IDENTITY THEFT: Outsmarting the Crooks

TRANSCRIPT (Edited for clarity)

NARRATOR: Welcome to "Identity Theft: Outsmarting the Crooks." This video presentation is brought to you by the United States Department of the Treasury. Here now is John Snow, Secretary of the Treasury.

SECRETARY OF THE TREASURY, JOHN SNOW: Hello. I'm John Snow, and I'm delighted to join you today to talk about a serious problem that's affecting America, and that's the problem of identity theft. Identity theft harms individuals and their families. It threatens to undermine confidence in our highly efficient credit system and, as a result, it imposes large and unnecessary costs on our economy.

Identity theft involves stealing your personal information – information like your financial account numbers, for instance – and then using that information to run up bills or accumulate assets fraudulently in your name.

Fortunately, there are things you can do. There are things we *all* can do to protect ourselves. This video helps to define that problem and to lay out steps you can take to protect yourself, or to repair the damage if you become a victim of identity theft. You'll also get a glimpse of how law enforcement is fighting back on your behalf.

I urge you to take the lessons of the video to heart and apply them in your own life. Thank you very much for watching.

VICTIM'S STORY: I was surprised that I was a victim of identity theft. I was a recent college graduate who was just starting out. I'd landed a job, managed my money and paid my bills on time. I had a credit card, but I didn't go overboard with it.

I should've been tipped off when I got a letter from some credit card company that I'd been turned down for a new card. It was odd, because I hadn't applied for the card, but I just shrugged it off as a computer glitch. A few weeks later, I got a welcome letter from *another* credit card company thanking me for opening a new account, but no card. I realized then that something was wrong.

I called the credit card company and was told the new card had been issued with a co-applicant, my neighbor. Not only that, but someone had spent over $300 shopping in another state. The company told me to file a police report, since they needed more verification before

they would close the account and delete the charge.

My neighbor was cooperative and said he would be glad to speak to the police. I called the local police, who took down my information, but they said the situation was difficult because the crime crossed state lines. I didn't know what to do, so I decided to contact federal law enforcement.

The investigation showed that the crooks would show up at my apartment building around three in the afternoon before most people would get home from work, and they would steal pieces of mail – bills, credit card applications and bank statements. My building has about 30 units. The mailboxes were outside, underneath a dark archway and organized into suites, so if you opened up one of the suites you had access to at least six mailboxes. After the investigation, we moved the mailboxes and secured them better.

MODERATOR: This is more than a cautionary story. It happens far too often. Somehow, someone manages to steal our identity, who we are, and opens up bank accounts, credit cards and loan accounts in our name, and then the imposter starts running up the tab. This crime is a tremendous waste of money and an enormous waste of time. Last year, victims spent over 250 million hours trying to sort out bogus accounts and set their credit record straight.

The United States Treasury asked two panels of experts to help us become more aware of the problem of identity theft, help us protect ourselves from the crime, and offer some tips about resolving the problem if we happen to become a victim.

You can watch the DVD straight through, or you can use the menu to watch any segment of the DVD in any order. Most importantly, we've included a Resource Library, a collection of materials – all sorts of reference information. Just pop this DVD into your computer to download whatever information you need. There's a list of web sites, too, so you can go online for even more information.

Well, let's get started. Our panel for the first segment includes Scott Parsons, Deputy Assistant Secretary for Critical Infrastructure Protection, from the Treasury Department; Special Agent-in-Charge Larry Johnson, Criminal Investigative Division, United States Secret Service; Anthony Demangone, Regulatory Compliance Counsel, National Association of Federal Credit Unions; and Alex Sanchez, CEO, Florida Bankers Association.

Scott, let's get right into it. What exactly is identity theft?

DEPUTY ASSISTANT SECRETARY SCOTT PARSONS: Identity theft is a fraud committed or attempted using the identifying information of another person without that person's permission or authority. Regulation under The FACT Act, the Fair and Accurate Credit Transactions Act of 2003, define identity theft in that way. And it's important, because the

definition is somewhat broad, but there're really two types of identity theft that we're talking about today. One is the actual hijacking of a person's identity to create new accounts, to go out and open new credit cards, to create a new banking account. That's one aspect of it.

The other aspect is actually credit card fraud, gaining your credit card number, or maybe some information that allows a person to complete a transaction using your credit card number. So, there are two different types of frauds, but they all have the same end result. Someone is trying to steal your information, and the thief is trying to steal money by using it.

MODERATOR: Alex, how can consumers fight back on this?

MR. ALEX SANCHEZ: You have to guard your I.D. like one of your biggest assets -- like you guard your home. You insure your home. You insure your car. Well, you have to make sure you take care of your I.D., as well.

MODERATOR: Anthony, how do we know if we've become a victim? What should we look for?

MR. ANTHONY DEMANGONE: The most common indication would be an unauthorized transaction. An example of that, I think Scott mentioned earlier, is credit card fraud. You can see a transaction on your statement that's not yours. It doesn't have to be a credit card. It could be your checking account. It could be a savings account. Again, looking at a statement, you're just going to see a transaction that looks fishy or you don't remember doing.

Now, the other problem is, though, sometimes with identity theft the crooks are actually going to open up new accounts. They're going to take your information and create a new account that you have no knowledge of. In a best-case scenario, you may find out within 24 hours. You may get a phone call. You may quickly learn that you're a victim. A worst-case scenario can take weeks, months. Some victims don't even find out until they get a call from a collection agency, wondering why the victim is not making payments.
MODERATOR: One of the techniques, I understand, is that after they steal it, they don't *act* on it, so you get kind of lulled into security, and then after a month or two, they come back and say – you know - *then* you get hit.

MR. DEMANGONE: Exactly. Something seemed fishy and, well, a week's gone by. Two weeks have gone by. You let your guard down and, like you said, the problem's just there waiting for you.

MODERATOR: Alex?

MR. SANCHEZ: Well, you know, I was going to say that the banking industry, the financial services industry, government and others are spending billions of dollars in technology to fight

I.D. theft. Yet, one of the best ways to combat I.D. theft is one of the simplest and most inexpensive ways, and that is consumer education. If we, as consumers – all of us, individually – act together, this is one of the simplest and cheapest ways to fight I.D. theft -- by taking the means to protect our own I.D.s.

MODERATOR: Scott, what kind of personal information is stolen, and what do the crooks do with it?

DEPUTY ASSISTANT SECRETARY PARSONS: Well, identity thieves are looking for anything they can use to create a profile to actually obtain financial instruments that they can then use to buy goods, services, or propagate other crimes. That includes your name, your Social Security number, and address. Date of birth is also an important one – all your basic pieces of information that you provide that identify who you are.

But they're also looking for other things, as well. We now live in this age of this wonderful thing known as the Internet, where people now have access to their accounts online, and so they're looking for your user name. They're looking for your PIN number. They're looking for any identifying information that they might find that they can use to gain access to your accounts, or to actually open new accounts.

MODERATOR: Yes, and we have a whole plethora of things that we deal with every day. I mean I went to the doctor the other day, and the receptionist required my Social Security number. And I said, "Do you need this to process this?" She said, "Yes, that's the way we track your records." And I said, "What about my *name*?" You know, "Is that any good?" She replied, "Well, we *could* use that, but it's much more difficult. We do it by the number." So, what do you do? Do you *not* give it to them?

DEPUTY ASSISTANT SECRETARY PARSONS: Well, that's an important issue. Right now there's a huge effort to remove the Social Security number as a primary form of identification for individuals.

I know in my own state, my home state, I used to have to give my Social Security number. It was right out there on my driver's license. But these days, many states have gone to using just a simple, different number, automatically so that people *can't* get access to your information.

