N.Y.C. CIVIL COURT COMMUNITY SEMINAR SERIES - 'IDENTITY THEFT'

Phaedra F. Perry

January 30, 2008

Ubiqus Reporting
Irvine, CA **(949) 477 4972**
New York, NY **(212) 227 7440**
www.ubiqus.com

[START 108_425-AUDIO.MP3]

MR. EDGAR PEREZ: Good afternoon. My name is Edgar Perez [phonetic]. And today, we're going to talk about identity theft. As we know, that's a big problem in America, a big financial mistake, and that is something that we need to take care of today. And we're going to know more about it today and, at the end of the presentation, we'll also have some questions to answer in that.

So again, my name, Edgar Perez. I work for Citibank. I'm a financial education specialist. We're going to have a presentation today. Looks like everybody got a handout with information there that is relevant to the presentation today. Not only that, there's also a summary of that documentation about identity theft that you need to know and also a seminar evaluation form that I will really appreciate if you can fill it out.

So with that, we're going to get started. And while going to leave some questions to the end, I'm going to ask you a few questions just for you to raise your hands. So let me start with this. How many people here have your Social Security card with you? Maybe two, three people. That's a good number. How many people have seen your credit report this year? Maybe it's too early for us to say this year, but let's say in the last six months. Still two people, three people. Okay. Let me ask you this. Do you have a shredder at home? Yes, that's great. It looks like 50% of the people have a shredder at home. Great.

Those are introductory questions, and it looks like you guys are already taking some of the initiatives to protect your identity. So let's go back to business.

Nowadays, identity theft is one

of the fastest-growing crimes in the United States. Every year, we have half a million Americans going through this problem. And you think the number is low, is high? Well, let me tell you. That number is probably even more than that, higher than that. Why? Because people don't know when their identity has been compromised. They get to know about that much, much later when they get a phone call from collections asking for a debt that you don't know about. So definitely, it's a growing crime.

We assume that in the United States, there might be around 25 million people who already been affected by identity theft, and that means 1 out of 12 Americans.

So today, we're going to speak about identity theft. We're going to speak the definition, the different types, signs that we can identify of identity

theft, how to protect ourselves and definitely what to do if something like that happened to us.

So we're going to go through the definition. Identity theft is basically when somebody uses our information to start a new credit account, to get new credit. So what's the information they can get? Well, name, address, Social Security Number, date of birth, mother's maiden name. Those are going to be the five pieces of information that people will need, only those five pieces of information, to go to online and apply for a credit card, to go online and apply for a new account. And therefore, they can do that if we, for some reason, allow them to do so.

So indeed, those five pieces of information are very important. And as I said and I asked before having your Social Security Number in a--at least the card--

in a safe location, it's important. You want to make sure that you protect your number and you don't give out your number to anybody who's going to call you, even though they might say they come from a bank or they come from anywhere. So definitely, we're going to go about through these measures in a few more seconds.

So let's talk about identity theft and fraud. We know about fraud. Let's say you have a checkbook. For some reason, you lose your checkbook. People are going to start writing checks. They're going to use your checks, they're going to forge your signature, and they're going to start paying bills with that. Is that identity theft? I see some heads nodding. Good.

Well, let me tell you. That's not identity theft because people steal, they can commit fraud, yes, but still,

they cannot open new accounts. They cannot go to the bank and say, I'm Mr. X and I would like to apply for a new credit card. They cannot do that. What do they need? Name, address, Social, date of birth, mother's maiden name. Those five pieces of information. When people can get access to that information and then go to the bank and apply for a credit card, that's identity theft. Okay?

So we'll continue here. Definitely there are different types of identity theft. We're going to focus today on financial identity theft. What do they mean by that? Well, basically, financial crimes. When people take your identity to get new credit and to get access to that. And potentially to damage our credit.

