theft Marketplace, or as these guys are going to say, it's really the dark web. And with me today I have two great panelists, Danny Rogers from Terbium Labs, and Rob Hoback from the United States Secret Service. And they're going to walk you through this, and we're going have some time to have a moderated discussion with me and them and hopefully take some questions from the audience. Remember those note cards. That's what they're used for. All right, with that, I'm going to hand it over to Danny.

DANNY ROGERS: Thanks, John, and thanks everyone for making it out. Thanks for everyone who's attending online. My name is Danny Rogers. I'm the founder and CEO of a dark web data intelligence company called Terbium Labs based just up the road in Baltimore, Maryland. And in the course of doing our job and building our commercial business, we have developed a pretty deep expertise, understanding, and collection, infrastructure for the dark web. And today I'm going to share a little bit of an overview of what that is and the sorts of things that we come across and deal with on a daily basis.

So for starters who here has heard of the dark web? Great. Awesome. So I promise there will be no follow-up questions to this one. But who has been on the dark web? Who is willing to admit it? Only about two or three people. Fair enough. It's an unfortunate word because it doesn't actually really mean anything. I like to define it as the nasty places on the internet, but it doesn't necessarily mean any one particular kind of technology or part of the internet. It's just the sorts of parts of the internet that traffic and things that the-- kind of that-- the more what we call the clear web or the more legitimate part of the internet traffic or trades and rights. So there's legitimate goods, and then there's the whole part of the internet that trades in illegitimate things like drugs, like stolen identities, et cetera.

One of the enabling technologies is one of the more high-profile ones is called Tor. Who here has heard of Tor? Excellent. Wow, this audience is well beyond most of the ones I speak to. So then I'll breeze through this really quickly, but Tor is an anonymity platform. It is a proxy network specifically kind of a proxy overlay network on the internet. It's essentially a volunteer network of about-- I don't know-- a few thousand, probably 6,000 or 7,000 volunteers who volunteer their computer to run this open source routing software maintained by the Tor Project.

The history is in the '90s three mathematicians at the Naval Research lab developed communications-- sorry, I'm rolling away here like Melissa McCarthy.

Sorry, I don't know if I can say that in this room. So they developed this communications platform to allow people to communicate over the internet anonymously, originally intended for kind of secure communications of government personnel on the internet. They then open sourced it, and it became this open source project called the Tor Project. The way it works is basically these volunteers volunteer their computers, the traffic-- I'll really breeze through this. It essentially gets mixed around in that network to anonymize the source and destination from each other. So if you're watching a network, the only thing you can see is someone is connected to the Tor network, and the only thing you can see is the Tor network is pulling down websites, but it's computationally intractable to tie the traffic of who is accessing the websites to the users connected to the Tor network. And it works when you have a few thousand volunteers and probably about two million people connected to Tor at any given time.

In addition, you're able to host content within the Tor network using what's called a hidden service. This was an interesting kind of academic project that the Tor authors had developed out of-- more out of curiosity than anything else. And then someone named Ross Ulbricht figured out that you can actually start e-commerce anonymously through this technology and start to sell things in a truly, as he liked to describe it, libertarian way, and sell things that you wouldn't normally be able to sell on the broader internet, things like drugs and stolen identities, et cetera. And so he started this website called the Silk Road. The history is probably very well known in this room, and that kind of led to a much broader online e-commerce ecosystem, mostly hosted-- actually it sort of split right-- partly hosted on Tor hidden services, partly hosted just around the world in places where-- kind of Western law enforcement may not be able to enforce any rules.

And so skipping forward here, what does that look like? I'll breeze through, again, a tour of the so-called dark web. On the left is a screen shot from what is right now the largest dark web marketplace called AlphaBay. You can buy all kinds of interesting things on AlphaBay. Think of it as kind of amazon.com for anything that you can't sell on Amazon. Here, for example, are Wells Fargo accounts for sale. On the right is a screen shot of probably the largest or one of the largest credit card-- stolen credit card marketplace sites called Rescator. If you look carefully, you can see that Rescator is not even hosted as a hidden service. It's just hosted at rescator.cm,

cc.

It moves around. But there's many, many hundreds of thousands, if not millions, of stolen credit cards for sale on this market. And you can search it by anything from zip code, issuer, network, type of card. If I want to buy a platinum Visa card issued by a certain bank in a certain zip code in a certain state, I can search this and find that exact thing, use it for whatever I want. Prices range anywhere from $15 to $50, depending on the value of the card. Platinum cards tend to go for more. Newer cards tend to go for more, et cetera.

Some other things-- so the dark web is also full of other interesting things. The RealDeal Marketplace was sort of the go-to marketplace for high-profile stolen data sets. You can see the Thomson Reuters world checked data set went up for sale on the RealDeal last year, creating a lot of headlines. In fact, most of the major breaches that you've read about in the newspaper were discovered because they were put up for sale on this particular marketplace where the journalists tend to hang out. So LinkedIn, Yahoo, et cetera were all advertisements on this particular market.

Other markets specialize in certain things. I have a screenshot here of something-- of forged identity documents. You can buy forged utility bills, forged bank statements, really anything like that.

And then even other parts of this internet-- this part of the internet specialize in things like doxing. So here is a dox of a government senior. Who here is familiar with the phrase doxing? So I'll explain it. So it's sort of a hacker speak for documents. It's essentially exposing personal information of high-profile people or people you want to particularly point-- harassment activities at in order to enable online harassment or physical harassment of them, and there have been extreme examples of this like calling in fake hostage situations and things like that that can get very, very dangerous for the people involved.

So one thing about the dark web I think is worth pointing out is that these technologies like Tor get a reputation for being synonymous with criminal activity. And we did a study last year to categorize the content on this part of the internet, and a couple of things emerged. For starters, it's worth pointing out that the Tor Project and Tor itself is a relatively neutral technology. It's a mathematical software thing that does a very specific thing, and it can be used for all kinds of activities, many of which are actually very valuable.

In fact, the Tor Project is, in large part, funded by the US State Department in order to enable free speech in places where the internet may be censored. And it played a very important role in the Arab Spring and in enabling dissent in parts of the world. In addition, the results of our study showed that most of the content on this part of the internet-- or at least about half of it was relatively mundane things, like a site called Tor Kittens, which shows pictures of cats or-- because it is the internet, and there must be pictures of cats somewhere.

Other parts are streaming radio stations and things that-- hobby projects, blogs. It's still a robust part of the internet. In fact, the big content distribution network Akamai did a study last year where they looked at the e-commerce traffic coming from Tor to big e-commerce sites and then from the clear net, and found that the convergence rates were exactly the same, meaning people were not just using Tor for malicious activity. They were using it because they believed in the mission or believed in online privacy, and we've seen with evolving regulations more interest in that online.

So I want to make sure it's emphasized that just from the technological perspective we can't equate technology with activity, that a lot of this is happening on, like I said, sites like Rescator.cc or something like that. A lot of dot RUs in there as well. And so I think it's worth pointing out that it's much more about the activity and much less about the technology

For my last few minutes, I want to get into a couple of points. One is what people are doing with this data, and I think we're hearing-- we've already heard a bunch about this, and then we'll hear a lot more about this. Right, there's the classic identity theft, people going online, buying identities, filing-- or opening bank accounts, taking out mortgages, destroying people's credit, things like that. These days obviously I think that's on the decline just because it's a lot more difficult than a lot of other ways to more easily make money, things like filing false tax returns. That's obviously, as we've heard today, one of the go-to, very easy ways to monetize this data.

One is what is called a three-way kind of retail scheme, where if I take a stolen credit card, I find a very popular, relatively expensive retail item. I advertise it on eBay for half price. Somebody buys it from me. I use that stolen credit card to buy it directly from the e-commerce retailer, drop ship it to my customer. I've made half the price of that at basically infinite margin, and I never had to leave my basement, right. Not personally, I don't actually do that, just to clarify.

But these are the kinds of schemes, and we actually-- keep an eye out on our site for a new report coming out that talks a lot about these various schemes and things that people do. And, in fact, on the dark web there's a large trade not in just the data to enable us but the things that you can do with the data, guides, instruction sets, pointing people to different ways they can so-call cash out of this kind of information. And obviously we've heard some of these, and we're going to hear about a few more today.

I want to spend my last few minutes talking about the impact. And I think again we're going to get into this more in the next panel and even more on this panel. But one of the go-to-- one of the things that should be emphasized here is often-- especially in the credit card world, the payment card world, this is viewed as a victimless crime, so to speak, meaning it's relatively small amounts of the payment industry. The individual consumers often don't have to cover the costs unless it's something more impactful like more traditional identity theft. The truth is it impacts all of us, not just in higher interest rates and fees and things like that.

But the fact that it has become sort of the go-to method of funding criminal activity around the country and even around the world, that why would you traffic in messy and dangerous things like drugs, when you can clone credit cards and buy perfume at Macy's. And so I think we need to-- my hope is to convey-- and I know John's hope in this conference is to convey that this is a much larger-- a piece of a much larger problem and the sort of hidden enabler of a lot of other things. So not only gaining activity domestically but even geopolitically, that this-- so the-- especially in payment cards, the economy is very specialized and very well-developed.