MODERATOR: Larry, do you have something to say?

SPECIAL AGENT IN CHARGE JOHNSON: I just wanted to bring up, Paul, the point that you made about asking your doctor's office whether or not the staff needed your Social Security number. I think that's an important question that everyone must ask: "Is this something you absolutely have to have to identify my records?" If it's not, then don't provide your Social

Security number.

MODERATOR: Anthony, we've heard of a lot of different scams here and things. What other things might we look for?

MR. DEMANGONE: I think it's important we mention just to be aware of the situation. These crooks are going to try to gather the information in a number of ways. Eavesdropping is a big way. When you're at an ATM, be self-conscious if somebody's behind you. Shoulder surfing, looking over your shoulder, trying to gather PIN numbers – that's another way people gather information.

But, again, through consumer education, I think we can at least raise the bar and make it much more difficult for the crooks to take the information.

MODERATOR: There's a term called "skimming," which, frankly, I hadn't heard until fairly recently. Explain to us, Larry, what skimming is and how they do it.

SPECIAL AGENT IN CHARGE JOHNSON: Well, Paul, I brought a few things: a scanner, a skimmer and a parasite that has a skimmer attached. Now this scanner could be easily attached to the monitor here, this parasite. What the Secret Service has seen is that this can be attached or placed over top an ATM machine, and it could have the skimmer or the scanner. And when the customer swipes his card, looking to get money out of the ATM machine, something may come across the screen as "NOT OPERABLE," "OUT OF ORDER. PLEASE COME BACK LATER and, actually, that customer has already given the fraudster his credit card information off the back of his card.

MODERATOR: This is the interesting one here.

SPECIAL AGENT IN CHARGE. JOHNSON: The skimmers come in various sizes. They are sold for legitimate purposes, as well as fraudulent purposes. Now, this skimmer was taken from a waiter who, after making a transaction, he also palmed the skimmer and swiped a customer's card and downloaded the credit card information onto the skimmer. Now, this size of a skimmer will hold about 120 to 150 credit cards -- or credit cared information…. And then the crook simply sells that to someone who knows what to do with it. That someone in turn will download it to either a laptop or a personal computer and then sell it online, or even produce the credit card. So, we've seen pretty sophisticated credit card scams that deal with identity theft.

MODERATOR: Now my favorite topic: "dumpster diving." I just love the term. The alliteration is great there. Alex, dumpster diving?

MR. SANCHEZ: Oh, that is when someone will literally go through your garbage. We throw all our financial documents out – the statements from the bank that we get, our insurance

company information, other sensitive information. We just read it, and then we throw it out. Dumpster diving is when people later on go through your garbage while you're at work or asleep and take all this information; they retrieve it, clean it up, and then use it.

What can we do to combat that? Obviously, tear it up. Shred it – shred, shred, shred. Tear it up.

Make sure you read it, first of all. As Anthony was saying, I think when you get your statement, you want to go through it to make sure that there are no unauthorized purchases that have been made against your account. But once you read it, if you're going to throw it out with the garbage, make sure you shred it. That's very, very important.

MR. DEMANGONE: If I could build on one thing that Alex was just saying. He mentioned read your statement. Most credit unions and banks give you online access to your account, so rather than having to wait until the tenth of the next month, you can go online every few days and take a look at the transactions you've just done. It's going to cut down on a lot of time and expense related to identity theft. So, it might be something consumers want to take a look at.

MODERATOR: And the thieves don't have 30 days to work your account, if you check it every day.

MR. DEMANGONE: It will greatly cut down the time to spot some of the crime.

MODERATOR: Larry, I have this question for you now. From the dumpster to the electronic highway – and we just alluded to it with Anthony here – the Internet and something called "phishing" – this is with a "ph" – are raising concerns, aren't they?

SPECIAL AGENT IN CHARGE JOHNSON: Yes, Paul. I think that everyone has seen something on their personal computer in the e-mails that is "phishing." It basically is brand spoofing. It's just like fishing for real fish, and the fact is the fraudster is looking for someone to "bite." And, if the criminals are successful two out of every ten times in a phishing site, then they feel that they are successful.

What users need to be aware of is the need to check the URL, or the IP address, of the sender of the fake e-mail to see if it matches up with the known address of your bank, or an online auction, or whatever site that is being spoofed, or phished, by the criminal.

MR. SANCHEZ: On the point of phishing, my suggestion for our viewers out there is that when you do get an e-mail, and it has a logo from your bank and is asking for your account number, just delete it. Just delete it. Just delete it.

Delete it because no bank or financial institution will e-mail you asking for confirmation

of your account numbers. It knows you. The bank knows your account numbers. You don't have to confirm anything. Just delete it.
DEPUTY ASSISTANT SECRETARY PARSONS: The federal government will not e-mail you and tell you that you're not in compliance with the Patriot Act, and you need to provide your Social Security number. This will not happen.

MR. DEMANGONE: There is one thing also I was going to mention. It's similar to phishing, and it's just a widespread problem. Con artists will use a variety of scams that probably play on the lesser of our angels, greed, and it goes a little something like this: "Paul, you are a lucky man today. You are inheriting $100,000," or, "you've won a lottery. You're going to get $250,000, but here's the deal. We have some taxes up front, and we just need $500. You give us $500. We're going to give you $100,000." Or, maybe it's not $500. Maybe it's your Social Security number because, "Well, we just need to fill out some paperwork on our end."

If you see offers like this, the old saying is – it's still a good one: "If it looks too good to be true, it likely is." It's just another way that crooks are trying to get your personal information.

MODERATOR: So, lottery scams in that form. Are there any other nuances to that?

MR. SANCHEZ: You know that old saying, "Follow the money" and, "Show me the money"? Well, one of our most vulnerable groups is seniors. Usually, that's our largest affluent group in our society, because they've had many years to build up wealth. And that's who these con artists, as everyone knows on this panel, like to follow. So, we ask our seniors to please be very, very careful about whom they talk to and deal with. If it's too good to be true, don't believe it.

MODERATOR: Larry, we turn to you again as our law enforcement officer. How are we doing against this?

SPECIAL AGENT IN CHARGE JOHNSON: A few years ago, we saw a lot of misdemeanor crimes in dealing with identity theft. Now, folks are going to jail as felons. We've also seen just a year, year and-a-half ago, the passing of the Identity Theft Penalty Enhancement Act, which tacks on two additional years for any component of identity theft within a crime.

MODERATOR: So, law enforcement is doing a great job, we're hearing, tracking these criminals down, and their work is reflected in the success of prosecutions, as Deputy Assistant Attorney General Laura Parsky from the Criminal Division of the Department of Justice explains.

DEPUTY ASSISTANT ATTORNEY GENERAL LAURA PARSKY: Hello. I'm Laura Parsky of the U.S. Department of Justice. I'd like to share with you what the Justice Department is doing aggressively to prosecute identity theft crime. We have 94 United States Attorneys offices across the country, as well as criminal division prosecutors who work with federal agents to go

after identity thieves. Our job is to get these criminals behind bars and out of circulation.

Recently, we've been extremely successful in securing long sentences that are warranted by the damage caused by identity theft crime. In New York, for example, a man who arranged for the theft and sale of tens of thousands of people's credit reports received a 14-year sentence. In Washington, D.C., a man who led a $1.1 million identity theft and credit card fraud scheme also received 14 years in prison. A computer hacker in Charlotte, North Carolina, who broke into the computers of a major retail company to steal credit card information, was sentenced to nine years; and someone running a phishing scheme in Houston, Texas, was sentenced to nearly four years in prison.

