

# Is Someone “Shopping” for Your Identity this Holiday Season?

By Melissa Guenther, Change Agents, Inc.

It seems hard to believe that Christmas is just three weeks away. The retail establishments are already sale pricing Holiday retail items. Other "businesses" are preparing also - yes, I'm referring to the "dark side".

Identity Theft is one of the fastest growing crimes in America today. As more people use credit cards to shop, the chances of having one's identity stolen increase. Identity theft is a crime in which someone takes your personal information and uses it posing as you. They then use the information to gain access to your credit card accounts, bank accounts, etc. You can then be stuck with huge debts to pay that, not to mention wrecking your credit and giving you a poor credit score. By stealing bits of your personal information, thieves can commit fraud against you by, *among other things*:

- Opening credit card accounts or other accounts in your name
- Purchasing merchandise or cars
- Withdrawing money from your bank accounts
- Adopting your identity with law enforcement

Some staggering statistics:

## Identity Theft and Holiday Shopping

- 44% of U.S. adults have either been a victim of identity theft or know someone who has been victimized.
- 44% of U.S. adults think that most people who are victims of identity theft were careless with their personal information.
- 83% of U.S. adults think people are more susceptible to identity theft around the holiday season.
- Nearly two-thirds (65%) of U.S. adults who are online plan to shop online this holiday season - with 14% planning to do more than half of their holiday shopping online.
- It costs approximately \$1400, 600 hours of your time, and years (sometimes as many as ten) to recover from identity theft? Not to mention how unbelievably devastating it can be.

The number one thing to remember is to always check your statements monthly to be sure that they are accurate. If you run into something that you know you did not make or do, contact the credit card company or bank immediately.

Get a copy of your credit report regularly. Check to be sure that there are no names on it that you do not recognize. Often they will list maiden names or past married names, even variations of your name. Be sure that the names listed are names you have used or do use. Also check to be sure there are no new accounts listed that you did not open.

There are steps and precautions that you can take to help prevent this from happening to you. These are not difficult but they do take commitment to help protect yourself.

Always keep your PIN numbers safe. Never keep them with your credit cards, and never make it obvious which cards they go to. Disguising them as a telephone number is just one way to make it less obvious what they are.

If using your debit card at the store, never let anyone see the number you enter and never give it to anyone. When withdrawing cash from an ATM machine, cover the area or shield it so that no one standing near you can see what you are entering.

While most websites are safe to use your credit card with, be sure the site is a secure encrypted site. Secure sites will have a tiny graphic of what looks like a lock in a corner, or the url address starts with <https://> - the "s" stands for secure. Installing a good firewall and anti-virus will help prevent problems online.

If you get a notice in the mail that you have been pre-approved for a credit card or line of credit, shred it or tear it up before disposing of the piece of mail. There are people who will actually dig through your trash in search of your personal information. Shred any mail you get that has any type of personal info on it.

Be wary of phone calls claiming to be from a credit card company, even if it is from one that you use. Often scammers will call pretending to be from a credit card company, claiming they need to update their files and they will ask you for your personal information. Legitimate companies already have your information and they have no need to call you to verify it or ask to update their files. Do not give out your information to anyone who calls you on the phone. They are most likely out to steal your information and use it for illegal purposes.

Also be wary of emails claiming you have won this or that. You cannot win something you never entered. Most of the time, the scammer is asking for money and/or wanting you to click on a link to give your information to have the imaginary prize sent to you. When you click on the link and go to their web page and enter your details, they have a program that captures all of it to use for their illegal purposes.

Keep a check on your mail. If you normally get mail everyday or most everyday and you see a sudden stop in service, contact your local post office immediately. Scammers are known to change the mailing address of someone and receive the mail themselves, going through it and obtaining credit card account numbers, etc.

If something sounds too good to be true, chances are it is. Remember to check your credit report on a regular basis, be careful with your PIN numbers, shred mail with personal information on it, be careful with emails and clicking on links in them, and always be sure that there is an encryption lock on any web page where you do shopping.

Using these precautions and safety measures can help prevent you from becoming a victim of identity theft. However, there is no absolute, guarantee, unless you lock yourself up in a closet and throw away the key! That said, here is what you need to do if you suspect you might be a victim of identity theft.

### **1. Place a fraud alert on your credit reports, and review your credit reports.**

Fraud alerts can help prevent an identity thief from opening any more accounts in your name. Contact the toll-free fraud number of any of the three consumer reporting companies below to place a fraud alert on your credit report. You only need to contact one of the three companies to place an alert. The company you call is required to contact the other two, which will place an alert on their versions of your report, too. If you do not receive a confirmation from a company, you should contact that company directly to place a fraud alert.

**Equifax:** 1-800-525-6285; P.O. Box 740241, Atlanta, GA 30374-0241

**Experian:** 1-888-EXPERIAN (397-3742); P.O. Box 9532, Allen, TX 75013

**TransUnion:** 1-800-680-7289; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Once you place the fraud alert in your file, you're entitled to order one free copy of your credit report from each of the three consumer reporting companies, and, if you ask, only the last four digits of your Social Security number will appear on your credit reports. Once you get your credit reports, review them carefully. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain. Check that information, like

your Social Security number, address(es), name or initials, and employers are correct. If you find fraudulent or inaccurate information, get it removed.

Continue to check your credit reports periodically, especially for the first year after you discover the identity theft, to make sure no new fraudulent activity has occurred.

## **2. Close the accounts that you know, or believe, have been tampered with or opened fraudulently.**

Call and speak with someone in the security or fraud department of each company. Follow up in writing, and include copies (NOT originals) of supporting documents. It's important to notify credit card companies and banks in writing. Send your letters by certified mail, return receipt requested, so you can document what the company received and when. Keep a file of your correspondence and enclosures.