There's technical capabilities that used to be kind of reserved for state-- kind of state level, intelligence level capabilities that are now being turned on retailers to do things like breach point of sale systems. These are being done as large, organized international criminal efforts. In fact, if you read the Yahoo data breach indictment, paragraph I believe 65 identifies two active duty FSB officers engaged in payment card and gift card fraud. This is not isolated. This is part of a much larger ecosystem that is going to fund much more impactful activities. So we can think of this almost as the ultimate geopolitical judo move, using our own advanced pieces of the economy like payments, like advertising against other larger parts of our political and economic system. And I think that's a really important point for people here to take away.

And ultimately, I think the most long-term impact of this is going to be fundamentally trust in the internet. That every day we see data breaches, and in fact, our company we see probably 5 to 10 times that in terms of volume of companies or organizations that don't even make the news. Nobody is going to write a large-scale or high-profile article in Wire magazine about a school district in Nevada that may have gotten hit, but at the same time, if the internet's really going to achieve its full commercial potential, much like shipping channels in the 1700s became a vital commercial channel in world commerce, the internet has a similar kind of potential.

But for people to use it and trust it especially at the consumer level, we need to solve this problem. They need to feel comfortable using the internet, putting their data in, using payment cards, et cetera. Otherwise, it will limit the commercial potential there, and I think that's another equally important takeaway. So that's really all I have for you for now. Obviously there will be a question and answer time, but I guess I'll turn it back over to John.

JOHN KREBS: All right, we're going to pass it on to Rob Hoback from the Secret Service.

ROBERT HOBACK: Good morning, everyone.

Danny, thank you for making that distinction between the Tor network and the dark web because I'm going to refer to-- a lot of what we do and a lot of this presentation is about the criminal online marketplace, but we interchange that word with the dark web because that is where a lot of this-- we refer to it as dark web because that's where a lot of this illegal activity goes, but it's not happening all on Tor or the Onion network, so to speak. So thank you for making that distinction.

I want to start with this one. Shadowcrew.com and Operation Firewall only because shadowcrew.com was really the precursor to these online marketplaces. This is really when the Secret Service began to investigate all these credit card dump sites. So back in 2003 we initiated Operation Firewall because we were working a standard Secret Service credit card investigation, and we developed information that a lot of the credit card information that was being stolen was being sold on this website shadowcrew.com, and that was something that we had never seen before, before 2002. So in an undercover capacity, we were able to gain access to this website, and then we also, during that investigation, found another one of these websites called carderplanet.com, which was really written in the Russian language.

There was a third website, carder.org, which is not on here. But the interesting thing about these websites that we discovered is that it truly was an eBay style business model, and it had a vendor review system. The interesting thing about this vendor review or this peer review system was the fact that the folks that ran the website would do extensive analysis on the information that was being dumped on the website. So they were making sure that it was valid information that was stolen, that it was information that could be used, so that only the top-tier information, the best stolen information was going to be allowed on their website. That peer review system is something that's kind of carried over throughout the years, and it's still very prevalent on a lot of these criminal online marketplaces.

So why did we start to see this phenomenon back in the early 2000, 2002? Because credit card fraud, identity theft-- I mean, these are crimes that have been going on for decades, right. I think people realized that hackers had access to a tremendous amount of data, a lot more data that you could glean as opposed to doing it the old fashioned way, dumpster diving, stealing your mail out of your mailbox, old-fashioned skimming devices. They realized hackers were a lot more efficient in getting his information.

So at that point, you needed a way to move and monetize all that information. This is a transactional site, shadowcrew.com, transactional site. It's a recruitment site.

You can find a partner to help you in some kind of complex fraudulent scheme. And it was a knowledge sharing site, information on how financial systems work, how to defeat security and anti-fraud measures. So the group on shadowcrew primarily traded in stolen credit card numbers and bank account information. However, even as early as 2002, they were selling counterfeit passports, driver's license, Social Security cards, birth certificates, college student IDs.

Some of the administrators or some of the vendors on the site even offered complete wallets, and a complete wallet is pretty much what it stands for. They'll give you a credit card number. They'll give you the fake driver's license to go with it. They'll give you the fake ID documents, date of birth, Social Security number, birth certificate. And you can actually go to a brick and mortar store and prove your fake identity.

So the way that these pre-2004 online criminal marketplaces were structured, it really was kind of a mafia style hierarchy, if you will. So there were rules. There was a code of conduct. At the top you had the administrators. These were the top-tier level, the entrepreneurs, if you will, that administered the website. Below them you had the moderators, and the moderators would kind of break off into different segments of the website, and they would cover an area of their expertise. So if the moderator was an expert in credit card dumps, that was the part of the site that you went to. If you were more interested in fake ID documents, that's the part of the website you would go to.

Underneath the moderators were the reviewers, which we've kind of already talked about. They were the testers of the information, to make sure it was valid. And then, of course, you have to have the vendors. You have to have people willing to come to your site and sell you this information. And then, of course, you had regular members that-- you could join this site if you wanted to buy credit card dumps, fake ID documents, et cetera.

So once we took this down in 2004, it had about 4,000 members, active members. We were able to identify the administrators of the website, the primary players. And I think there were 28 arrests total, 21 of those were based in the US and seven of those were overseas.

Just to finish up about this, I just want to make the point that the internet allowed for the development of these early online criminal marketplaces. You saw the convergence of hackers. You saw the convergence of people who wanted to monetize this information. And then you had the convergence of the folks that could launder this money for you. So this was the first time we had seen all three of those groups come together and work together. Once we took it down, these criminal communities regrouped on Eurasian sites, but they use a shadowcrew concept.

The mentality and the culture among these cyber criminals continued, but the organizational structure changed. The rules and codes of conduct were self-policed at this point. There was no more leadership to enforce the rules because we took the leadership out, but the continued mentality created reliability. The only time that these folks were in contact with each other was in the virtual world. So that's very contrary to how normal criminals operate. It's kind of an honor among thieves mindset, if you will. So these criminals began to trust each other with larger jobs and more money as time progressed.

By 2005 the number of underground online criminal forums and marketplaces really started to expand and so too did the amount of information and types of information that could be used for fraudulent schemes. In 2005 we started seeing a lot of conversations about PIN decryption, ATM PIN decryption, ATM networks and architecture, how to defeat those systems. Also 2005 was really the year when we started to see the volume dealers. If you remember back to the 2005-2006 time frame, that's when we started to hear about some of these larger data breaches. Heartland Payment Systems was a Secret Service case, OfficeMax, Dave & Busters, TJX, Cheesecake Factory, Bloomingdale's, et cetera, et cetera. So you had millions and millions of credit card numbers, debit card numbers, driver's licenses, Social Security numbers, all this information starting to flood a lot of these sites. It was really more information than the sites could handle, so that's why you started to see the expansion of these.

In 2006, the conversation was really about buying encrypted databases, databases of credit card dumps with PIN numbers from credit card processors and ATM companies. 2007, we had a continued growth of bank account vendor sites. I mean, there were some of these online marketplaces that were totally dedicated to just selling bank account information from some of these large data breaches. And then logically, of course, what followed after that was the trading and brokerage accounts. If you could get enough trading accounts, brokerage accounts, you could obviously start to manipulate stock prices.

Did you guys-- anybody here-- Monday night I think DOJ put out a press release about the PRNewswire hack. Anybody see that? That was just an example of something that had been going on really since 2010. A group of Ukrainian hackers hacked into PRNewswire, and they were able to steal upcoming press releases about company news and then obviously either short or go long on a stock, depending on what the news was going to be.

Also, this 2005 to 2007 time frame is when we really started to see the explosion of online currency, cryptocurrency, unlicensed money remitters. This is how they were laundering the money e-gold, Liberty Reserve, and of course, now you have Bitcoin. And this cryptocurrency is really something that is for another day and another presentation because we could probably talk all day about that.

Some of the recent trends, cybercrime as a service or malware as a service-- I probably mischaracterize this as a recent trend because it's actually been going on for a few years, but it just continues to evolve on almost a monthly basis. These marketplaces evolve to the point where they're not just selling my information and your information. They realize that it's a lot lower risk for me as a cyber criminal if I'm willing to sell my technology, if I'm willing to sell my research and development, if you will. The actual tool that I used, that I developed to pull off some of these schemes. Everything you could think of is offered.

This is just a very small example of some of the services, quote, unquote, that you can buy on some of these sites. The interesting point about this is it's a lot lower risk for the cyber criminal. Then the other point is, if you've always had a penchant for doing these fraudulent schemes but you never really had the technology or the know how to develop your own malware, now you can go to these sites and you can purchase this information for you. You can have it tailor made for you, depending on what kind of fraudulent scheme that you say you want to commit. So it really lowered the barrier to entry. So anyone now can use top-notch malware. It really is one-stop shopping.

This we already covered.

Medical records, electronic health record databases, this is kind of a hot topic lately, especially in the last year or two. And the reason for that is health records have gone digital in the last seven years, and it's very lucrative. Think about the information that your health records contain, everything, right. All your PII information, all your payment information. Every time you go to the doctor, that's why they tell you to show up 10 minutes early so you can fill out those five or six forms. You have to list an emergency contact, their information. It really is a treasure trove of information to the point where a complete electronic health care record database can command almost a half a million dollars on the dark web. And the reason for that is because it contains so much data that you can use to commit new fraudulent schemes, fraudulent tax returns, stolen prescription, prescription fraud. The list goes on and on.