Serious sentences like these are possible only because of solid investigative work from local, state and federal law enforcement agencies, such as the FBI, the United States Secret Service, and the U.S. Postal Inspection Service.

But we also need your help. If you are a victim of identity theft, the best thing you can do to serve justice is to file a police report. The more details you can give the investigators, the better the chance they can bring us a good case to prosecute. Together we can take the profit out of identity theft.
Thank you.

MODERATOR: I want to thank Laura Parsky and the Department of Justice for that video. Thank you very much. It's reassuring to hear that more of these folks are getting longer sentences.

Alex, what are financial institutions doing to help protect us and to help prevent this kind of crime?

MR. SANCHEZ: Well, it's the three C's: compliance, consumer education, and cooperation. First, compliance. Every bank has an IT program – information technology program. So, the banks are spending billions of dollars to ensure that that information is being kept confidential.

Again, you know, consumer education is very important. I would ask everyone to please take every safeguard possible within his or her control -- like shredding, like not leaving mail in the mailbox, like not answering the phishing e-mails and deleting them; and then, finally, there is cooperation.

Cooperation with law enforcement is critical. You know, at the Florida Bankers Association, the system has been created in cooperation with our law enforcement in Florida, now on a national level. Twenty-three states are using this system, called FraudNET, to share information with each other – the banks and law enforcement. So, the sharing of information is essential to get these people off the streets.

MODERATOR: Well, that's great. Now, that happened on the institutional level. Scott, what do we as individuals-- what can we do to prevent this crime, or at least lessen the opportunity for identity thieves?

DEPUTY ASSISTANT SECRETARY PARSONS: Well, individuals have a few, basic things that they can do that will dramatically lower the incidence of identity theft. One is checking your credit report. **T**hanks to the FACT Act, which was signed into law by President Bush in 2003, all consumers now have the ability to get one free credit report each year from all three credit reporting agencies. And a credit report is an important way to check to see if your identity's being misused by fraudsters.

There are a number of other things that you can do if you're a consumer. Don't carry your Social Security card around in your wallet is one. You've heard about a number of ways that consumers can behave. Check your mail. Read your credit card statements.

MR. SANCHEZ: But one other thing -- if I can just say -- is don't carry your PIN number for your ATM card and other PIN numbers in your wallet.

Just a note of humor - My PIN number is my favorite two baseball players of all time, the numbers that they wore on their back.

MODERATOR: Uh-huh. That's a tough one to get.

MR. SANCHEZ: Yeah. And so who are they? Only I know.

MODERATOR: Exactly.

MR. SANCHEZ: If you live at 1010 Mockingbird Lane, don't use 1010 as your PIN number.

MODERATOR: Right. Right. The common things that you would normally use – your birthday or things like that.
MR. SANCHEZ: Right.

MODERATOR: And it's a good bet that if you use it on one thing, you probably use it on 20 others, so you don't have to remember them all.

MR. SANCHEZ: Right.

SPECIAL AGENT IN CHARGE JOHNSON: And that also brings up the point of changing your password. I know that's a difficult thing, because you can't remember what your last password was, but updating firewalls and changing your password frequently are also good

practice.

MODERATOR: We talked about the credit reports, which are very important to get, and they're free. One a year is free from the three consumer reporting agencies. This is a good time to show you how you can get those reports. Stuart Pratt, President of the Consumer Data Industries Association, explains.

MR. STUART PRATT: Hello. I'm Stuart Pratt, President of the Consumer Data Industry Association. We represent consumer reporting agencies, or "credit bureaus," as they are often called. They maintain credit reports that help make it possible for you to get credit cards, mortgages, car loans and other forms of credit.

Reviewing your credit report is a valuable step to take. You should do this before making a major purchase, such as a home or a car. The Fair Credit Reporting Act ensures that you may always order a copy of your report from *any* consumer reporting agency and also provides a number of instances when you are entitled to review your credit report free of charge.

The easiest and fastest way to get your report free of charge is to go online at www.annualcreditreport.com. We believe an educated consumer functions best in the marketplace, and understanding your credit report and the information in it is critical to this process.

MODERATOR: That's very good advice. Checking your credit report is one way to spot identity theft before too much damage is done and to begin to clean up the record.

DEPUTY ASSISTANT SECRETARY PARSONS: If you are a victim of identity theft, you have free access to that credit report more than one time each year.

MODERATOR: Yes, because you want to keep track of it and what's going on.

DEPUTY ASSISTANT SECRETARY PARSONS: Absolutely.

MODERATOR: Anthony, any more advice on how to fend off the identity thieves?

MR. DEMANGONE: I think, as Alex mentioned, if you're a customer of a bank, if you're a member of a credit union, you will find they're doing a great deal to protect your identity, but they need your help.

If something seems wrong, if you're missing a statement – a statement hasn't shown up – contact your financial institution and see what's going on. Again, better to be cautious, better to be safe. And, finally, just don't leave information around. There are areas that you might think are secure. They might not be as secure as you think. Your workplace and your home – you

want to secure your financial data, receipts, statements. Just don't leave them out. Take your receipt from the ATM. Don't leave your receipt at the gas station.

Again, you can't protect against all chances of identity theft, but there are a lot of things consumers can do.

MODERATOR: What about, when we're using computers, about putting a PIN number to actually access the computer itself?

SPECIAL AGENT IN CHARGE. JOHNSON: I think it's also best practice, if you've gotten through the password protection part of your computer, but you walk away -- whether it's at home and you have people running around, or it's at work -- that you turn your computer off**.** Otherwise**,** it would be very easy for someone to come in and look at all your documents, or look in other places and find personal information. I even have a watch that, if that were the case, I could download it onto a thumb drive that I have attached to my watch band and walk out of your room or your office with some information.

MODERATOR: Gee, whiz!

MR. SANCHEZ: Well, one other thing. As we update our computers, and we buy a new one, it is recommended that you clean out your hard drive before you donate it to charity or to other groups, to a school, because there could be a lot of information stored in your hard drive that you've kept over the years that people can easily access once you donate it to charity.

MODERATOR: Right. Some people may say, watching this, "That's a great idea. How do I do it?" Talk to your eight-year-old grandson or kid. They'll know how to do it. Talk to somebody young, and they can do that for you.

MR. SANCHEZ: Right, right. [laugh] [laugh]

MODERATOR: Okay. We've talked about some sophisticated things here now, but there's still more that we need to emphasize, Scott, like, you know, signing new credit cards as soon as possible and things like that.

DEPUTY ASSISTANT SECRETARY PARSONS: Well, that's one of the most important things that you can do. Just sign your cards. It's a verification mechanism that people can use to make sure that it really is you. They match signatures. Another thing that's emerged that I actually think is a very good idea: I've seen more and more merchants lately asking for I.D.s when you present your credit card. That is not a bad thing if you're a consumer.

But a couple of other things. Anthony mentioned the ATM transactions earlier. Make sure that people aren't looking over your shoulder to try to get your PIN number. Finally,

solicitors don't need your personal information. They don't need your Social Security number. They don't need your credit card number. If someone's just calling, and we've heard stories about that today, of phishing instances – people asking you to provide this information – you don't need to do it. Your financial institution knows your customer information. If you get that request, the best thing to do is to hang up, or to log off and contact your institution yourself and find out if that really is the case.

MODERATOR: These are some straightforward things to do to protect your information and yourself, but what happens in a disaster. Alex, you're from Florida. You know a lot about this.