Now, the big question is, how people get our information. And believe it or not, people are very smart about

that. It's not really high-tech. It might be something as low-tech. When we don't have a shredder at home, people are actually looking at the garbage cans. So they can go outside, the garbage we throw out and we think is gone, people for that might be a gold mine. And they could be looking through that information to see if they can find access to your name, address, Social, date of birth. They already know where you live. They know your name. So they're missing your Social, they're missing date of birth and mother's maiden name to get a full profile. So garbage cans, important. Any information that we have at home, it's going to be discarded if we don't need it anymore, well, let's use a shredder. Otherwise, it's going to stay at home, protect it.

Important documents like your passport, your Social Security cards, date

of birth, your birth certificate, all these documents have to be protected at home in a safe location. You cannot leave stuff even on the table because people come and go. Maybe your friends bring some other friends and they want to take some documents there. Later on, you realize and that document is not there. So again, protecting our information starts at home.

You don't want to carry all things that you might need in your wallet. You want to carry only the minimum things that you need. Even you carry your ATM cards, maybe that's a good way to minimize cash, but still, if you carry your ATM cards, make sure that your PIN number is always going to be changed as often as you can. Those four digits cannot be your date of birth. That's something that everybody can guess or know some way. So again, it has to be a number that is only

relevant to you and you want to change that from time to time so people don't remember that. Even if they know it, that won't work next time.

The mail is also important, and especially for some people who live in the suburbs. If we go out on vacation and we see mail coming in, coming in, coming in, some people walking by might say, oh, nobody's home. I'm just going to go, I'm going to take the mail. And people, especially in the suburbs, when nobody works outside, it's easy to do that. So it's going to be the case that you're going to be outside on vacation for let's say a week or two weeks, it's a good idea to go to the U.S. postal office and tell them, stop my mail. I'll pick it up when I'm back. Unless you have somebody else who's going to do it for you. But definitely, that's something that we can do to protect our information.

Something else also, we get a lot of mail, paper statements from banks, credit card companies, Social Security, Motor Vehicles and so on. We want to minimize these paper component. How can we do that? If you have a bank account, maybe it's a good idea to ask the bank, I don't want to receive paper statements. I want to start getting electronic statements. So any time you have a new statement, you're going to get an email saying your statement is available online and then you can go and check that anytime. That's another way to minimize that paper component that is so risky.

When we talk about computers, that's another frontier about identity theft. For some reason, we have a desktop and now we bought a brand-new laptop. Do we put the desktop outside? No, we have to make sure that the desktop's going to be destroyed, that all the information

there is going to be destroyed. So if you have, let's say, a hard drive, that's a lot of information there. And some people might be looking at that information to get it, to learn about us. So what do we do? Make sure that you destroy that hard drive. You might use Norton, you might use Symantec, those programs to delete all the information. If not, get a hammer, destroy the hard disk. If not, put the hard disk in a microwave for ten minutes and that way, all the information will be destroyed, okay?

Let's continue. And in terms of credit and debit card accounts, something important to realize. Let me ask you something. How many people here use your credit card online? One, two, three, four, five, six. It looks like most people use that. And, indeed, that's very convenient, we can do that, yes. On the other hand, if you want to buy books, I

can go to Amazon.com and I can be comfortable that they will protect my information. However, there are also mom-and-pops Web sites, that they don't invest enough money in protecting my information. So how--what could I do if I would still want to buy something from these companies and I don't have access, another way to buy from there?

Well, in those cases, banks thought about that and decided, we're going to create the virtual account number. And what's that? If you want to use your credit card online and you don't want to give your real credit card number, you can call your customer service number on the back of the credit card and you can ask them, I'm going to use my credit card today and tomorrow for up to, let's say, $300. I want to get a virtual account number. And that's what you will get. They will give you a 16-digit number that

will work as a credit card number, but only for the days that you ask for and only up to the level that you decided. After that, let's say you want to use that credit card or that virtual number today and tomorrow. After that, it will be expired. Nobody will be able to use it. Okay. So that's the virtual account number. And the beauty of that is that nowadays, even you can go to your credit card company's Web site and you can generate yourself a virtual account number that you can just copy and paste in the Web site where you want to use it, okay? So that is something we can do now to protect our real credit card numbers from identity theft.

