

"Are You Consumer Savvy"

Questions and Answers:

1. During 2007, what percent of complaints, received by the Federal Trade Commission (FTC), dealt with identity theft?
 - a. 9%
 - b. 17%
 - c. 32%
 - d. 51%

Answer: (c) 32 % which equates to 258,427 complaints related to ID theft. This was the number one (1) complaint received. Between January and December 2007, the Consumer Sentinel, the complaint database developed and maintained by the FTC, received over **800,000** consumer fraud and identity theft complaints. New York is ranked sixth in per-capita incidence of identity theft in the country with 19,319 identity theft complaints.

2. What is an effective step to take to prevent someone from gaining access to your personal information?
 - a. Throw your documents into a bonfire
 - b. Bury your documents in your yard
 - c. Cover all personal information with a permanent magic marker
 - d. Shred the documents prior to throwing them away

Answer: (d) Although all the methods will work in helping to prevent someone from gaining access to your personal information, shredding (using confetti or cross cut) is the easiest and most effective method.

3. What is a warning sign that you have become a victim of identity theft?
 - a. You receive bills for purchases you never made
 - b. You stop receiving monthly bank or credit card statements
 - c. You are denied credit for no apparent reason
 - d. All of the above

Answer: (d) There are many indicators signaling possible victimization of identity theft. Many of these indicators are generally easy to spot such as the receipt of bills for unauthorized products/purchases or no longer receiving bills or statements. Watching for these patterns may help you quickly identify victimization and limit harm.

4. What can you do to help ensure that your credit report is accurate?
- Toss coins into a fountain and wish for the best
 - Stop using credit cards
 - Carefully review your credit reports on a regular basis
 - Politely ask retailers to stop reporting to credit reporting agencies

Answer: (c) *If an identity thief is opening new accounts in your name, these accounts are likely to show up on your credit report. New Yorkers may obtain a free credit report from each of the three national credit reporting agencies, once every 12 months. Visit www.annualcreditreport.com or call 1-877-322-8228 to request this free report. Carefully check your credit report for accuracy and ask the credit reporting agency to document and review any incomplete or incorrect information.*

5. What are ways to safeguard personal identifying information?
- Minimize the use of your Social Security number
 - Limit information kept in your wallet
 - Review your medical explanation of benefits statement regularly
 - All of the above

Answer: (d) *Provide your Social Security number only when necessary. Ask to use another type of identifying number whenever possible. When mailing a payment to a creditor, do not write your Social Security number on your check. It is illegal in New York State for a business to require you to put your Social Security number on a check. New York also prohibits your Social Security number from being used as a personal identifier, password, or code on a membership or services card. An entity cannot require you to transmit your Social Security number over the Internet unless the connection is secure or the Social Security number is encrypted. It is also illegal for anyone to intentionally disclose your Social Security number.*

Carry only the credit cards you plan to use and only carry your Social Security card when absolutely necessary. Make copies and/or a list of everything in your wallet containing personal information and keep this information in a safe place. Additionally, review your medical account information because a person's stolen identity can be used to obtain medical services.

6. What should you do when you realize you may be the victim of identity theft?
- Report fraud immediately to the three major credit reporting bureaus
 - File a report with your local law enforcement department
 - Contact the security/fraud departments of your financial accounts (credit cards, banks, store charge cards, etc.)
 - All of the above

Answer: (d) Being a victim of identity theft requires your time and attention to adequately prevent further damage to your credit and financial well being. You need to stop the "thief" from opening more accounts in your name, appropriating current accounts, or using your information for other nefarious purposes. You should also obtain a police report as proof of the theft. Without a report from local law enforcement, you may not be able to place freezes or alerts on your credit reports or access business transactions records from creditors.