The other recent trend-- which we won't talk about too much. I think it's pretty self-explanatory. A lot of colleges and universities have been victims in the last couple of years. The reason, again, low risk and it's very lucrative.

These colleges have thousands of students. All your I information is housed on their servers. So obviously if you can get your hands on that and you can monetize that, it's very lucrative. Account checkers. Anybody here heard of the account checkers?

This is something that we've seen-- you could probably say 2016 was the year of the account checker. We saw a big increase in discussion on underground forums related to the sale of account logins in bulk, account checking tools and the frameworks on how to build these things. And I think the reason for this is you just think of those large data breaches, and Danny touched on it, Yahoo, LinkedIn, all those user names, all those passwords.

How many in-- and don't raise your hands. Really a rhetorical question. But how many have been guilty of using the same user name and password across your bank account site, your social media account? I mean, I've done it myself. I've caught myself a couple of times. I mean, you have to manage your work email, your personal email, your social media account, your E-ZPass account, your department store accounts. I mean, you name it, you have 30 different passwords. So it's easy to do. I saw a recent study where password reuse rate is about 70%, and I think that's probably pretty accurate.

These account checker tools, very inexpensive, very easy to use. Again, this goes back to the cyber crime as a service that we just talked about. I can go to the marketplace. I can buy some of these username and passwords, and then I can go to these account checker sites and I can brute force and just check them, and I'm going to get a hit. And imagine if I said, let me see if this user name and password is just on Gmail or Hotmail or live.com, and what if it does? Now I basically have committed an account takeover, and I can control your email account and I can do a password reset and I can lock you out of your own email account.

My time is up. So I'm going to-- keep going, all right. These are a couple of the more popular account checker, Private Keeper is kind of sold the way it is. It has a set list of functionalities, but you can customize it if you go direct with the tool administrator. Sensory MBA is the more popular one that we've seen. It uses configuration files that are customized to target different companies and account types. This I can skip because we've talked about that already.

And I'm going to finish up with this. Slilpp is an interesting site. So this is kind of a three-step process, with this website being the third and final step. So the first step is obviously you have to go out to the web, these criminal marketplaces, and you have to obtain the information you're looking for, whether that's credit card information, debit card, bank accounts, et cetera, user names, passwords. If I purchased 250, the next step for me is to go to one of those account checkers and test them out and see how many hits I can get. The success rate is about 0.02%. So out of those 250 user names and passwords that I bought, five of them are probably going to work. So obviously it behooves you, if you're into this kind of thing, to purchase as many of these as you can because that's going to increase your success rate.

And then the third and final step is once I've gotten the information and I've validated that some of it works, I have to make a decision. Do I want to use those five user names and passwords that I got to commit fraud myself, or is it more lucrative for me to go to a site like this and sell it to the site and then take the proceeds from that? So that's kind of how this works. Once you log into Slilpp, you have an inventory screen.

Now that you've tested your credentials, you know the ones that work, you go here and you can sell them to the site, or if you're just a member, you can buy these that have already been tested. You can see from the tabs at the top that they are advertising the companies where they have credentials that have been harvested that actually work for these sites, Wells Fargo, PayPal. So pick your poison, pick whichever one you want to use, click on the tab. And then that's where the fun begins.

The last thing I want to point out is customer support. We talked about this in the beginning with shadowcrew.com. Customer support was even big back in 2002, 2003 because of this virtual world and the fact that these criminals are not meeting each other face to face. Your screen name is your livelihood. That's your reputation. So if you're going to run one of these sites, if you're going to participate, you really have to offer outstanding customer service. I don't know if you saw on the last screen it even had the cute little shopping cart up in the right-hand corner so you can keep track of your purchases, just like you would a regular e-commerce site.

On this site in particular, they'll offer a tutorial on how to use their site for $15. They'll show you how to upload your database that you recently got to their site, and you can change the language to Russian if you prefer. So the site even provides comprehensive order tracking and detailed reports on what you sold.

So the whole point of this presentation was to show you that it's not just your credit card information and your financial information that they're after. They're after everything. They want all of it because they can monetize all of it, and it's very lucrative, which I think we'll talk about in the panel discussion. But because of these online criminal marketplaces, all the information that you have can be monetized, not just your financial information. That's it.

JOHN KREBS: All right, so we're going to-- I'm going to get the chance to sit down and talk to these guys. I have a million questions, and there may be reason that I chose myself to be the moderator of this panel, and part of that is just this because they're--

DANNY ROGERS: I have a question, if that's OK, for the audience.

JOHN KREBS: Yeah

DANNY ROGERS: To Robert's question, but in a way that I kind of encourage people to raise their hand. Who here uses a password manager? All right, so who here has two-factor authentication enabled on their personal email account?

The people raising their hands should be very proud of themselves, and everyone should be like those people. That's all I have to say.

JOHN KREBS: So there's lesson one.

ROBERT HOBACK: Just real quick, the only point I would make with the two-factor authentication is make sure that it's not email based. In other words, if you write-- because if I have your--

DANNY ROGERS: That's not really two-factor. That's the same factor.

ROBERT HOBACK: Right, because if they're going to send you some kind of code on your email but I control your email account, that's not going to do you any good. Obviously text message is better.

DANNY ROGERS: Time is the best way to go.

JOHN KREBS: That's OK. Clearly there are a million questions to ask, and I apologize that we only have a certain amount of time to do it in. But I kind of want to start with one of the things that always intrigues me the most. I go buy my $50 platinum card or my $15 card or I purchase other information, what's my rate of return?

DANNY ROGERS: I mean, it's obviously a pretty high-margin business. I mean, you're spending $15 and you're going-- to get the stolen credit card and then you're committing hundreds or thousands of dollars' worth of fake purchases-- or real purchases that you're then reselling or are cashing out. So I mean, it's SAS level margins there. It's pretty good.

JOHN KREBS: And one of the other things too, which we've talked a lot about the big breaches, like, those are all the ones that are in the news, the ones the FTC has brought cases against. Is that where we're seeing most of the data come from on the dark web?

DANNY ROGERS: As I mentioned in my talk, we see the really high-profile ones that people write newspaper articles about, but most of the activity actually comes from-- and it's, like, 5 to 20 times the number of breaches and things that come out of organizations that you probably never read about in the newspaper, school districts, smaller restaurant chains, retailers, things like that, medical practices but small ones. And the reason is that these attacks, when they get this data, these are automated attacks. There's sort of this popular culture image of a hacker in the basement with a ski mask on targeting JP Morgan. This is hacking, by the way.

So it doesn't usually work like that. It's really automated systems looking for vulnerabilities that exist. And when JP Morgan spends a quarter of a billion dollars on security, they become a much harder target. And so if I attack 1,000 mid-market organizations or smaller organizations, I get the same amount of data, and they're much easier because they're just much less well-defended. So most of the stuff that happens is happening from sites and organizations that we never hear about. Like I said, five times at least, if not up to 10, 20 times.

ROBERT HOBACK: Yeah, I would say that-- I can't put a percentage on it, but every day I would say that the majority of the network intrusions that we respond to, that our agents in the field respond to are small businesses. For example, back in 2014, one of our agents responded to a small mom and pop liquor store in Syracuse because they thought they had been breached. And when the agent did the analysis on the network and sent the information down here to DC to the NCIC, that's how they found the backoff malware. So this is a small mom and pop liquor store in Syracuse, and those are the types of places that our agents in the field are responding to five or six times on a daily basis across the-- those are the ones we just know about.

JOHN KREBS: So do you guys have a sense of how much data is out there?

DANNY ROGERS: I mean, I think the latest studies puts it in the billions of accounts. I think four or six billion, something like that.

JOHN KREBS: Accounts?

DANNY ROGERS: Yeah, four billion user names kind of thing.

JOHN KREBS: OK, I feel better.

DANNY ROGERS: Almost everybody does.

JOHN KREBS: So one of the things-- we talked about the breaches, and you guys mentioned they come from a lot of sources other than the ones we read about in the newspaper.

How long does it take from that information from the breach to get into the dark web? And maybe even then used?

ROBERT HOBACK: It depends, but fairly quickly.

A couple of days. It doesn't take long. I mean, it depends-- it depends on how the intrusion happened, right. It depends on what data they're looking for, and it depends on how they're going to exfiltrate that data. They may be in the network-- I mean, I think the average time that someone discovers they've been breached is eight months. So I'm in your network for eight months. I may have just started exfiltrating your data two months ago, all that credit card data. So it really depends. But once I've exfiltrated it back to my command and control server and then I've downloaded it or uploaded it on some of these sites, it could just be a matter of a couple of days.

DANNY ROGERS: And I mean, at the same time, it's a high variance, right, like you said. There's seven or eight months before companies even realize that they've been hit, if they ever do at all, and then often it goes very quickly because some of the data is very timely.

Other times we've seen things like credit cards sit for a long time to sort of let them cool off, so to speak. You get access to a really big box retailer. Some of the groups have different trade craft. Some move them really quickly. Some of them hold onto them for a long time and put them out in batches, in small amounts to kind of throw the trail off the law enforcement. So the longer you hold them, the less forensic evidence exists. And so there's a balance, and there's different tradecraft depending on which group is kind of perpetrating it. But yeah, it's a very high variance of answers to that question.