MR. SANCHEZ: Well, this is something that everyone should do, no matter where you live, whether you're in an area or a zone where disasters could happen, or not. It doesn't really matter. Everyone should look at home and, in a simple manila envelope, put in that manila envelope birth certificates, other sensitive documents like financial account numbers, and other identification documentation that you may have. Put it in that envelope, and put it in a drawer where you can remember to retrieve it.

These are difficult times when these disasters happen, whether it's floods, hurricanes, earthquakes or other things. Be ready to take that manila envelope with you in time of evacuation, so you'll have those important sensitive documents with you.

MODERATOR: Now, what would happen if you didn't do that?

MR. SANCHEZ: You'd have to begin rebuilding your ID. It's not too difficult to do. The first thing you do is to call your financial institution and let the people there know what happened. Obviously, you need to talk to the state authorities, *e.g.,* the driver's license bureau. Call other government agencies -- the Social Security Administration and other state and federal agencies. In times of disasters, all these groups gear up to provide an even higher level of service than usual because they know that the demand for their services will be extremely high.

MODERATOR: And they may be asking you some more detailed questions, because you have *nothing* to go from. So, you should not be cautioned against that, because in this case it may be necessary to provide some sensitive details.

MR. SANCHEZ: That's right. The governmental agencies and financial institutions understand that in these difficult times of disaster recovery you may have lost sensitive personal information and identification, and they will help you regain your ID.

MODERATOR: But, at the same time, you have to be careful that you're not being scammed by somebody who calls you when you are in distress and claims to be from the government or your financial institution.

MR. SANCHEZ: Right. In the case of the government, they know your Social Security number. In the case of a financial institution, they know your account numbers. So, be leery about who's on the other side of that phone call. Do not give out your credit card numbers or your Social Security number.

MODERATOR: It seems, Alex, that our Social Security numbers, as you talk about, are used to establish our identities in so many areas. So, how important is guarding our Social Security numbers in fighting identity theft?

MR. SANCHEZ: It's very important. The cornerstone of any financial institution is to safeguard your information.

MR. DEMANGONE: And I think also it's important to know that a lot of the organizations or institutions that are asking for your Social Security number, they may be doing it out of habit and not out of necessity. If you're looking at an application form and it doesn't seem obvious why your Social Security number is needed, you know, take charge. Ask, "Is this absolutely necessary? I'd rather not give it out." I think you'll be surprised to find that many times, the institutions or the entity doesn't need it and won't mind if you keep it private.

MODERATOR: But financial institutions *do* need that information.

MR. SANCHEZ: Well, Paul, that's true. Obviously, financial institutions need your Social Security numbers for the reporting that they have to do the government for tax purposes and other identifying purposes.

MODERATOR: The caution there is you have to use your head and not just give this out willy-nilly to everybody. But, there are places that you would need to do that.

MR. SANCHEZ: That's correct.

MODERATOR: The IRS uses your Social Security number as your taxpayer I.D., in fact, and we've gone to the Internal Revenue Service, a bureau of the Treasury Department, for more about our Social Security number and our taxes.

MS. JULIE RUSHIN: Hello. I'm Julie Rushin from the Internal Revenue Service. Did you know that your Social Security number can also be used by identity theft crooks to file tax returns and get refunds using your name?

What if someone used your Social Security number in order to get a job? That person's employer would report W-2 wages earned using your information to the IRS, so it might appear that you did not report all of your income on your real return.

What if they filed a tax return with your Social Security number in order to receive a refund? When you file your real tax return, the IRS will believe that you have already filed, received your refund, and that a real return is a second copy or a duplicate.

When it comes to your tax records, if you do not prepare your own return, be careful in choosing your tax preparer, as careful as you would be in choosing a doctor or a lawyer. That person will have access to your personal financial records.

You should also know that the IRS does not communicate with taxpayers through e-mail. So, if you receive any request for information in that format, it is fraudulent. Knowing these simple rules can help prevent identity theft.

If you do receive a notice from the IRS that leads you to believe someone may have used your Social Security number fraudulently, please notify us immediately by responding to the person's name and number printed on the notice. Our tax examiners will work with you and other agencies, such as the Social Security Administration, to help resolve these types of problems.

The Taxpayer Advocate Service can also help. If you've attempted to resolve your problems through our normal processes and are about to suffer a significant hardship, the Taxpayer Advocate Service has expert resources that can assist you. Go to our web site at www.irs.gov and select the link at the bottom of the page for Taxpayer Advocate to learn more, or call the toll-free number at the bottom of the screen: 877-777-4778.

Finally, at the IRS, as we become aware of identity theft schemes that target taxpayers, we will issue public warnings so you can be on guard for these schemes. You can find those warnings on our web site, along with information about recent criminal prosecutions of the perpetrators of identity theft schemes that relate to tax administration.

MODERATOR: Thanks to the IRS for educating us all on that matter. So far, we've heard about some of the ways crooks can steal your identity, your credit and numbers and banking accounts, and we've just heard some of the things we can do to help protect ourselves. I want to thank our panel, Scott, Alex, Anthony and Larry.

In our next panel discussion, we're going to learn where to go for some help. And this is a good time to remind you about our Resource Library. Just pop this DVD into your computer to download whatever information you need. There's a lot of web sites, too, so you can go online for even more information.

NARRATOR: It's important that you check your credit reports regularly. Everyone can get a free report once a year from all three, nationwide consumer reporting agencies, or credit bureaus: Equifax, Experian, and TransUnion. Contact their centralized response system to obtain this free

annual report at: www.annualcreditreport.com.

Secondly, there are certain conditions under which you can request a free report from any credit bureau. If you are unemployed and seeking employment, receiving public welfare assistance, or if you believe information in your credit file is incorrect due to fraud, you can request a free credit report from any consumer reporting agency by contacting them directly. Also, if a company denies your application for credit or insurance, for example, it must notify you of the adverse action. The "adverse action" notice will tell you how you can request a free credit report from the appropriate credit bureau.

Finally, if you suspect you are, or are about to become, a victim of fraud, including identity theft, you can put a fraud alert in your credit file and get a report from each of the nationwide credit bureaus. You just need to make one call to one of them to trigger this service. Whichever one you contact will pass your information to the other two. Here is the contact information for those credit bureaus: Equifax … Experian … TransUnion. Of course, you can also buy your report at any time, and you can subscribe to credit monitoring services.

More details about credit reports can be found in the Resource Library and by going to www.consumer.gov/idtheft.

VICTIM'S STORY: The federal agent I contacted was very helpful. He filed a report, which I took back to my credit card company. That formal report was important to clearing up the mess. I found out that someone had also tried to withdraw money from my checking account, *and* somebody tried to open a couple of online accounts in my name. The thief didn't get away with it, though. Banks and credit card companies are getting pretty smart at detecting these things.

When I got that first rejection letter, I should've contacted the credit card company to learn what I could about the false applications. Fortunately, I did contact one of the major credit bureaus to place an initial fraud alert in my report. I'm really glad that I did that. The alert warns prospective creditors that you may be a victim of identity theft or other fraud.

Actually, a few weeks later, a credit card issuer called me to verify more information after I applied for a card. They said they probably wouldn't have called me if the alert had not been on my credit report.

Because I caught the problem relatively early, it was more a hassle than anything. I didn't lose any money, and my credit rating is okay. Still, it's an experience I really didn't need.

MODERATOR: In the last segment, we looked at a number of steps people can take to try to prevent identity theft. In this discussion, we're going to hear about the resources you can turn to, to protect your information and take action if you think you may be a victim. To help us with some of the answers, we have with us Nessa Feddis of the American Bankers Association; Betsy

Broder from the Bureau of Consumer Protection at the Federal Trade Commission; Michael Desrosiers from the U.S. Postal Inspection Service; and Howard Schmidt, former cyber security advisor to the White House, currently serving as a Special Agent, U.S. Army Reserve, for the Computer Crime Investigations Unit.

