Wi$e Up Teleconference Call
November 30, 2007
Understanding Credit
Speaker 3 – Quisaira Almanzar Whitney

Jane Walstedt: And before I turn to Lucia Bruce, our Regional Administrator in Philadelphia, I’d like to make sure that our third speaker is on the call and has an open mike. Quisaira, are you with us?

Quisaira Almanzar Whitney: Yes. I am on the call. And I will apologize. I had ahead of time because for some reason my call keeps getting dropped. I am traveling for work. Actually I'm in a hotel room in Ohio.

Jane Walstedt: Oh.

Quisaira Almanzar Whitney: And so I'm not moving, I'm trying not to … to barely breathe. So hopefully I will not get dropped again while I'm speaking.

Jane Walstedt: Oh, dear. Okay, well then let me turn to Lucia Bruce to introduce you.

Lucia Bruce: Good afternoon. Quisaira Almanzar Whitney is a staff attorney in the Federal Trade Commission Bureau of Consumer Protection in Washington D.C., where she conducts nonpublic investigations into unfair and deceptive trade practices.

She also sits… assists with business and consumer education and other outreach activities. Ms. Whitney previously worked in the Federal Trade Commission’s Division of Marketing Practices. She has received a B.A. degree in Government with a concentration in international relations from Cornell University and a JD degree from the New York University School of Law.
The Federal Trade Commission offers many consumer publications on credit and loans, and I believe Ms. Whitney will tell us about that also. Good day, Ms. Whitney.

Quisaira Almanzar Whitney: Good afternoon. I'm going to talk to you about identity theft, and then also about some ways to protect yourself when shopping online, because more and more identity theft can be found through online purchases. So those are the two general areas that I'm going to cover today.

Identity theft is a problem that has affected millions of Americans, including Oprah Winfrey, Bill Gates, and Tiger Woods. And chances are that it's hurt somebody on this call. If you carry a wallet or a purse, if you have a credit card or a Social Security number, you're at risk for identity theft.

The Federal Trade Commission released a survey showing that 8.3 million American adults or 3.7% of all American adults were victims of identity theft in 2005. The victims--3.2 million or 1.4% of all adults--experienced misuse of their existing credit card accounts, 3.3 million or 1.5% experienced misuse of non credit card accounts, and 1.8 million victims or 0.8% found that new accounts were opened or other frauds were committed using their personal identifying information.

So today I'm hoping to help you learn how to protect your identity and minimize the chances of having an identity theft occur to you. So what is identity theft? It happens when someone uses your personal information, like your name and Social Security number or your credit card number to commit fraud in your name.

Identity thieves can do a lot of damage. They can go on shopping sprees using credit cards; they can open a new credit card account using your name and Social Security number; they can get cell phone service in your name with
your credit history; they can even get arrested and give your name to the police.

People whose identities are stolen frequently spend a lot of... lots of time and money cleaning up the mess the thief has made of their good name and credit records. They may lose out on a job opportunity, loans for education, housing, or cars, and they may even be arrested for crimes they didn't commit.

Now let me ask you a few questions to help assess all of our identity theft IQ. All of these questions involve a yes or no answer. And you don't have to answer out loud. You just need to keep track of how many times you answered yes or no.

Question 1. Do you shred or destroy every bill, credit card statement or bank statement that comes to your home before you throw it out?

Question 2. Have you ever seen a copy of your credit report?

Question 3. Do you have what... sorry, do you know what a fraud alert is?

If you’ve answered yes to all three, then you know some of the important steps to protect your identity and reduce the potential damage from identity theft.

If you answered yes to two out of the three, then you’re definitely cramping the style of many identity thieves, but there is still more than you can do to minimize the chance of identity theft and the toll it can take.

If you answered yes to only one question or if you didn't answer yes to any of them, well then you have good company. Many of us just don't know that it
takes a few steps to make a real difference in reducing the risk of identity theft.

Hopefully after today you’ll know how to better protect one of your most important assets—your identity. Identity theft is a serious crime. Law enforcement and government agencies are devoting greater resources to the problem. Now let’s talk about how thieves steal your identity.

Unfortunately there are a lot of ways, from sophisticated computer hacking to low tech dumpster diving into your trash, to plain old-fashioned stealing your wallet or purse. But you can take some very practical steps to minimize your risk and to reduce the damage to your identity.

To help us all in the fight against identity theft, the Federal Trade Commission has embarked upon a national outreach campaign, and the campaign theme is summed up in three key words -- deter, detect, and defend. First you deter. We all know the old saying that an ounce of prevention is worth a pound of cure. The same holds true for identity theft. Making your personal information hard for thieves to get their hands on can reduce your risk.

Here are the key steps to deter an identity theft. Shred your financial documents and paperwork with personal information before you discard them. Protect your Social Security number. Don't carry your Social Security card in your wallet or write your Social Security number on a check. Give it only if it’s absolutely necessary or ask to use another identifier.

Don't give out personal information on the phone, through the mail, or even the Internet unless you know who you’re dealing with. Never click on links sent in unsolicited emails. Instead, type in a web address you know. Use firewalls, anti-spyware, and anti-virus software to protect your home computer. Keep them up to date.
You can visit onguardonline--all one word – O, N, G, U, A, R, D, O, N, L, I, N, E .gov for more information on how to protect your computer. Don't use an obvious password like your birth date, your mother’s maiden name, or the last four digits of your Social Security number. Keep your personal information in a secure place at home, especially if you have roommates, employ outside help or are having work done in your house.