JOHN KREBS: So Rob, you mentioned two recent trends, which were medical records and educational records. And I think for a lot of people, like, oh, wow, you're right, there's a lot of PII there. It can we monetized an infinite number of ways. Are there other examples that we as society aren't thinking about that fit into that category?

ROBERT HOBACK: No, I think when you just think of it in terms of how much of your information that you have to-- that's out there that you have to input into some of these sites, all those user name and passwords.

Your PII information is being housed in all these places because it has to be.

I would just-- in anything, any institution that has PII information, any institution that does financial transactions are obviously a target, and that's whether that's a big bank, whether that's a hospital database, whether that's a small mom and pop liquor store.

DANNY ROGERS: Yeah, I think that's a really good point. We often get asked, what market do we serve as a company, and people say, well, obviously you serve finance or health care, right. The truth is every company on Earth has valuable personal information, even if it's just their employee W-2s. And so I think it's a misconception to think well, I'm just a liquor store, I'm just a hardware store, or I'm just a logistics company or a factory. I don't have anything that any hacker would want. You have monetizable personal information.

And I think it goes to a much larger trend, and really this whole conference, this whole subject is just sort of a result of this trend, which is-- and the Economist wrote their whole issue of their magazine about this last-- two weeks ago, I guess, called "Data is the New Oil," that the largest companies now on Earth are data repository companies. And so when you-- when large businesses are built on the collection of personal data for advertising targeting or other-- other ends, trading, whatever it is, there's bound to be leakage, just like if you have a giant tank of oil, some is undoubtedly going to spill.

And so the whole kind of economy, underground economy of data exploitation is a result of the kind of larger economic trend of data collection. And so you say all these places have all this personal information because they have to. I mean, they only have to because it's the new economy, and you're essentially graded in the new economy on how much data you collect. I think this is the competing trend here because companies collect way more data than they need oftentimes because that's what they can then monetize later. And so you end up with just tons of data being housed in tons of places, many of which don't actually need to be, and a lot of which is not stored as securely as it could be.

And so I think it's really important going forward for the government, for companies, for individuals to think about the idea of only collecting what you need to do the specific job you are trying to do because the more you collect, the more of a target you become, and the more likely you could contribute to this whole problem of undermining trust and identity in the rest of the economy. So I think it's an important point.

JOHN KREBS: So that leads into maybe the most important question. What can we do? And I'll start with Danny because there's two different perspectives here, and I want to get both of yours. But starting with you, Danny, what can we do? How can we address some of these issues?

DANNY ROGERS: Yeah, I mean, that's partly what I was just talking about, which is companies, for starters, need to think about what they collect and how they protect what they collect. At the same time, I think there's a lot that-- and again, I bring a commercial perspective to this, but I think there's a lot that the commercial industry could do to make this data less valuable, whether it's, like I said, being careful of what you collect and how you protect that to the payment industry, for example, getting more serious about fighting fraud as a-- jointly and together. I mean, part of it is that there's a lot of misaligned incentives in the payment industry between the folks that have the data and the folks that have the liability and the folks that have the risk. So the large networks and processors have a lot of data they can use to fight-- to fight this, but they're not the ones taking the losses. In fact, a lot of times they're selling that as a service, and so they don't necessarily work together.

There's the issuers which can take losses, but a lot of that liability has been pushed to the retailers where they have the least amount of ability to fight this. I mean, yes, they can implement more secure payment systems, but at the same time, if you're coming up against a state-level intelligence apparatus, there's only so much you're going to do to stop that at a technical level. And so really that's an example of an industry that could-- that should be incentivized to work together, not because the losses are huge to the industry. The reason that they haven't fought it harder is because the losses are relatively small compared to how much money the payment industry makes off of the payment system.

But as we've been talking about today, the impact more broadly is enormous. So here we have this industry that maybe doesn't care so much about this, as long as it stays within certain bounds. But those bounds are then creating all of this gang violence and geopolitical meddling and things like that are ultimately being subsidized by that activity. So I think there's a place for more of a push to fight it at the industrial level. There's also opportunities for cooperation and information sharing that I don't think are happening broadly enough, whether it's techniques with tech-- within the industry of how to fight this, whether it's data that can be used across the industry to fight this. I think there's room for a much more concerted effort on the industrial side, for sure.

JOHN KREBS: So Danny set you up perfectly for-- what are the challenges for law enforcement? And what are the things that law enforcement needs to be doing going forward to address some of these challenges?

ROBERT HOBACK: Yeah, so obviously from our perspective, we're kind of on the back end of this problem. So we don't get notified or we don't get called until the breach has already happened. I mean, we do obviously do community outreach, and we talk about cyber hygiene on a personal level and also with financial institutions that accept payments and use point of sale terminals and how to secure those.

But 90% of the time it's responding to a data breach after it's already happened or going to a company and presenting them with the evidence that they've probably been breached, and they don't even know that they've been breached. So for us, from our perspective, it's such a big problem. It's not something that the Secret Service obviously can do by themselves. It's not something that the FBI can do by themselves. From a law enforcement perspective, you really have to-- you really have to work together.

That's why we train state and local police officers at our NCFI facility, our national criminal-- our National Cyber Forensics Institute in Hoover, Alabama. We bring them in from all over the country. They get the same training we get. We provide them the equipment, and they can then go back to their communities and they can do these investigations themselves.

You need cooperation not just from the federal level but the state and local level as well. And then probably just as important is you have to have good relationships with your foreign law enforcement partners. 95% or maybe even 100% of the high-value cyber targets that we look at are all located overseas.

When they leave a country that we don't have an extradition treaty with and they go to a country that we do, it's important that you have that established relationship so that you can actually put handcuffs on some of these people because I think that's the way that law enforcement can approach this is the more punitive damage you can do to these folks, the more of their comrades that they see that are being locked up for this type of thing, it may slow it down a little bit.

JOHN KREBS: So you guys have made it clear that it would not be very hard for me to become identity thief. Not that I'm really-- think of my next career already. But I can get the mail or I can get everything. How many sites are there out there? You've referenced a couple. But are there a lot? Are they relatively easy for me to find? How do I go about this process?

DANNY ROGERS: I mean, there's at least a few hundred of-- and again, different specialties. I mean, there's Tor and service out there that specializes in data on rigged horse and dog races in certain parts of the world, very, very specialized. It also might just be a complete scam. You have no idea because it is the unregulated part of the internet or not regulated, but there is no-- there's no governing body. There's no recourse if you get screwed. It's reputation based, but it's-- I mean, there was this phrase used before, honor among thieves. I mean, there isn't that much honor among thieves on that part of the internet, and so it's not too hard to find. It's easy to do it poorly and either get screwed or get arrested.

JOHN KREBS: So I think in our-- I have two questions for our last couple minutes. And one of them is, we've seen a lot of these websites and there's been a lot of breaches of email addresses and passwords. Do you see a movement towards compiling this information from different breaches or for different maybe high-value assets going forward? Or maybe that's already happening.

DANNY ROGERS: I mean, we-- I certainly think we're in the early days of this. I mean, I think we're also in the early days of realizing the full commercial potential of the internet, but analogously we're in the early days of seeing the full realization of online crime, too. I mean, more and more crime is being committed online because it's just easier, the same reason more and more activities are going online because there are efficiencies gained. Why would you go out on the street if you can stay in your basement? And so I think we've always been surprised by the creativity, and I think again we're only at the beginning of seeing it happen. At the same time, at the end of the day, like crime is crime, and we know how to fight it, and the techniques to do so aren't all that different than what we've been doing for decades, if not centuries.

ROBERT HOBACK: Yeah, I mean, I'm sure it will evolve. I mean, it always does. I don't know how to quantify that or describe how it's going to evolve. I just know that it will. The one concrete example I can give you is the new EMV chip for the credit cards, debit cards. That obviously was instituted overseas in Europe already a few years ago. We are here in the United States in the process of doing that. So I think you will see less card present fraud, but that's going to increase card not present fraud. So all the e-commerce sites are probably going to see a spike in that, and that trend held true overseas in Europe when they instituted the EMV chip. They did see a drop in card present fraud, but there was an increase in card not present fraud. And rest assured, I'm sure that the criminals are looking at trying to find ways to circumvent the EMV chip.

And they probably will. It's very possible at some point that they will find some way to do that. And then once that happens, you'll probably see a spike back up in card present fraud.

JOHN KREBS: Well, I want to thank you both. Our hour's up, unfortunately. But I want to thank you both for participating, giving great presentations, and helping us educate our audience on this. To me this is a great example, although I said earlier, for those who weren't here, that we have a public comments section on our web page. We'll be taking comments through June 30, and we really encourage people to add their thoughts or additional questions so that we can add to the depth of this discussion. Thank you both.

[APPLAUSE]

And I'm going to ask our next panel to come up.