MODERATOR: Howard, I'd like to follow up on the cyber security issue that was raised in the phishing segment earlier. Are people being discouraged from doing business or banking online these days because of the fear of identity theft?

MR. HOWARD SCHMIDT: Generally not. I think today we're probably safer online now than ever before, but there are still some things we need to pay attention to, to better protect ourselves online.

MODERATOR: Okay. What about phishing. Is that still a problem, though, on the Internet?

MR. SCHMIDT: We've seen the number of phishing e-mails going out increase, but we're actually seeing the number of victims going down, which is a good thing, because people are basically becoming more aware of their surroundings and what they need to do online.

MODERATOR: Although they are getting more sophisticated.

MR. SCHMIDT: Absolutely, they are.

MODERATOR: The United States Secret Service has a report that shows us examples of phishing e-mails for your edification.

SPECIAL AGENT STANLEY CROWDER: Hello. I'm Special Agent Stanley Crowder of the United States Secret Service's Electronic Crimes Taskforce. I want to talk to you about phishing, spelled with a "ph." It is a popular scam that can trick you into revealing confidential information about yourself that could be used to steal your money and, even worse, your identity.

Phishing is usually done through junk e-mails that are sent to hundreds of thousands of people at a time. Spam filters catch most of them, but some get through to you.

Let's say you get an e-mail that looks like it is from your bank. It says that the bank is undergoing a computer upgrade and needs you to go to a web site to verify and enter some information. The e-mail looks just like other, legitimate
e-mails that you might have received from your bank. It has their logos and color scheme. The link in the e-mail will even take you to a web site that looks just like your bank's.

But the fact is the e-mail and web site could both be fake. Crooks are copying, or

"spoofing," graphics from the bank's real web site to make their e-mail look legitimate. Here's what the crooks are phishing for: information like your name, address, and phone number; your Social Security number; date of birth, or your mother's maiden name; account numbers and online banking information, like your password. They will even try to get your card expiration dates and the security code printed on the back of credit and ATM cards.

About 65 percent of all phishing attacks have mimicked a financial institution. Others pretend to be from organizations, such as the Federal Deposit Insurance Corporation, the agency that insures your bank and thrift deposits; the Internal Revenue Service; computer software companies; or e-commerce sites. Phishing has become so popular among crooks, it is wise to assume you may get one of these bogus e-mails.

First of all, never respond to an e-mail from anyone soliciting personal or account information. If you do not initiate the communication, do not give this information, regardless of how legitimate or genuine the e-mail appears to be.

Second, visit a web site only by entering the web address into your web browser, not by clicking a link in an
e-mail. When contacting your bank, for example, use the web address listed on your monthly statements or other literature from the institution. Remember, your bank or credit card issuer should already have all the information they need. They shouldn't be sending you an e-mail asking for it.

By recognizing these fraud schemes, installing and updating your anti-virus and anti-spyware software regularly, and spreading the word about Internet phishing, you can help prevent these crimes. It's up to you. Don't be the bait.
For further information, or to report phishing, contact your local law enforcement agency, or contact the nearest Secret Service office listed in the front cover of your telephone book. You can also visit the Anti Phishing Working Group web site at www.antiphishing.org, or the Federal Trade Commission's web site at www.ftc.gov.

I want to thank Agent Crowder and the Secret Service for that video. Howard, that sounds pretty crafty. What's being done to stop the phishers – or, the phisherman, or if you want to call them that.

MR. SCHMIDT: Well, there're basically four categories of things that are being done. One, first and foremost, is new technology. We're starting to see different companies, whether they're e-commerce companies, or operating systems operators, even small companies, developing new technologies to help fight phishing.

The second thing is the institutional perspective, where companies are working better together, security groups from one company calling another one, saying, "By the way, we see

something that affects your company" -- that sharing of information, which is somewhat natural.

The other thing is the education awareness, and this is really a big part, because we can make really, really safe cars, but if you drive them too fast, you don't put brake fluid in, you're going to have a problem. So, educating people about what to watch out for is the third piece of that.

The fourth one clearly is the law enforcement piece. If the first three are not 100 percent successful, which we never really expect them to be, law enforcement has new tools and new mechanisms by which to investigate these things and hold these criminals accountable.

MODERATOR: Howard, I have another question for you. What about the software itself?

MR. SCHMIDT: In a lot of cases, for example the browsers - the interface that we have between us and the online world – a couple of things take place on that. One, first and foremost, you need to keep that updated. It's vitally important to do so, and we talk about this all the time. You need to make sure you use the anti-virus software. If you have a high-speed connection, such as cable modem or a DSL system, have a personal firewall that you use. There are now suites of software out there that include anti-virus, anti-spyware, anti-spamware, personal firewalls all built into a single package, which are very, very easy to use.

We're also seeing now the proliferation of new gateway devices. For example, when you use a cable modem or DSL modem, those are now coming built in with wireless connections and software in the device, so there's even less for you to manage.

MODERATOR: Now, URLs, for example, we have to look at the URL – the e-mail address -- and not just click back on it, because it may not be where we really want to go. How many of the institutions or people we deal with have the "s" on the end of the "http," which indicates a secure web site?

MR. SCHMIDT: That's correct. It basically is an encryption or a scrambled connection between your desktop and theirs. Any time you're doing some sort of a transaction that involves either credit cards or money, look for the presence of that "https," and make sure that you've typed in the URL yourself, the universal resource locator. Don't take one where you get one in the e-mail that says, "Click here to update your information." It may have an "s." It will not be a *legitimate* "s."

MODERATOR: *Ah*.

MR. SCHMIDT: So, type it in yourself: www.mybank.com -- whatever the name of it is, so you know that you're legitimately there. Look for that "s," and also look for a little lock mark. On the lower right-hand corner of your screen normally is where the lock icon is currently

placed, and it shows that it's an encrypted session.

MODERATOR: Okay. Nessa, crime is crime, whether it's online or offline, right?

MS. NESSA FEDDIS: If a consumer thinks that he or she may have provided information to a phisher, the information provided will determine what steps the person should take. If the individual provided account information, credit card information, debit card information, the person should immediately contact the financial institution. That individual may have to close the account down, get a new credit card, et cetera. But, consumers should be looking for transactions they didn't make, and if they find that there are transactions that they didn't make, they should immediately contact their financial institution.

In most cases, these are resolved fairly quickly, but the more quickly they notify the institution, the more quickly and more easily it is that the issue will be resolved.

Now, in a phishing incident where you're not providing account information, but personal information - such as your address, Social Security number, date of birth, mother's maiden name, all that information that could be used to open an account in your name - you may want to take a different step. It might be a good idea to put an alert on your credit report so that a lender reviewing an application will make sure that they'll take extra steps to ensure that the person who's applying for a loan in your name is, in fact, you.

And, in addition, if you provided that personal information, you might want to periodically review your credit report to ensure that accounts were not opened in your name.

MODERATOR: Okay. And that takes care of phishing. Howard, there's something new called "spyware." I thought that was a *good* thing.

MR. SCHMIDT: Well, not necessarily – no. Spyware ranges from one spectrum, where it actually, without your knowledge, installs software on your computer system and actually captures your keystrokes. So, for example, if you're going to your bank and you type in your user ID and password, it would capture that and transmit it someplace else, and someone then could become *you* at that bank. And it could also be the other spectrum, where it just tracks your activities through the Internet for marketing purposes.