Now the second part of this three-step action plan is detect. With identity theft-- each detection is key. In addition to taking the preventive…preventative steps I just mentioned, detect suspicious activity by routinely monitoring your financial accounts and billing statements. Doing so can help you catch a potential problem before it gets out of hand.

For instance, read your credit card statements and financial accounts carefully, looking for any charges you did not make. Be alert to signs that require immediate action,—bills that do not arrive as expected, unexpected credit card or account statements, denials of credit for no apparent reason, [for no apparent]cause, or letters about purchases you did not make.

Inspect your credit report. Credit reports contain information about you, including what accounts you have and your bill payment history. And Tom did a great job about talking about the different credit agencies and how you can get a free credit report, which again is by visiting the website, www.annualcreditreport.com

Finally, the third part of this three-step strategy is called defend. I talked about how you can reduce your risk, but what if it’s too late? What if you’re already a victim? The answer is to act quickly. You can place a fraud alert on your credit score report and review the reports carefully. The alert tells
creditors to follow certain procedures before they open new accounts in your name or make changes to your existing accounts.

The three nationwide credit reporting companies have toll free numbers for placing an initial 90-day fraud alert. Calling one [credit reporting] company is sufficient. Placing a fraud alert entitles you to free copies of your credit report. Look for inquiries from companies you haven’t contacted, accounts you didn't open, and debt on your account that you can't explain.

The next thing that you can do is close accounts. Close any accounts that have been tampered with or established fraudulently. Call the security or fraud department of each company where an account was opened or changed without your okay. Follow up in writing with copies of supporting documents. You should also use the ID theft affidavit at www.FTC.gov/idtheft to support your written statement.

Ask for written verification that the disputed account has been closed and the fraudulent debt discharged. Keep copies of documents and records of your conversations about the theft. Also file a police report. You file a report with law enforcement officials to help you with creditors who may want proof of the crime. And report the theft to the Federal Trade Commission. Your reports help law enforcement officials across the country in their investigations.

So, you know, right now as I speak there are criminals out there looking for identity information to steal. They like identity theft because it can be what’s called an easy crime. They do their best work when no one is paying attention, when information is easy to get, because they think the damage will go undetected.
But by paying attention and following the three Ds of identity protection --
deter, detect, and defend -- we can all make it a lot more difficult for thieves
to walk away with our identities.

Now the next thing that I want to talk to you about is just some quick tips on
how to be smart when you shop online.

You should always check out the seller. If you’re thinking about shopping on
a site that you’re not familiar with, you should do independent research before
you buy. You can type in the site’s name on a search engine, and if you find
unfavorable reviews posted, you may defer doing business with that company.
You read the site’s privacy policies to learn how it uses and
shares your personal information, and consider using a software toolbar that
rates websites and warns you if a site has gotten unfavorable reports from
experts and other Internet users. [Download one such toolbar at
http://www.toolbar.netcraft.com/.] 

You should read return policies because sometimes some of these companies
are really good about return policies, but others will only give you a week in
which you can return the stuff that you purchased online. Know what you’re
getting. Make sure you read very carefully the product description, because
name brand items that are [sold at] a greatly reduced price actually could be
counterfeit.

As I mentioned earlier, don't fall for false emails or popups. Legitimate
companies are not going to send you unsolicited emails asking you for your
password, your login information, your financial information, or anything like
that. You should delete any emails that you get like that. They’re an attempt
to get information to facilitate identity theft.
Look for signs that a site is safe. When you’re ready to buy something from a seller that you trust, you can look for signs that tell you the site is secure, such as a closed padlock on the browser status bar, before you enter your personal and financial information.

And when you’re asked to provide payment information, the beginning of the website’s URL address should change from http to shttp or to https, and that tells you that the site is encrypted or secure. You should secure your computer. You should, at a minimum, as I mentioned earlier, have anti-virus and anti-spyware software and a firewall. And this will help to protect your computer.

Consider how you’re going to pay. Credit cards are generally safe options because they allow buyers to seek a credit from the issuer if the product isn’t delivered or if it was, you know, or if it wasn’t ordered. Also if your credit card number is stolen, you generally won’t be liable for more than $50 in charges. Do not send cash, do not use money wiring services, and be careful about using debit cards, because debit cards are attached to your checking account and, you know, then your money is just gone.

Know the full price and check out incentives -- things like, you know, “This is the best deal,” you know, “You can get free shipping.” They come with all kinds of strings attached, and so you need to be careful about that and read what these incentives are carefully. You should keep a paper trail. Print and save records of your online transactions, including the product descriptions and price, the online receipt, and copies of any emails you exchange with the seller.

You should also read your credit card statements as soon as you get them to make sure that there are not any unauthorized charges. And the last thing is you should always turn off your computer when you finish shopping. A lot of
people leave their computers running 24/7. And that’s the dream scenario for
scammers, because they can use that to install malicious software on your
machine and then they can control it remotely and commit cyber crime. So
those are all my tips. Thank you.

Jane Walstedt: Well thank you very much, Quisaira. That… what you said about stealing
your identity by giving your name when someone else is arrested, that’s
amazing.