MARK EICHORN: Well, as everyone gets settled, I'm Mark Eichorn. I'm an assistant director in the privacy and identity protection division at the FTC. It's my pleasure to moderate The Big Picture panel. So we're going to look into some of the issues we've been talking about this morning in greater depth and also some greater abstraction as well. And each of the panelists I will sort of introduce as they begin their remarks, but I just wanted to comment that I think everyone here basically has a job title or a job that sort of probably didn't exist 20 years ago. And that's a good segue to Christopher Mascaro's title as vice president of threat intelligence & analytics, which sounds like a pretty cool title. So Christopher, why don't you tell us a bit about what you do at First Data

CHRISTOPHER MASCARO: Yeah, so for those that don't know what or who First Data is, we are the world's largest global payment processor. In total, we process about a few thousand transactions per second, which amounts to about 80 billion per year. So if you have a payment card in your wallet, if you've had any sort of interaction with a payment in some way, we probably issued the card or were the acquiring side of it at the merchant level. So as a result of that, we see a lot of things in the payment space. Payments are our business. We have a lot of consumer facing brands that you may not know about. We manufacture POS systems. Apple Pay technology was developed at First Data. So we're moving beyond just the traditional point of sale system, which is interesting when on the last panel we talked about maybe compromising the EMV.

They might just move past that because mobile payments, other things like that are starting to take on. One of the things that's interesting, I think, about First Data is that because of the amount of payment data and financial data that we see, we see all types of fraud. Payment card fraud is obviously our main business. A lot of my team that I manage is in those shops that the previous panelists were talking about. We're collecting data from those shops, trying to couple it with our proprietary data that we have, the 80 billion transactions, to try and make sense of it and hopefully identify these compromises before fraud or identity theft actually happens.

In addition to that, we see a lot of aspects of application fraud, mortgages, loans, lines of credit. When it comes to synthetic identities, this is where we see a lot of really interesting schemes that are discussed, and obviously the tutorials and other things like that are sold, as Danny mentioned, on the dark web. I really think that one of the interesting things about synthetic identity fraud in the application space, applying for mortgages and lines of credit, relative to the payment space is that you can go on for years or at least months without being caught because not many people check their credit report, not many people have alerting around that. But when it comes to payment card fraud, especially if you're looking to make money quickly, people see money disappearing from their bank account or their credit limits decreasing pretty quickly. So we definitely see that.

Also, account takeover is something that my team has really been focused on a lot recently because of the amount of data that's out there. So account takeover is facilitated through stolen credentials, stolen-- things like that to have some sort of identity theft there. The extent of malware that we see in addition to the extent of sites that are out there is pretty impressive. There was a question in the last panel about how many sites are out there. We have about 350 sites that sell just stolen payment card data that we've tracked. They come and go. They're not the most stable. But over the past 2 and 1/2 years, that's what we're up to right now. And I can talk a little bit more about that after that.

I think a lot of the factors that contribute to the fraud, in addition to the availability of the data, is fatigue. I think consumers are less concerned because there's just so much. How many people here have had a payment card replaced in the past few years? I would imagine everyone. I've had two payment cards compromised on the same day before, which is oddly ironic. I think it was on purpose, but still I think one of the problems that we have in this space is that everyone's payment-- it's not a question of if the payment card you have in your wallet is compromised. It's how many times it's been compromised.

The same thing with your identity and your credentials. It's not how many times you've had your credentials stolen. It's how many-- or what sites they've been stolen from. It's how many places are selling them. And I think that really this whole marketplace, when it comes down to identity theft and monetizing that through a number of schemes, is it just intractable to identify and stop this all.

I think one of the most interesting things that my team follows is the novelty ingenuity of some of these criminals. They know payment cards. They know fraud. They know how to manage the systems better than some of the best people-- at my company there are some of the best people in the payment space in general, and it's because they have time to play around. They have time to figure these things out. Some of the scarier things that I've seen when it comes to malware and identity theft is in the past there's malware that looked for credentials. There was malware that looked at the point of sale system for credit card number, expiration date, CVV codes. We started to see some identification of malware that's looking for driver's licenses, other sort of PII data that then could be monetized or sold along with that data.

In that last panel there was discussion about card present versus card not present fraud. My team is actually responsible for identifying a breach of gamestop.com recently. It was one of the largest card not present compromises that we've seen in the past few years of tracking this on the analytic side. What was concerning about this breach-- if you go and buy a store-- or go to the store and buy something with your credit card, your card is stolen, maybe your name, where you shopped is known. Card not present breaches, it's your name, it's your telephone number, it's your address, date of birth sometimes, other things like that, which, again, isn't just your payment card number. It could facilitate a number of other vectors of fraud.

Looking at the magnitude of the problem-- this is always a question that I get-- payment card fraud amounts to-- there's estimates between 7 and 10 billion a year. A lot of this is taken on by the banks or the merchants, but I feel like with the recent liability shift with the banks not being responsible anymore and the merchants being more responsible because of the adoption of EMV, at least in the US, we're going to start seeing some interesting regulation battles over that because the merchants have more at stake. And also just to put numbers on some of the marketplaces, using some Bitcoin analysis back in 2015, we identified that one of the most prominent card shops that actually Danny had a shot of earlier on his slide made about $45 million in just transactions alone. So that's a pretty good profit since it doesn't cost any money to steal that.

MARK EICHORN: Christopher, was that 7 to 10 billion in the US or worldwide?

CHRISTOPHER MASCARO: Worldwide. And it used to be split evenly between card present and card not present, but we are definitely seeing more of the shift.

MARK EICHORN: Next is Ann Patterson, senior vice president and program director at the Medical Identity Fraud Alliance. Ann.

ANN PATTERSON: Hi. Thanks. I want to start off by saying I'm unexpectedly not on my A game today, so if I-- if you feel like I'm leaving huge holes in what I'm trying to tell you, try to contact me later on, and I can give you all different kinds of answers. For those of you who don't know the Medical Identity Fraud Alliance, it's a nonprofit coalition of the health care providers-- and by providers we mean hospital systems, not individual physicians-- so the providers, the payers, which are our insurance companies, their business associates as defined-- typically defined by HIPAA, academia such as some that are in the audience today and speaking, public entities like the FTC, and other non-profits that are also here today that are like-minded in terms of they either do, on the consumer side, some kind of consumer or victim assistance or they work like MIFA does on the business side.

And so the goal of MIFA is that these-- all the stakeholders, those parties come together, and we're trying to move the needle on specifically very narrowly defined medical identity fraud. So not medical fraud, not all things health care fraud, and not all things identity fraud. Just the intersection that's small that's considered medical identity fraud, and so that's what we're focusing on. And the reason why was a few years ago when the alliance started, there was not that focus specifically on that. Most groups are either all things identity theft or identity fraud, which a lot of that is financial, or there's huge amounts of health care fraud and a lot of that is in billing that's not directly identity fraud. And so the coalition started to focus on that narrow focus.

So I wanted to give you-- you've heard some, as you know, opening remarks by the chairwoman about-- a little bit about what medical identity fraud is, but I just wanted to make sure that everybody understands. So we define medical identity fraud as fraudulently using an identity. So that can be an outright identity wholly Ann Paterson or it can be the synthetic identities you've heard about that are cobbled together with this person's name, this person's birth date, that kind of thing. But using an identity that's not your own for financial gain or medical goods or services.

So it's specifically using-- you've heard PII. Everybody knows PII. In health care, it's PHI, Protected Health Information. That's defined by HIPAA. So the PHI will contain all of your traditional PII but also additionally things that are specifically health care. So typically anything you would find in your medical records. So it could be things like your insurance carrier name, your ID-- your insurance ID number, group number, things like that for the processing of the claims. It's your medical information that's in your medical records, the medical record number. So all of that is PHI that-- when we talk about medical identity fraud, it's the fraudulent use of PHI.

To kind of give you an example of the types of things that we're seeing in terms of medical identity fraud, so one of them is kind of a leading topic and it's oftentimes maybe with synthetic identities that you'll see presented coming through hospital emergency departments. So within the EDs for-- first of all, to level set the basic understanding is that we have laws in our country that say that when somebody presents to an ED-- so this is not just going to a regular physician's office. But if you go to an ED in the United States, you're not refused care based on your ability to pay, and so you usually do see those signs in the EDs when you go-- it'll be like a patients' kind of notification, patients' rights posters and things like that.

So going sort of hand-in-hand with your inability to prove that you can pay, part of that is proving that you have health insurance or not health insurance, it's who you are too. And particularly in the emergency department where the care is oftentimes emergent of what you need, the last concern of the physicians or the triage nurse, what have you, is going to be about who you are and can you pay. Well, the can you pay part they're legally-- it's not supposed to be a concern. You're supposed to get evaluated.

So what we see that's kind of a current topic now is people presenting into the EDs for prescriptions, in particular opioids. And so that will be oftentimes two different scenarios. One will be the addict, and so that's the addict that's actually using stolen identities or synthetic identities that are hopping from emergency room to emergency room to get the prescriptions that they want for that narcotics.

Then the other one you might see is more of a crime ring type kind of situation where they're going in, presenting with the ailment I have a back pain, what have you. The doctor can't tell are you lying or not. Pain is not something you can take a test for. It's not like, oh, he tested positive for pain. So then you get the prescription that you want, and then the criminals then are obviously reselling them, the opioids. And so from a very current type kind of situation that a lot of people in health care have been talking about and community health and public health with the epidemic there, we do see identity theft and fraud playing a pretty big role there.