Oftentimes, you don't know you do this. You think you're downloading a good game, some sort of a geography program, something like that, and in the background it installs the spyware. And one of the things you really need to be cautious of when you download software like that is take a real good look at the licensing agreement that is posted. Make sure that basically you're getting what you think you are, and nothing extra.

MODERATOR: So, what can we do about that? I mean what do we do about spyware?

MR. SCHMIDT: Well, there're a few things. One, first and foremost, anti-spyware software is currently available, which
is easy. It's part of the security suites that are currently available out there. Using software, particularly for younger members of the family – parental control software actually
blocks that sort of activity, as well. So, there're two mechanisms to do it.

MODERATOR: Well, we go from the "in box" to the "mailbox," Michael. Presumably, we need to be careful in using the regular U.S. mail, as well – right?

POSTAL INSPECTOR DESROSIERS: That's right, Paul. The U.S. Postal Service delivers mail to approximately 142 million addresses every day. Most of those deliveries are made to the typical, American mailbox that you find located on the rural routes, at the end of your driveway, or located at the curbside, and most of those mailboxes – those typical, American mailboxes – are unsecured. They don't have any locking device at all, and that is what makes them a target for thieves, potentially.

And the potential gain of information from that theft of mail is enormous. We don't think a lot about what goes in the mailbox and what can happen to that mail if it's stolen by the thieves. Things like checks, credit cards, monthly statements, and driver's licenses all go into the mailbox. In the mail is included your name, address, Social Security number, your telephone number, your date of birth, account numbers to your bank accounts, account numbers to your credit cards – all of which can be used by the thieves to conduct an identity theft scam for their own personal benefit and gain.

MODERATOR: Boy. And so you're really hanging out there
with all that information. Now, what do we do to protect ourselves from that?

POSTAL INSPECTOR DESROSIERS: Well, first of all, for incoming mail – that's mail that the Postal Service is delivering to your mailbox – the Postal Service recommends that once the letter carrier delivers that mail to your box, that you remove that mail promptly. The longer the mail is in the box, the greater the chance that thieves can come by and steal it or tamper with it. So, remove that mail as soon as possible.

MR. DESROSIERS: Second, we would recommend getting a mailbox with some type of security, some type of lock attached to it.
And thirdly, another option **i**s getting a post office box at the post office. There is no safer way to get your mail delivered to you. The mail never leaves the post office.

MODERATIOR: What about when you're sending mail out? How should you handle it?

MR. DESROSIERS: The outgoing mail – that's when you are putting mail into the mail stream,

you're sending a letter to your cousin -- then people put that mail in their mailbox at the curbside, their unsecured mailbox at the curbside, and they'll put that red flag up. Now, we all know what the red flag is for. It's so the letter carrier the next day, who's delivering mail on the route, will see the red flag up, and he'll know that means that there's outgoing mail in the box.

However, it's also a good indicator to the mail thieves, who are looking for an opportunity to steal something. They're going through a neighborhood. They see that red flag up, and it's like it's saying, "There's mail in me. Come and get me."

So, we urge that if you're going to use your personal mailbox for your outgoing mail, that's okay, just don't put that red flag up. What we would prefer you do is you take your outgoing mail to the Postal Service – the big, blue collection boxes that you see on every street corner. Or, bring it to the post office itself. That is the safest way to get your mail into the mail stream.

MODERATOR: It's encouraging to hear that there's so much we can do to help ourselves fend off the identity thieves, but some of us are going to become victims anyway. Betsy, what should we do when we think we are a victim of identity theft?

MS. BETSY BRODER: If you think you are a victim of identity theft, you have to take action and take it quickly. So, the first thing you need to do is contact the credit reporting agencies. These are the people who keep records of how you pay your bills and the accounts that are open in your name. So, you contact them, and you let them know that you believe that you are or may become a victim of identity theft, and they should put a fraud alert in your file.

The second thing you need to do is contact the financial institutions where the accounts were opened in your name, or may have been used – a credit card used in your name, or withdrawals from your bank account. Contact that company. Probably, you'll want to do it quickly by phone initially, but follow up by mail – certified letter sent to them – and keep good records of everything that you've done.

The third thing that you need to do is contact your local police department. You're a victim of a crime, and you need to have a record of this. When you go to the police, explain to them in detail what has happened, and ask for a copy of a police report, and that's going to be essential down the line.

MODERATOR: I was just going to say that's important, you know.

MS. BRODER: Right.

And finally, the fourth thing you need to do is contact the Federal Trade Commission. We have a lot of resources for victims of identity theft, the steps that they need to take towards

recovery and how to minimize the harm to themselves, and lots of tools for them to use. We also have an online complaint form and a toll-free number for victims to use.

Those are the four steps.

MODERATOR: Okay. And you need documentation in how many of those cases?

MS. BRODER: Well, every time you send out a letter, you should keep a copy of the letter. You need to keep a copy of any documents that are indicative of the fraud. That is, you may have gotten actually a bill from a credit card account that was opened fraudulently in your name. Of course, you need to keep that and keep meticulous records of every step that you take, from contacting the police to contacting the financial institutions, so that if any question arises, you can establish what you've done and when.

MODERATOR: A paper trail. Okay.

MS. BRODER: Yes.

MODERATOR: Well, financial institutions are certainly an important aspect of that, Nessa, and what can we expect?

MS. FEDDIS: As Betsy said, you want to contact the financial institution as quickly as possible. Phone and then follow up with a letter.

What you'll expect in most cases, is that they'll have to close the account. Now, if it's an account that's been misused – maybe a unauthorized debit card transactions, or some sort of access to an account that the victim did open – this means that they'll probably have to get new checks, new debit card and PIN; or, if it's a credit card account, new credit card, new online passwords, et cetera.

Some people may have to take some additional steps. Many people have arranged to have certain payments – their mortgage payment, their utility payment – automatically deducted from their checking account electronically, or paid by credit card each month. They need to contact those companies to ensure that their payments continue and that they're not late and don't run into some trouble there. So, they need to contact those companies with the new information.

In other cases where the fraudsters opened an account that the victim was unaware of, or they've really taken over an account with prolonged use of an existing account belonging to the victim – maybe they've changed the address to divert the monthly statements – that's a little bit more serious. The account, of course, will be closed; but, presumably, you don't want a new account number for an account that has been taken over or established without your knowledge. In those cases, you do want to place an alert in your credit report so that when another creditor

gets an application, he will know to take a couple of extra steps to ensure that the person who's applying for credit is, in fact, you. And it's also a good idea in those cases to pull your credit report on a periodic basis to ensure that no other new accounts have been opened in your name, and that the fraudulent accounts are no longer being reported.

Time is of the essence. The FTC studies and other studies have shown that when the identity theft is caught quickly, there is less inconvenience. There is less cost for everyone. So, time is absolutely of the essence.

I would also recommend very much the FTC web site. There's a lot of good information in there, and they have the affidavit. They have other tips on how to prevent identity theft and also what to do if you're a victim of identity theft.

MODERATOR: I think they have sample letters, too, that you can send to the institutions, you know, as part of the package, so you know how to –

MS. BRODER: We believe that the best way for consumers to resolve these issues is to take control of them, themselves. So, as you say, Paul, there are sample letters to send to creditors and the credit reporting agencies to dispute fraudulent accounts. There are affidavits that Nessa referred to, that you can use – again, a standard affidavit that you can use - for multiple creditors and financial institutions to dispute these fraudulent accounts. We want to make it easier for victims to work through what is a very stressful situation.