It's always important also to be careful how people use our credit cards when we shop. If you're going to go to a restaurant, make sure that if you get two copies of your credit card information

that it's only showing the last four digits, okay? So for your copy. Similarly, if you want to use your debit cards or your ATM cards, make sure that you always going to go only to ATMs from banks, not deli ATMs. For some reason, some people are actually going to ATM delis and they are actually inserting some materials there to get the information that were used in there. So again, using ATMs only to banks. It's secure, better protection that way. And, of course, if it's going to be your banks, you don't pay a fee.

So let's continue here. The Internet, it's another frontier, as I said before. There are going to be ways for people to try to get our information using the Internet. And probably, we are familiar with that. Let's say sometimes we get emails that say, your account has been frozen, you need to update your

information. And basically, they show you a form with a lot of fields, name, address, Social, date of birth, everything. And they want you to update that information and to send it back. As soon as you get those emails, you delete those emails. Because no serious institution will ask you to update your information online. If there's something to update, they will ask you to come to the branch so therefore, it's going to be a different story. Only unscrupulous people will do that, and they do it, and they still do it because still some people fall into that. So whenever we get those emails asking to update my information by email, delete those emails. Make sure that you mark that spam.

Not only that, we can get those emails or we can get links. And those links, when you click on them, will take you to another screen that will have the

same forms, with name, address, Social, date of birth, Social Security Number and so on. All these documents for us to enter. We don't need to fall into that. As soon as we get those emails, delete those emails because that's the easiest way for people to get information. And some people, as I said, still fall into that.

If you bank, let's say, with any bank, and you want to go online, make sure that you go to the exact Web site they can give you. Let's say you want to bank with Citibank, go to www.citibank.com because that's where you want to go. Don't believe the links. Sometimes you might get an email that might look exactly like Citibank's email, the same color, the same logo and everything else. You click on that and they show you a Web site that looks like Citibank's Web site. That's not. They are not going to ask you to do

that. You got to make sure that you understand what's the address you're going to, and you don't give your information easily that way. Okay? So those are going to be extra precautionary measures to take because we want to protect our identity.

When you think about Web sites too, it's important for us to protect our information by using antiviruses or firewalls. As you know, people are very creative. They are always coming out with new viruses and some of these viruses might actually try to get information from your computer. They might delete information. And they might even install copiers so they know exactly where you're going, which Web sites, which user names and passwords you're using. So again, for that, it's important to have antivirus. Norton Antivirus, Symantec, either one, but it's important to have those installed

in your computer.

It’s important also to know that we don’t want to be using or accessing financial confidential information in public locations. Maybe you’re confident to do that at home, yes, at work, yes, but not at the public library. Because you might just leave, some people might come after you and they might be able to see the information there. Just going back and back and back, they might see information that they don’t need to see.

So again, be careful about using that, even if you want to use a wireless network. As you know, that’s not secure. So basically, the information between you and the network will be public information. So that’s something that we need to protect. So we don’t want to access bank information, your mutual fund information or your retirement information in these unsafe locations.

Let me go to the final point in terms of how people actually can get our information. If you get emails offering you discounts to go to a cruise in the Caribbean for 5 days for $300, you might send the information back, but most of the time probably you won't hear back from them. They only want to have your information. So you want to be careful. Whenever they ask for information, make sure that you know who's asking for that information.

Let's say even going online, you might see a banner there that says, free credit report. Free credit report. And you say, oh, I want to know my credit report, I'm going to go there. Well, if you click on these companies, some of them, they only want to know your information so they won't give you anything. They will just give you the information and then even charge you

something for that. We're going to show you later how to get your real score, how to, where to get your credit reports, but not through these emails, not through these links in the Web sites.

So again, those are going to be different ways how people get our information. We have to be extra cautious now before we give any information. Later on, we'll talk about the specific ways to deal with this, how we can do about protecting our information. For now, we discover so far how people can get our information. So we'll continue in a few minutes with the next part of the presentation.

[END 108_425-AUDIO.MP3]