Another thing that you might see in medical identity fraud are field studies, which the last time we did a field study of medical identity fraud victims was in late 2014 was when we collected the data. So it's a little bit dated. But what we found is that about 20%, just over 20%-- which is a pretty high number-- of specifically medical identity fraud victims-- so we're not talking about all identity theft victims, but specifically medical identity fraud victims, just over 20% experienced some sort of negative health outcome. And so we've heard this mentioned before. And when that happens is that these victims are either being mistreated or misdiagnosed or there was a delay in receiving the proper type of care because there's confusion about the type of-- what their actual health status is because their records now are commingled with an identity thief who got care in their name. And so those are some typical things that medical identity fraud, both on the provider side, the insurance side, and the victims, we see happening are things like that.

MARK EICHORN: Thank you. And how long has the alliance been around?

ANN PATTERSON: A couple of years. A couple of years in operation. This will be our third full year of operations.

MARK EICHORN: Next I'd like to introduce two counterparts from the IRS, Mike Beebe and Todd Egaas. Mike is the director of return integrity and compliance services and the IRS's security summit executive lead, and Todd is the executive liaison official responsible for the identity theft tax refund fraud ISAC.

Which one, Mike?

MICHAEL BEEBE: Yeah, so I thought I'd tell everyone a little bit about what IRS has been doing to combat identity theft. Some of the things that we've done, we've certainly taken some pretty big steps in regards to improving our filters to identify identity theft tax returns. Where previously we had one system that identified from a fraud base, we now actually have a separate system that focuses also on identity theft. And where we originally started these identity theft filters, we had four filters in place, and we've come pretty far because now we have over 200 different filters and subfilters.

Also, some of the things that we've done to combat identity theft, we've limited the amount of direct deposits that can be filed into a bank account. We've also worked with banks to suspend suspicious refunds. We've locked decedent taxpayer accounts. We've also worked with other federal agencies to identify prisoners and identify those tax returns. We've also created identity protection PINs for those victims of identity theft. So when they come back in the following year, they're able to provide a PIN to us so we can authenticate them. We've worked closely with our Criminal Investigation Division, and we've put over 2,000 individuals behind bars.

Although we've made some significant strides, one of the things that's concerning-- and I've heard on several of the panels-- just the amount of data that's available. We continue to see confirmed identity theft cases where the amount of historical characteristics continues to grow. Where originally it was the primary Social Security number, now we're seeing spousal Social Security numbers on the returns, dependents' Social Security numbers, dates of birth, wage information, or employer information, and even current wage information. As a matter of fact, this year we've seen over a 400% increase in what we call business email compromises. This would be when a fraudster is actually able to fish an employer and get the current year W-2s and then start filing tax returns to the Internal Revenue Service.

In 2015 it was reported that we had released approximately $5.8 billion in identity theft refunds. It was a pivotal year for us. There was also a series of tax-related identity theft incidences. So the IRS Commissioner John Koskinen convened a summit in March of that year, meeting with state agencies and the tax industry. We formed what we call the Security Summit. It now consists of over 40 states, 20 state software providers, and six endorsing organizations. And really we focused on communications to the general public, improving safeguards, and information sharing. And I'll share a little bit about what we've done on each of those.

Communications, we focused on two areas. One for the individual filer. You can go to irs.gov, and if you enter in the search area taxes security together, there will be information there as to what you can do to protect yourself against tax-related identity theft. Also, what to do if you are a victim of tax-related identity theft. Also, there's another communication initiative. It's called Protecting Yourself From Protecting Your Clients. That's geared towards tax preparers and what they can do to protect their systems and their clients.

Another area that we focused on, like I said, was improving safeguards. There we implemented what we call trusted customer requirements, which is to strengthen password protocols and prevent account takeovers. And then we engage both the states and industry in information sharing in several different fronts. One on the front end at a point of filing there's a large amount of data elements that we can leverage within existing authorities with the preparer community and with the states. So we've worked very closely with them to share that information to help further make our filters more robust. Also, on the back end, we've worked with the financial institution and also with many of the states to better identify where suspicious refunds-- or where refunds are maybe going to suspicious accounts.

And then one of the things-- when the returns are coming in, we create a conduit for both the states and industry to share leads with us. They may be seeing things that are suspicious in nature. So they can report to us those returns, and then we can better identify schemes and trends and identify those returns and put in what we call our taxpayer treatment program where we ask the individual to authenticate whether or not that is their return or not. One of the things that we are actively pursuing-- I'm going to turn it over to Todd in regards to the ISAC-- is more real time data sharing and alert. So Todd.

TODD EGAAS: Yeah, thanks, Mike. One of the-- Mike talks about the security summit and for the IRS-- I mean, this was a notion that we couldn't just look at solving this problem unilaterally. We had to look at the ecosystem, and we had to consider where does a return enter the ecosystem and then where does the refund come out. So in that way the tax preparation and software industry was-- you might consider the front door, and then you have federal government and state governments where the refunds are coming out. And so looking at the problem holistically helped us coordinate these activities, as Mike described. But then a natural outflow of that was creating what we call Information Sharing and Analysis Center.

I had thought that ISACs would have already been talked about at this time. So I'll explain a little bit about the concept that ISAC-- I mean, public/private partnership is not a new concept, right, federal government working with-- federal and state government working with private industry. But ISACs were set up in Presidential Directive 63 to protect critical infrastructure for public and private organizations to share information that-- especially I think at the time cybersecurity was very pressing. And to coordinate efforts there. They since have blossomed. Anybody in the federal government might recognize ISAC or an ISAL as being a popular buzzword, and there hadn't been one in the the tax refunds space. And we weren't going to jump on the popularity train, but we did see a need to kind of put some structure behind what was started in the security summit into a organization with the intent and purpose of sharing information to help identify and reduce identity theft.

So we have a trusted third party in the middle. As you might imagine, some of our tax preparation industries or companies are highly competitive. We have a trusted third party in the middle that helps facilitate information when otherwise it would not necessarily be shared. Biggest issue we have right now is just sharing information and the trust around sharing that information. And we can talk more about that in the Q&A.

MICHAEL BEEBE: I do want to, if I could, share-- again, coupled with the ISAC and the effort of the security summit, we've actually been able to reduce the amount of tax-related identity theft. For the processing year 2015, we saw roughly about 700,000 incidences of confirmed identity theft. This last year as a result of this summit, it was down to about 375,000. So it's a reduction of about 45%. And we continue to see about a 50% reduction through this filing season. So it's about a quarter of where it was when we started the security summit and the ISAC.

TODD EGAAS: In talking to our participants, I think in general we feel that taking this more holistic approach, this is the right angle on the problem. The IRS is only so big. We only have so many resources. But now we have many more eyes. Everybody sees a different part of the puzzle. Pulling all those together and be it in the security summit, some activities are now in our ISAC, we have a much greater chance of making an impact and identifying and reducing identity theft.

MARK EICHORN: Thank you. Our last panelist is Kenn Kern. He's the chief of staff to the investigative division and special assistant for international relations in the New York County District Attorney's office. Kenn's on the front lines fighting identity theft.

KENN KERN: Thank you, Mark.

Hi. Good afternoon, ladies and gentlemen. It's a great pleasure to be here and have the opportunity to talk with you. I want to thank the FTC on behalf of District Attorney Cyrus R. Vance, Jr., who is the New York County District Attorney, for inviting us here to be part of this conversation with you. And thank you very much for the tremendous coordination and work with this great panel.

So as Mark made clear, our office is really on the front lines trying to address this problem. From a scale and scope of what our office sees, we have 600 attorneys. 105,000 cases a year come through our office. We've had to really rejigger our structure in order to deal with the complexity of the identity theft problem. I remember as a prosecutor standing before judges on identity theft cases where they were annoyed that we had brought the case. It was complicated and there was paperwork, and it just seemed troublesome. And I don't make light of this. And then as more of them were victims of identity theft, it became an easier conversation in terms of bringing these cases.

So our office is-- right now in terms of our felony cases, well over 25% of all of our felony cases involve some identity theft or cyber enabled crime. It's a tremendous uptick over the last decade where 10 years ago it would have been roughly around 3%. So 25%. What it means for us is we now-- of our 600 attorneys, over 100 of them are dedicated to addressing the identity theft tsunami that's happened and is continuing to happen going forward. What we have tried to do in order to address that is-- you have to have the technology on the front lines. That means you have to have your own lab to deal with the smart phones that's in every criminal's hands as they traffic the personal identification information and as they execute their plans. We've also created a cyber intelligence unit which is investigators on the dark web communicating directly with criminals in the forums and trying to glean intelligence from that and build cases.

Some of the matters that we've had to address-- I'll just highlight two cases. One that happened this month was 39 defendants in a traditional counterfeit check cashing. So the scale of it-- the uniqueness of this was a debit card cracking scheme, which is becoming more and more common. Technology plays such a huge role in encryption. If you were to go onto your Instagram and sort of look up individuals, you'll see recruiting methods on all social media designed to lure typically young individuals into the criminal act, get them to deposit a check, get them into the scheme, give them some percentage of the money, and then use them to facilitate it. So that's happening in the technological sphere.

I'll talk about the challenges that prosecutors are having in terms of using that data and getting access to that data. But in this debit card cracking scheme, essentially phony checks are going into the banking system, and then before the bank can figure out exactly what was happening, despite the best protocols in place, the criminals are using debit cards to quickly move that money out. So it's a quick cycle of getting checks in and getting checks-- and getting money out through debit cards. So that's this month.