MS. FEDDIS: I would just add about the affidavit that the affidavit is a very good start, and the financial institutions appreciate the uniform affidavit. But victims should also expect that they'll probably have to supplement that affidavit with other information about the specifics of the transactions, specifics of the account, and that could vary, depending on the situation.

MODERATOR: Betsy, Nessa's talked about the financial institutions. Give us a little more detail about how we deal with the credit bureaus in an instance like this.

MS. BRODER: There're key players if you're a victim of identity theft. So, there're three, major credit reporting agencies, and if you realize that your information has been obtained and can be misused, or actually has been misused – let's say your wallet is stolen and it contained documents with your Social Security number, date of birth – you may want to put an alert in your credit report file, because someone could use that information and use it to commit identity theft. We used to think that if your wallet was stolen, the worst thing that could happen is that the thieves would take your money. It's now a little more treacherous, because they have your information, which also can be misused.

So, there're three, major credit reporting agencies, and you need to make sure that each of them places an alert on your credit file. The good news is you only have to call one of them.

Now, the FTC's web site that Nessa referred to is at www.consumer.gov/idtheft. And on it, we list the contact information for the three, major credit reporting agencies. You call one of them, and you say, "My information has been obtained. I feel like I'm at risk for fraud. Please put a fraud alert on my file." That agency will contact the other two and transmit to them the request for the fraud alert, so you only have to make the one phone call.

After the alert is in place, they will also make available to you a free copy of your credit report.

MODERATOR: If you do not suspect fraud, can you still get one free credit report a year?

MS. BRODER: You certainly can. Under federal law, you're entitled to a free credit report, regardless of whether you're a victim of fraud. It's good for maintaining your financial health, so you can establish that the information is correct.

Sometimes mistakes happen. Sometimes there's more than one Betsy Broder, and unfortunately I may get her information in my credit file. I want to make sure that everything in that file is accurate, because the next time I go in to refinance my house, or finance a car, I want to make sure that my credit is in as good shape as possible.

POSTAL INSPECTOR DESROSIERS: Betsy, if you're a victim of identity theft, would you get where you need to go if you log on to www.ftc.gov?

MS. BRODER: Yes, if you go on to our home page for the Federal Trade Commission, there is a link for the identity theft page. We also have a toll-free number for victims of identity theft, which is 877-IDTHEFT.

MODERATOR: And by the way, all of you watching, all of these dot-govs and all of the things we're talking about are part of our resource file in the Resource Library, which is part of this DVD.

MODERATOR: Howard, there are thousands of men and women in the National Guard or any of the Armed Services, who might not be able to pick up the phone and do what we've been talking about here. What do we do about that?

MR. SCHMIDT: Well, there was a special provision in the FACT Act of 2003, which we discussed earlier today, that had a specific what we call "active duty alert" in there. So, if the

men and women who are serving in the military – whether it's active duty, National Guard, Reserve – are deployed somewhere else, they can call the credit bureau -- one call applies as well, because it applies to all three credit bureaus – and let them know that they want an active duty alert in their file. And it does a couple things. One, it stays in there for one year. It's renewable if they're deployed longer. But, it also gives the merchants and the lenders notice to, basically, scrutinize credit applications a little bit better, because it may or may not be from that person, because that person is out serving somewhere.

Better protection that's vastly needed for the military folks that are deployed.

MODERATOR: Betsy, that brings us to the third point of your original four, and that is, how do we, and why do we, and what do we do when we report to law enforcement officials?

MS. BRODER: Well, you can report to your local police department. And, in fact, we advise consumers to do that. Report where you reside. And police departments are supposed to take the report where you reside. It's important for a couple of reasons to go to the police and report this crime. First of all, you want them to investigate. You want them to follow up, so there needs to be a record of this.

You also should get a copy of the police report that documents your complaint, and this, again, serves two purposes. First of all, it establishes that you're a *bona fide* victim of a crime, so that if someone tries to collect on the debt that was incurred by the thief, you have some documentation that, "That's not me. It was someone else." And there're even more serious cases where someone who was a victim of identity theft finds that the bad guy has used the victim's name in committing a crime – right? And so you have the police report that establishes that you were a victim of a crime, and you're not the bad guy.

But also, the police report itself is of great value in resolving the problems of identity theft. So, under the law, if you have the police report, you can take some important steps to clean up the financial damage done by the identity thief. The first is you can strike from your credit report all of those fraudulent accounts. So, you provide a copy of the police report to the credit reporting agencies, and they should block those accounts that you've specified that were the product of fraud.

It also makes it a lot easier to get copies of the documents that were used to open up the fraudulent accounts. Let me just spin that out a little bit.

MODERATOR: Sure.

MS. BRODER: Okay. I'm a victim of identity theft. Someone goes to the department store and opens up an account using my name and my information and I start getting bills on this. And I want to dispute that account, so I call up the department store, and I say, "This is fraudulent. I

am not responsible for this debt, and I would like to see a copy of the application for the account" And the store employee says, "Well, you said you didn't sign this application. It's not yours, so we're not entitled to give it to you, but you also need to pay your bills."

Well, Congress recognized that was a real problem. So, if you have a copy of the police report and you can provide it to the company with other documentation that the merchant may require, the company will give you a copy of that application. You can also authorize law enforcement to get access to that information without a subpoena. So, the police report is going to allow you to block fraudulent information on your file. It's going to give you access to these documents that were used to commit the fraud. And also, if you want to get a seven-year fraud alert on your file, because you have, in fact, become a victim, the police report will help you with that.

MODERATOR: Great. Sounds great. Michael, should we call you if something happens if we're victims.–

POSTAL INSPECTOR DESROSIERS: You should definitely call the Postal Inspection Service. For those who don't know, the Postal Inspection Service is the federal law enforcement agency of the U.S. Postal Service. We are the guys who are responsible for investigating all the federal violations dealing with the federal statutes that apply to the U.S. Postal Service and the mail. So, we are the guys who investigate all the mail fraud scams, all the thefts of mail and about 200 other federal statutes.

So, if you have been a victim of identity theft, I encourage you to contact us, and the best way to do that is through our web site, www.usps.gov/postalinspectors. When you log onto that web site, you'll be able to find your nearest Postal Inspector address and telephone number.

MS. BRODER: Can I add something here?

MODERATOR: Yeah, sure. Um-hum.

MS. BRODER: Because I know these cases get prosecuted, because every time I see Mike, he tells me about new cases that he's working on. And that's really encouraging.

But sometimes – you know, we talk about "go get a copy of a police report," and it sounds fairly simple. Sometimes, consumers may have trouble getting that police report, and so the advice that we give to them is, "Be persistent." Be persistent. Keep going back. Tell your local police department, "The FTC and the financial institutions tell me that I need a copy of a police report." If they're not able to get it from their local police departments, they should investigate other law enforcement agencies in their jurisdiction, either on the federal level, or maybe their state attorney general's office. But, again, it's essential that they do get a copy of this police report.

MODERATOR: I think the things we've talked about seem logical. Some people might wonder why the FTC element is so important. Betsy?

MS. BRODER: We're there for the consumer. We're there for the consumer. We work very closely with law enforcement. We work very closely also with industry and with technology. But, we understand that consumers also have a lot that they can do both to protect themselves, to minimize their risk of identity theft, and in recovery.

I mentioned earlier that we have a web site at www.consumer.gov/idtheft that has an online complaint form. Now, a couple things happen when people come to our web site. As Nessa said, they get access to our affidavit. They get access to a lot of material to take them through the steps of recovery. But we want something from them, and that is all the information that they've been able to gather about how this crime occurred, because we put it into a database that we share with over 1400 other law enforcement agencies around the country.