When you open new accounts, use new Personal Identification Numbers (PINs) and passwords. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your Social Security number or your phone number, or a series of consecutive numbers.

If the identity thief has made charges or debits on your accounts, or has fraudulently opened accounts, ask the company for the forms to dispute those transactions:

- For charges and debits on existing accounts, ask the representative to send you the company's fraud dispute forms. Write to the company at the address given for "billing inquiries," NOT the address for sending your payments.
- For new unauthorized accounts, you can either file a dispute directly with the company or file a report with the police and provide a copy, called an "Identity Theft Report," to the company.
  - If you want to file a dispute directly with the company, and do not want to file a report with the police, ask if the company accepts the FTC's ID Theft Affidavit (PDF, 56 KB). If it does not, ask the representative to send you the company's fraud dispute forms.
  - However, filing a report with the police and then providing the company with an Identity Theft Report will give you greater protection. For example, if the company has already reported these unauthorized accounts or debts on your credit report, an Identity Theft Report will require them to stop reporting that fraudulent information. Send a letter to explain to the company the rights you have by using the Identity Theft Report. Once you have resolved your identity theft dispute with the company, ask for a letter stating that the company has closed the disputed accounts and has discharged the fraudulent debts. This letter is your best proof if errors relating to this account reappear on your credit report or you are contacted again about the fraudulent debt.

## **3. File a complaint with the Federal Trade Commission.**

You can file a complaint with the FTC by calling the FTC's Identity Theft Hotline, toll-free: 1-877-ID-THEFT (438-4338); TTY: 1-866-653-4261; or write Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Be sure to call the Hotline to update your complaint if you have any additional information or problems.

By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials across the nation track down identity thieves and stop them. The FTC can refer victims' complaints to other government agencies and companies for further action, as well as investigate companies for violations of laws the agency enforces.

Additionally, you can provide a printed copy of your online Complaint form to the police to incorporate into their police report. The printed FTC ID Theft Complaint, in conjunction with the police report, can constitute an Identity Theft Report and entitle you to certain protections. This

Identity Theft Report can be used to (1) permanently block fraudulent information from appearing on your credit report; (2) ensure that debts do not reappear on your credit report; (3) prevent a company from continuing to collect debts that result from identity theft; and (4) place an extended fraud alert on your credit report.

**4. File a report with your local police or the police in the community where the identity theft took place.**

Call your local police department and tell them that you want to file a report about your identity theft. Ask them if you can file the report in person. If you cannot, ask if you can file a report over the Internet or telephone. See below for information about Automated Reports.

If the police are reluctant to take your report, ask to file a "Miscellaneous Incident" report, or try another jurisdiction, like your state police. You also can check with your state Attorney General's office to find out if state law requires the police to take reports for identity theft.

Ask the officer to attach or incorporate the ID Theft Complaint into their police report. Tell them that you need a copy of the Identity Theft Report (the police report with your ID Theft Complaint attached or incorporated) to dispute the fraudulent accounts and debts created by the identity thief. (In some jurisdictions the officer will not be able to give you a copy of the official police report, but should be able to sign your Complaint and write the police report number in the "Law Enforcement Report" section.)

**Checklist – Put a checkmark next to each statement you do not practice.**

I shred or burn all unused documents which contain my personal information such as bank statements, utility bills, canceled checks, and credit card offers I receive in the mail.	
When I am out of town I either have my mail held by the US Postal Service or collected each day by someone I trust.	
My mailbox or PO Box is locked so that no one can view my <i>incoming</i> mail.	
My <i>outgoing</i> mail is never left in an unsecured home mailbox.	
I never mail return postcards (not in an envelope) which contain my name and address such as contest cards and warranty cards.	
I know when I usually receive bills in the mail each month and call the creditor if the bill is a week overdue.	
I never leave personal information unprotected in my home where it can be viewed by others.	
My Drivers License number is not printed on my personal checks.	
My Social Security Number is not the same as my Drivers License Number.	
My Social Security Number is not used to identify me at work or school.	
I never reveal personal information unless absolutely necessary.	
I look around me for who might be listening when in public places, such as banks, before giving anyone my Social Security Number.	
I do not carry identification cards in my wallet or purse which contain my social security number.	
I normally carry less than 3 credit cards:	

If I submit reimbursement receipts for work or other purposes, I always remove my credit card number first.	
I review my credit report from each of the three main credit bureaus (Experian, Equifax, and TransUnion) and look for items which might indicate identity theft:	
On my computer or laptop I use an internet firewall and anti-spyware software.	
My computer or laptop requires a security login password to access it.	
When left unused for more than 10 minutes, my computer requires a password to log on. (Password protected screensaver)	
When using an ATM, I always make sure no one can see what PIN number I use.	
I review all my bank or brokerage account statements when I receive them and look for any transactions which I don't recognize.	
I put credit card receipts in my wallet or purse until I get home instead of leaving them in shopping bags.	

**Review the statements that are checked. Those are the areas you need to focus on in order to protect your personal information.**

More information can be found on the Federal trade commission site at <http://www.ftc.gov/bcp/edu/microsites/idtheft/>

### **About Melissa Guenther**

Melissa Guenther is an agent with Change Agents, Inc. of Phoenix, Arizona. She is an expert in both culture change management and training and in designing customized blueprints and interventions for change, particularly in the realm of security awareness. She created the plan and blueprint for the University of Arizona's Security Awareness Campaign and assisted in its implementation. She has also consulted in the design and implementation of the Department of Economic Security and the Department of Health Services, Department of Homeland Services for the State of Arizona, statewide campaigns. For more information about Melissa or about Change Agents, Inc, please visit <http://www.changeagentsinc.com/ouragents> .