The complexity of these cases-- why we devote one-sixth of our prosecutorial resources to this is because these are long-term investigations involving multiple countries, involving multiple languages that have to be analyzed and deciphered. Just about two years ago our office, along with the City of London police, the Royal Canadian Mounted Police brought a case involving StubHub fraud in which they utilized-- they got into the StubHub systems, were able to gain personal identification information off of various cardholders, basically get tickets, resell them, and then they have to, of course, move that laundered money. So the mastermind who's controlling this using his technological skills is in Russia, money launderers in Canada and London, and then a set of actors physically in New York.

So you have then four locations in which criminal activity is happening, and all of those have to be coordinated using different sets of laws and different principles in order to bring down what everybody is always aspiring to do, which is not to go after the small fish but to go after the large fish. So you can imagine the challenges in terms of coordinating the legal and police actions in that case. 1,600 StubHub victims and money launderers were brought down. These were some of the partners that were involved in the case as well-- I mentioned City of London Police, but the attorney general of Singapore was also involved.

How have we had to change the way we operate as prosecutors, as investigators? We can no longer be content with being physically in New York or Kansas or wherever our home base is. Our office has to send individuals, our own resources, overseas. So we have secunded staff to London, Paris, Singapore in order to be on the ground working on those cases. We receive assets from those offices. We're a state office, basically a local prosecutor's office trying to grapple with the scale of this. And in order to effectuate that, you have to think differently.

Just one last point before my time runs out, the barriers to us doing these sort of complex cases-- we can get past the language issues. We can get past the technology issues, to some extent. Encryption, something that I'll address in some of the questions here. I just want to point out that right now my office sits upon approximately 550 phones and devices that we're not able to get into because of end-to-end encryption. It's a real barrier. And what I really want to point out is that 40% of those are related to identity theft cases. So the thieves are trafficking the information. They're using their smartphones to do it, and we have a barrier to entry that we're trying to work with the private sector to try to get past. So thank you so much for this opportunity. I look forward to talking with you more.

MARK EICHORN: All right, thank you to the panelists. I just wanted to invite everyone to-- if you have a comment or question, you can fill them out, and we'll have someone pick them up and bring them up to me. So I guess I wanted to sort of follow up on Kenn's last point about international cooperation. I guess technically it was-- encryption was the last point. But right before that was-- I mean, it's pretty stunning that a New York County Prosecutor's Office has people in London and Singapore and all over the world. And I guess it just sort of raises the international aspect of this, and so I wanted to see the-- with respect to the other panelists, is there other international coordination or collaboration that you all are involved in to address the issues that you're working on more holistically?

ANN PATTERSON: For MIFA, we have concentrated just in-- the numbers that we look at are just in the US. Like, the 2014 study that I mentioned to you had over two million-- 2.3 million medical identity fraud victims just for that year, that previous 12 months, so from the end of 2013 to the end of 2014. And so we're looking to move those two million victims into being not a victim because those are annual numbers, and that number has grown in the previous five years that we looked at the numbers.

MARK EICHORN: So grown to 2.3 million from about what?

ANN PATTERSON: It about almost doubled. I don't remember what the 2010 number was, but it was close to

doubling.

TODD EGAAS: I'll say from-- my day job, so as the executive over our ISAC that we just stood up, my day job is actually in our Criminal Investigation Division inside IRS, and CI and chasing criminals around the world, just as our Secret Service partner had described. We have 10 attaches attached to embassies-- or sorry, attaches attached to 10 different embassies around the world. We routinely partner with law enforcement agencies in different parts of the world. There's only one dark web, right. You can't constrain that to national borders.

CHRISTOPHER MASCARO: And we-- we're a global company, so we have operations in 40 countries and merchants or banks we work with in 110. And so if there's compromises or other sort of issues, we often go to our US counterparts first, but we oftentimes have to work with local law enforcement and/or regulatory agencies as a result of the clean-up or remediation.

MARK EICHORN: Kenn, I had a question for you about-- obviously you can have a lot of identity theft where the perpetrator may be located somewhere else and maybe the victim is in New York or vice versa. So that seems particularly challenging. I mean, I think you all are incredibly sophisticated to have 100 attorneys working on this problem, but especially for-- if you're in rural Alabama or something, you're probably not going to be doing that. How do you sort of decide which cases to go after? Do you sort of try to focus on cases with lots of victims in New York?

KENN KERN: It's a great question. So one thing that we-- because we have the advantage of 105,000 cases coming in the door, there's a lot of intelligence to study to figure out patterns and opportunities.

Our goal is to really attack even the small because I think what often gets left behind is somebody arrested at a Macy's with a forged card on them can often be that thread that would get me to Russia, and we just have to slowly, slowly build there. We make a concerted effort because we want to be attentive to all of the victims that we know of and the ones that we can study is to try to bring them a sense of justice.

And so each case to us has to be addressed. There's no leaving some to the side. The resources that we might be able to send to our dark web are higher-end matters, those we want to really focus on. Can we get at the ringleaders? Can we make a dramatic impact within some part of the ecosystem? And that is a conversation that we'll have with partners such as-- at the table. We've worked with the IRS repeatedly in terms of fraud that's happening with the taxation system, and I can run down many examples.

So the short answer is there's so much to work on, you have to take those opportunities, even if it appears small, because not only does-- it matters to the victim of that crime but because there's an opportunity to really build fantastic cases from it.

MARK EICHORN: I hesitate to ask this question because I'm afraid I know what the answer is. But is there a low-hanging fruit in going after identity theft? So in sort of moving the ball forward-- so Christopher, you mentioned possibly new types of mobile payments, and I don't know whether you see that as sort of something that might change the situation, at least for financial theft.

CHRISTOPHER MASCARO: Yeah, no, I think that there-- the problem is when you go after or focus on emerging technologies, there's often a resurgence of all types of fraud. That was actually mentioned in the presentation about the check fraud scheme. We've seen a lot of check fraud happening lately. Actually one of our businesses or lines of business is Telecheck, which is the conversion of checks into electronic funds, and we've seen-- I'd say over the past 14 months, dating back to the start of spring last year, a significant re-emergence-- I don't know if it's a re-emergence, but definitely more fraud in the check's face than you would think. So as there's more focus on combating payment card fraud in our space but also newer types of payment issues and technology, there's definitely a reversion back to old ways in some ways, because we're not looking for it like we once were.

MARK EICHORN: The earlier panelists-- I'm talking about all the paper documents that are still exploited 50%. Does anyone else have any thoughts on easy solutions or solutions?

ANN PATTERSON: I don't have solutions. But in terms of the low-hanging fruit, I think definitely health care has a fair amount of vulnerability. You talked about Telecheck. And part of the reason in health care is that there isn't the same sort of legal and regulatory regime as there is that protects our money. Things like know your customer. There's no such thing as know your patient. Like I mentioned when you come in through the ED, you don't really have to know that patient. You are, by law, required to evaluate them. And then things like the Telecheck, we've got different health care delivery mechanisms kind of emerging.

Telemedicine is kind of-- I mean, it's got some legal and regulatory hurdles to go through, but that's becoming a popular thing of wanting. It's definitely the mobile device space. You've got all your-- like the FitBit type kinds of things, not just that, but there's tons of the mobile devices that are capturing and transmitting all kinds of PHI. And so those types of things aren't completely under HIPAA or HITECH right now because they're new and emerging. And so unfortunately, the bad guys can move quicker than our laws and regs can move, and so they can jump on those channels right away in terms of low-hanging fruit when they find that. I think the bad guys are pretty smart about moving ahead into those channels.

CHRISTOPHER MASCARO: Kind of a follow-up to that. I don't know if you've seen this in the health care space. But what we see-- we have relationships with large banks, small banks, large merchants, small merchants. Larger banks, larger merchants can afford the countermeasures and strategies to combat certain types of issues. And as I mentioned earlier, these criminals know the space better than us. So they'll target these really small banks, one or two branches, clean them out over a weekend when no one's working. And $100,000 to some of these small institutions is a question of keeping their lights on or not. So I don't know if you've seen that in health care.

ANN PATTERSON: I think definitely in health care there is a difference between a small clinic or a private physician, his ability to protect my records, that's not part of a large hospital system, that doesn't have the same kind of resources. Oftentimes your average private practice doc, solo practitioner isn't going to have somebody with a CIO title at all.

KENN KERN: And Mark, I think what we see is because there's so much money to be earned out there that insiders at the financial institutions, at the small doctor's office, they are the ones who are capturing that personal identification information, stealing it, and then placing it into the open market. So the challenge is there's so much opportunity for the theft of this information in small and large places, and some of our statutes-- I can speak to New York, frankly the penalties for engaging in this sort of activity, identity theft and others, while there is the opportunity for jail, typically it's just not strong enough. The laws are a bit outdated.

And in studying these criminals over years and knowing how-- when you go in for a search warrant, they often keep articles about other criminals who have been caught, and they study what people get and what law enforcement is doing. It's such a cat-and-mouse game. So the ability to really build sophisticated, high-end matters is also contingent on having laws where you can go ahead and effectively punish and deter. So that's from a prosecutor's standpoint, of course.