So, we get all of this complaint data into the system, and then someone like Mike Desrosiers in the Postal Inspection Service, he gets a complaint that comes across his desk. And then he can go into the FTC database, and he can put in whatever features, whatever facts that he has and investigate it and realize it's not just that one incident of identity theft that was reported to him, but maybe there're five other people who've put in complaints. So, suddenly he has a bigger case, a more robust case, which is easier to get prosecuted. And when you do get it prosecuted, a conviction is more likely to give you a major sentence for that suspect. So, it works all around for everybody.

MODERATOR: So, that's it. We call the institution, number one. Two, contact the nationwide credit bureaus for a fraud alert and free credit report. Three, file a police report to use in clearing up disputes. Four, let the Federal Trade Commission know about it. Anything else?
MS. BRODER: Well, let me just add one other thing that we haven't touched upon. Sometimes people find out about identity theft because they're contacted by the merchant, who says, "An account has been opened, but it seemed a little fishy." Sometimes, you find out when you look at your credit report. Sometimes, people find out when they're contacted by a debt collector, and it's only then that they realize that someone has gone on using their good name to open up new accounts and run up a lot of debt that has been referred to debt collectors.

Now, under federal law, you have the right to get the information from that debt collector about the nature of the debt, what it's all about, information about the debt collector itself. And that's the way you're going to find out about this fraudulent account so you can take those other steps to dispute the account.

So, all of this information is in the Resource Library, also on the FTC web site.

MODERATOR: Get as much information as possible – right?

MS. BRODER: Keep good records – meticulous records – of everything that you've done.

MODERATOR: Get police reports and make sure – this is, again, all fairly common sense, but we need to spell it out so people understand what's going on. Any other comments from anybody?

MS. FEDDIS: Well, just as we said, this is a cooperative effort. And with the vigilance and education of the consumers, the imagination and commitment of financial institutions, and the energy and cooperation of law enforcement, we can really help minimize the impact on consumers and financial institutions.

MODERATOR: So, I'd like to thank our panel, Howard, Betsy, Michael, and Nessa, for being with us and sharing such great information with us on this program.

MODERATOR: In summary, there are some very clear things you can do to protect your e-mail and your regular mail from being used to commit identity theft against you. If at some time you think you may be a victim of identity theft, you should work with the financial institutions to close any fraudulent accounts, or take steps to safeguard compromised accounts. You should contact the nationwide credit reporting agencies to place a fraud alert on your files and request a copy of your credit report to get a clear picture of your situation. And contact law enforcement and the Federal Trade Commission for assistance and to report the crime.

United States Department of Treasury hopes that you have found these panels to be helpful. We hope the information provided in this DVD helps you understand what identity theft is, how you can protect yourself and what you should do if you are a victim.

Remember, the Resource Library, also on this DVD, can be viewed by inserting it into a computer disk reader. The Resource Library contains valuable documents and links to important web sites that provide information and tips on identity theft.

Thank you very much for watching.

DEPUTY ASSISTANT SECRETARY PARSONS: Hi. My name is Scott Parsons. I'm Deputy Assistant Secretary, Department of Treasury for Critical Infrastructure Protection. What you've seen so far is an example of the public and private sectors working together to get the message out loud and clear that identity theft is not acceptable, and there is much we can do to stop the thieves who are responsible for this crime.

Before we conclude, we thought you might like an inside look at how our federal law enforcement agents are stepping up to take on the challenge of stopping identity theft. Let's go now to the Cyber Crimes Command Center at the headquarters of the United States Secret Service in Washington, D.C.

NARRATOR: This is the Cyber Crimes Command Center for the U.S. Secret Service. It's the central point of contact for gathering evidence for prosecution, intelligence and research. Agents come here to better focus their efforts when fighting large-scale Internet crime.

Teamwork is needed to crack complicated cyber crimes. Typically, the trail starts here with the forensic specialists trying to crack the criminal's hard drives.

AGENT #1: What I've done is I took his computer, and I took the hard drive out of that computer, and I made a copy of it. It's called a forensic copy – an exact copy of it. And now I'm reviewing my copy of that, looking for evidence, or intelligence, or whatever might help us in the case.

NARRATOR: They have to be particularly careful in developing evidence from computers if they want that evidence to stand up in court.

AGENT #1: What I found is a document that he had on his computer, and it has what appear to be credit card numbers and the expiration dates. So, that obviously is a good lead for us right there, because now we have something that we can follow up on.

NARRATOR: With information obtained from the hard drive, the team starts tracking and tracing the cyber criminal's movement, starting with the data retrieved from the forensic inspection.

AGENT #2: What I'm doing is I'm looking up the bank identification information to see who issued the various credit cards. And then we'll be able to call the fraud investigators at those banks to determine whether or not fraud has occurred on the cards and, possibly, to see if the bank investigators have determined a point of compromise as to where the information was obtained.

NARRATOR: Any investigation requires cooperation and careful attention to legal requirements.

AGENT #3: What I'm going to do now is determine where this credit card came from. I understand it came from an e-mail. And I'm taking the e-mail and looking at it through the "headers" to determine where it originated. Some of the things that I'm looking for in the e-mail header are who is it from, the IP address where it originated, and the message ID.

NARRATOR: Those stolen credit card numbers we saw earlier are valuable commodities on the street. Crooks who collect the numbers need to convert them into cash. Where better to do that than the Internet? The crooks use notice boards to advertise their special wares in what is a virtual bazaar.

AGENT #4: "Credit Cards," "Cell Phone Security," "Free Drops," "Physical Key Loggers," "Money Order Scams," "Anonymous Surfing," "Criminal's Guide to Releasing Holds on Debt," "Tutorial" –

NARRATOR: The Secret Service special agents go under cyber cover to break up these highly organized cyber markets.

AGENT #4: Some of these run them just like a Fortune 500 business, where they have a president who's in charge of everybody. He has a hacking group. He has an identity theft group. He has a passport group, and each one of those factions is responsible solely for what they do. So, if he contracts a hit to go hit a credit card processor or a business, they do the hack, bring him back the numbers. He supplies it to his people providing them on credit cards, to make the counterfeit cards. So, it's very structured and very hierarchical on how they do things.

NARRATOR: What is traded on the cyber super highway finds its cash value on Main Street.

AGENT #5: In other words, the account numbers, the Social Security numbers, the birth certificates – all this stolen information – doesn't have a value 'til it's put back out on the street in the form of fake identities, fake credit cards and is actually used.

NARRATOR: The Secret Service helps to train local law enforcement.

AGENT #5: We in the Secret Service have been specifically targeting local law enforcement, to train them to identify evidence of these crimes so that for routine traffic stops and things of that nature, they recognize what's in the backseat of the car they're walking up on. When they're executing a search warrant, they recognize the tools that further these crimes.

NARRATOR: With a team 200 strong and growing, the Secret Service works on all sides of the problem to catch these increasingly clever cyber crooks.

DEPUTY ASSISTANT SECRETARY PARSONS: We hope the information contained in this program has proven valuable to you as it describes the problem of identity theft, what you can do to better protect your personal information and what actions you can take if you, unfortunately, become a victim of identity theft. With smart, innovative technology, committed financial institutions and educated citizens, we can all continue to enjoy a strong and vibrant financial system that is part of our everyday lives.

I also want to remind you about the DVD Resource Library contained at the end of this program, which includes important documents and provides links to web sites that provide tips and valuable information on identity theft.

I want to thank the participants and panelists. And on behalf of the Department of Treasury, I want to thank you for watching.

[END]