7. What mechanism exists to block access to credit reports and unauthorized opening of accounts?
- Security Freeze
 - Credit Capsule
 - Identity Deadbolt
 - Fraud Buster

Answer: (a) New York State has a Security Freeze law. A Security Freeze works by preventing most lenders and others from gaining access to your credit report for review prior to granting a new line of credit. If there is a Security Freeze on your credit file, the lender won't be able to get a copy of your credit history and, as a result, most lenders will refuse to open a new credit account. The Security Freeze will, in most cases, block someone from opening a new account or borrowing money using your name or personal and financial information. That's bad news for the bad guys. In addition to mailing costs, you can be charged up to \$5 to place a second or subsequent freeze on your report or to remove the Security Freeze. If you are a victim of Identity Theft, there is no charge for restoring a Security Freeze as long as you provide a copy of an ID theft report from a law enforcement agency or an ID Theft Victim Affidavit from the FTC.

8. What can you do to protect your personal identifying information when you are on-line?
- Never give your personal information in response to an unsolicited e-mail
 - Use a website that has "https" in the URL address line
 - Call the president of the Internet service and ask about the security of the website you are visiting
 - a and b

Answer: (c) As you're checking your e-mail, learn to recognize the signs of phishing scams. "Phishing" occurs when someone creates an e-mail requesting your personal information that appears to be from a bank or some other type of well-known business. For example, they will often ask you to verify your Social Security number or other important personal information to prevent your account from being "closed." If you click on the link in the message, it will take you to a "spoofed" or fake version of the reputable website. To protect your personal information online, always copy and paste web addresses into your browser window and call the company directly if you are asked to provide personal information via e-mail.

Note that **https** is "Hyper Text Transfer Protocol" with an added dash of "s", or Secure Sockets Layer, another protocol primarily developed with secure, safe Internet transactions. When you see https in front of the URL, it indicates that you are in a "secure session."

Extra Credit

9. What percent of identity theft victims knew the thief?
- 2%
 - 16%
 - 29%
 - 55%

Answer: (b) In the FTC survey of ID theft in the U.S., out of the forty-four (44) percent who had some knowledge of how their personal information was stolen, 16% had a personal relationship with the thief. Victims who reported a personal relationship with the thief mentioned three types of relationships: six (6) percent of all victims cited family members or relatives as the thief; eight (8) percent cited friends, neighbors, or in-home employees; and two (2) percent cited someone with whom they worked.

10. How can you decrease the number of pre-approved credit card applications you receive?
- Write a letter to every credit card company telling them to stop sending it
 - Call 1-888-5OPTOUT
 - Glue shut your mailbox
 - Ask your postal carrier to stop delivering all pre-approved credit card applications

Answer: (b) Generally, the fewer credit card applications you receive, the less likely a credit card account can be hijacked. Call **1-888-5OPTOUT** to have your name removed from these marketing lists and opt-out of information sharing with non-affiliated companies by your financial institutions.

11. What government agency should you contact to report that you have been the victim of identity theft?
- Department of Labor
 - National Reconnaissance Office
 - Bureau of Reclamation
 - Federal Trade Commission (FTC)

Answer: (d) Call the FTC Identity Theft Clearinghouse at 1-877-ID-THEFT (1-877-438-4338); TDD: (1-202-326-2502). <http://www.consumer.gov/idtheft/>. In addition to filing the complaint, the FTC can provide information regarding ID theft.

12. Who can you contact to learn more about restitution when you are a victim of identity theft and secure direct assistance to mediate/resolve your problem?
- The New York State Consumer Protection Board
 - A financial advisor
 - The District Attorney's Office
 - a and c

Answer: (c) Both the Consumer Protection Board (CPB) and the District Attorney can provide you with resources and guidance regarding seeking restitution. In 2008, Governor Paterson signed legislation creating the Identity Theft Mitigation and Prevention Program within the CPB. One aspect of this law is that it enables victims of identity theft to seek restitution for the value of the time they spend fixing the damage that the criminal has inflicted. According to one study, identity theft victims spent 330 hours in addressing the damage caused by the identity thief. For the first time, these victims may be able to be compensated for their lost time.

For additional information and references, please contact the New York State Consumer Protection Board ID Theft Prevention and Mitigation Program at 1-800-697-1220.