TODD EGAAS: I was thinking when you mentioned low-hanging fruit and if you had maybe a panel of criminals up here talking about what are the low-hanging fruit in the industry, to steal more identity theft. I know that we've certainly seen some evidence that because of our collaborative efforts, we've raised the bar. And so you do need some types of sophistication. The schemes that we're seeing are just-- it's very-- I think there's very-- we're seeing very few just kind of wholesale schemes. They seem to be-- retail-based, you have to-- they're so complicated that you have to spend a lot of effort to do it. The cost of doing business as a criminal, at least for tax fraud, is rising because of these efforts. I'm not saying, by any means, that we think we have a solid handle, but we think we have evidence on that we're moving in the right direction just because of the schemes that we're seeing are just so complicated. There's no way that you could do it at scale.

MARK EICHORN: Raising the costs for the thieves to do what they do.

A question from the audience, and I guess this could have been for the dark web panel as well, but I don't know if Christopher, in particular, can answer this. Is there any way an individual can check if their credit cards or other PII or PHI is on the dark web?

CHRISTOPHER MASCARO: That's actually a really good question.

Yes and no. I mean, as Danny mentioned in the panel, you can log into some of these sites, but they don't provide you the full information. Credit card sites, they'll provide you, as a consumer, the BIN, the last four, expiration, date, and state of compromise. Because of the team I run and the data we have access to, we're able to reverse engineer that to identify the card. Now on the PHI, PII side, they'll usually sell it either with a first name or a state or some demographic information. They won't actually just post it. Sometimes they do post samples out there just to demonstrate the type of data they have to say it's from a loan application, a mortgage application. And in those cases, you can look in some aggregators out there to see if your name is out there, but it's unlikely that you would know. I would assume that your data is probably out there, though.

MARK EICHORN: Now I can say there are sites that I've seen where they do provide that service. If there's a known breach where your data was included in that breach, you can find that.

CHRISTOPHER MASCARO: But those are focused a lot on credentials mainly, and like Have I Been Pwned I think is one or Have I Been Breached. I think more on the record side, I think it's-- those are less findable.

MARK EICHORN: So I guess another one for Christopher, and we sort of touched on this in the last panel a little bit. I guess what you foresee is the implications of the introduction of the chip technology and how that might change credit card exploitation.

CHRISTOPHER MASCARO: Yeah, so I think we've started to see a little bit of this just from the-- this actually would have been a good topic for the last panel too, that the type of shops that are out there that sell data-- there's a lot of shops that sell PII. There's a lot of shops that sell PHI. For the most part, there's been-- the data available on the payment card side has been mostly tracked data, so dumps compromised through POS. In the past six to nine months, we've seen more card not present data being sold. So I think EMV is having an effect there. I think we track-- and I'm sure Kenn's office does too, some of these discussions on the dark web around compromising certain technologies.

We've seen a lot of focus on EMV lately, but there haven't been any sort of confirmed successes of compromising it. One of the things with technology in the US is-- I mean, I ask people to say how many times have you dipped your card versus swipe your card in the past year and a half since EMV was introduced broadly. And for the most part, people still probably at least 50% swipe their card. So regardless of the technology, you're still exposing it in some way.

MARK EICHORN: Kenn, here's a question for you, and I guess it's sort of a question a lot of us have based on sort of this common idea that the criminals are located overseas and so forth and not findable. But the question basically is that, if we know so much about the criminals, why don't we prosecute them? And I think part of your answer is we do, but I don't know if you want to respond to that.

KENN KERN: It's a terrific question because how does someone in Iowa who's victims of some identity theft scam and the individuals are in Russia or some other place-- I don't want to pick on Russia, if they're over there-- I think both the federal government and the state government have, over the last couple of years, taken a different approach to analyzing this challenge, which is we should indict, pursue it through whatever grand jury process, get to essentially a criminal complaint or indictment, and then essentially wait for individuals to make mistakes because in the end, if you're engaged in this sort of criminal behavior, you're doing it because you want money. And then you have to hopefully spend money. So people want to travel. They want to go to car shows. They want to do all of this.

And what we have seen many times is if we just play the long game, which is we've got to have a set of eyes on a particular actor that we've indicted and track them via social media or other intelligence, eventually-- maybe not the first year, maybe not the second, but maybe the third year they decide to go to Spain to go to a car show that they've been wanting to go and they travel.

And this is a real life example for us where in the StubHub case, the individual decided to travel. We had a Russian analyst who caught that, was able to see that they were going to be traveling, and then we were working with the United States Secret Service where they had an asset in Spain to detain him and eventually bring him back to New York through a long process of extradition. That individual who led the StubHub is-- pled guilty and is still serving time in a New York state jail.

So it's a success story to say don't throw your hands up because they are located in China or somewhere else. Our colleagues in the Southern District on the cases involving Chinese have pursued indictments, and whatever will happen will happen. But from a law enforcement posture, that's the only responsible action we can do.

MARK EICHORN: Ann, when we did the prep call, Todd raised information sharing through the ISACs. I just wanted to give you an opportunity to talk about that in the health-related area. I mean, what do you see as the potential for more information sharing?

ANN PATTERSON: I think that's one thing that's really different from-- my background, I didn't mention, was I did for-- I worked for a long time in financial fraud, and so-- which is why I was brought on by the MIFA alliance to kind of do similar things in health care fraud. One of the big things that I-- and I didn't know anything about health care prior to that-- that I learned is that definitely within health care I think part of-- there's so many different factors. It's just health care is about keeping your medical information private, right. Doctors are tasked with not sharing your information. That's kind of-- not from a data or cybersecurity type kind of not sharing, but just in general you don't really share medical information, isn't something that's easily shareable even within a research university type kind of environment.

So that whole environment of health care being very, very hush hush, the laws are different, like I mentioned. And so all of these things kind of converge together, and it makes privacy-- and then there's consumer attitudes as well where consumers would freak out, I think, if they thought that their health care providers or their insurers were sharing some sort of information.

And so that-- it creates this whole environment within health care that is fairly tight lipped. That's very different from other industries, like financial services that have come to recognize that if we're going to fight fraud, we have to look at it as a noncompetitive issue. You can't say, I'm afraid to talk about the fraud that's happening in my hospital because then people will go to the other hospital and I'm going to lose business, and most hospitals in the US are nonprofit. So there are very thin margins that they're working with. So things like that that kind of come into play that make sharing very difficult in health care.

There is an ISAC. Health care is one of the critical infrastructures that we mentioned that-- Kenn mentioned that-- or I think Todd mentioned the Presidential Directive 63 where the ISACs were created. So there is a NH-ISAC, a national health care ISAC. It's fully stood up. It's not as robust as the financial services ISAC or some of the other ISACs. But there is an NH-ISAC. If you are part of the health care environment, I do encourage you to join the health care ISAC. Actually regardless of what industry you're in, you should look into the ISAC that's for your industry.

In terms of information sharing, particularly for cyber threats and physical threats, I think it's one of the great mechanisms to be able to get real-time information, to input information and to get that information fed back out to you, kind of like with the IRS and their tax ISAC, that-- it has the ability to reduce all kinds of fraud tremendously. But just in health care, we've got a lot of privacy concerns in terms of just when you talk about sharing in health care, people just tend to get really, really nervous because we're-- nobody wants their-- I don't want my medical information shared with anybody either, but yet I work in a place where I'm trying to encourage people to share more in some way to figure out what kind of legislative regulatory regime do we need that allows us to share that information so that we can track the fraud schemes, and not for the purposes obviously of finding out who's got what kind of diseases.

MARK EICHORN: Thank you. I have one last question. We're nearing lunch, but this is a question, I guess, for Mike and Todd. And so the question is that we heard earlier today basically about the advice that the IRS won't call you. So the question relates to the idea that there are sort of like some outsource, sort of like private collection efforts for taxes and that those folks might directly call taxpayers about paying their back taxes. Does that ring a bell?

MICHAEL BEEBE: Yeah, but generally what you will get is a notice from the IRS instructing you to call them. That's one of the things for audits and those sorts of things. We do not make out calls, and we've actually published that because we want people to make sure that-- because there's so many schemes out there. So you will generally get a-- well, you will, you'll get a notice directing you which phone call-- which number to call.

ANN PATTERSON: How do I know that letter's a real letter?

MICHAEL BEEBE: You can go to irs.gov and actually pull up the letter because sometimes-- yeah, we do have that, people will call us and say this letter doesn't look legitimate, and-- well, a case in our point, we sometimes will send-- we send-- when we select someone for our process, we'll send a letter to the taxpayer, and they will get this letter saying we received a return on your behalf. And they'll say, I didn't file a tax return. So that's where they're instructed to call us and basically tell us that they did not file it. Now, if they did file a tax return, then we have to go through an authentication process, but that's where they've received the notice. But to your point, sometimes they get it and they say, what's this notice? I didn't do anything.

TODD EGAAS: We also have that for agents. So a revenue agent or a CIA agent shows up at your door. How do you authenticate them? And there's a service on the website that helps a taxpayer do that. On the law enforcement side generally, you call up your local law enforcement because we do that coordination.

MARK EICHORN: Well, please join me in thanking the panelists today. Appreciate it.

[APPLAUSE]

MARK EICHORN: Were on lunch break and returning at 2:00 for the next panel.