Identity Theft - Safeguarding Your Personal Information

Nancy Hannan
Security Awareness Program Manager
Fifth Third Bank
True or False. ID theft is the fastest growing crime in America?

- True
- False
True or False. ID theft is the fastest growing crime in America?

- True
- False

ID theft surpassed drug trafficking as the fastest growing crime in America several years ago.
How many consumers were victims of identity theft in 2012?

- 6.7 million
- 7.9 million
- 8.1 million
- 12.6 million
How many consumers were victims of identity theft in 2012?

- 6.7 million
- 7.9 million
- 8.1 million
- 12.6 million

There were 12.6 million identity theft victims in the U.S. in 2012.
19 people fall victim to identity theft every __________.

- Minute
- 15 minutes
- Hour
- Day
19 people fall victim to identity theft every __________.

- ✔ Minute
- ❌ 15 minutes
- ❌ Hour
- ❌ Day

19 people fall victim to identity theft every minute, which equates to approximately 1 person every 3 seconds.
What is the most common way for an identity thief to take over your bank account?

- Add their name as a registered user on the account
- Obtain checks for the account
- Change the registered address on the account
- Obtain a credit or debit card in their name
What is the most common way for an identity thief to take over your bank account?

✓ Add their name as a registered user on the account
☐ Obtain checks for the account
☐ Change the registered address on the account
☐ Obtain a credit or debit card in their name

While identity thieves rely on all of these methods, adding their name to your account is the most common way to take control of it.
What is the most common way people fall victim to identity theft?

- Computer viruses, spyware, hackers and phishing schemes
- Having their wallet, checkbook and/or credit card lost or stolen
- Having their paper mail stolen
- Having their data stolen from a business or financial institution
What is the most common way people fall victim to identity theft?

- Computer viruses, spyware, hackers and phishing schemes
- Having their wallet, checkbook and/or credit card lost or stolen
- Having their paper mail stolen
- Having their data stolen from a business or financial institution

Although this only accounts for 38% of all occurrences.
Which of the following methods of identity theft often results in the largest financial loss for the victim?

- Computer viruses, spyware, hackers and phishing schemes
- Having their wallet, checkbook and/or credit card lost or stolen
- Having their paper mail stolen
- Having their data stolen from a business or financial institution
Which of the following methods of identity theft often results in the largest financial loss for the victim?

- Computer viruses, spyware, hackers and phishing schemes
- Having their wallet, checkbook and/or credit card lost or stolen
- Having their paper mail stolen
- Having their data stolen from a business or financial institution

Viruses, spyware, hacking and phishing schemes often result in the highest financial loss to the victim.
What is the average length of time a person spends trying to resolve a case of identity fraud?

- 5 hours
- 14 hours
- 30 hours
- 45 hours
What is the average length of time a person spends trying to resolve a case of identity fraud?

- 5 hours
- 14 hours
- 30 hours
- 45 hours

An identity theft victim spends an average of 30 hours resolving their case, with an average cost of $500. More damaging and complicated cases can take hundreds of hours to resolve.
True or False. A thief can pose as a bank, employer or landlord to obtain your vital stats directly from a credit bureau.

- True
- False
True or False. A thief can pose as a bank, employer or landlord to obtain your vital stats directly from a credit bureau.

- True
- False

A skilled thief can con a credit bureau into turning your personal information over to them.
Which of the three main types of identity fraud is the most prevalent?

- New account fraud
- Existing card account fraud
- Existing non-card account fraud
Which of the three main types of identity fraud is the most prevalent?

- New Account Fraud
- Existing Card Account Fraud
- Existing Non-Card Account Fraud

Existing Card Account Fraud constitutes more than half of all identity fraud incidents. However, the monetary loss for each incident of Existing Card Account Fraud is typically only half that of the other two main types of fraud.
What is the average length of time it takes a consumer to discover that they are a victim of identity theft?

- 14 days
- 25 days
- 34 days
- 51 days
What is the average length of time it takes a consumer to discover that they are a victim of identity theft?

- 14 days
- 25 days
- 34 days
- **51 days**

The average detection time for identity fraud is 51 days. However, a thief misuses your information an average of 71 days before moving on.
What Is Identity Theft?

Identity theft (ID theft) occurs when someone assumes another person’s personal identifying information (e.g., name, social security number, date of birth) with the intent of committing fraud.
How Can Your Identity Be Stolen?

- Loss or theft of your wallet, purse, or credit card
- Mail theft
- Skimming information from the magnetic strip on credit or debit cards
- “Dumpster diving” through the trash
- “Shoulder surfing” - looking over your shoulder when you are entering a PIN or password
- Eavesdropping
- Scam phone calls where a stranger asks for personal or financial information
- Phishing and spyware
- Computer hacking
How Does Identity Theft Work?

Using one or more of the methods identified on the previous slide, the fraudster obtains key pieces of personal information (e.g., Social Security number, driver’s license number, home address, etc.) that is then used to open new bank accounts in your name, apply for mortgages, apply for credit, etc.
What Should You Be Looking For?

- Unauthorized charges that appear on your checking account or credit card statement
- Accounts appearing on your credit report that you did not open
- Calls from collection agencies asking why you have not paid a bill
- Calls from financial institutions regarding accounts you did not open

- Missing bills or credit card statements that don’t arrive when they are supposed to
- Unauthorized transfers or withdrawals on your bank statements
What Can You Do To Prevent It?

- Review your financial statements regularly.
- Never give out personal information, such as your Social Security number unless it is absolutely necessary.
- Do not have your Social Security number printed on your driver’s license or your checks.
- Beware of giving information to anyone over the telephone or the internet unless you initiated the contact.
- Secure your personal information at home.
  - Keep credit and debit cards in a safe place and report missing cards immediately.
  - Be aware of what you throw away. Shred all documents with any personal data on them.
  - Watch for regular bills that aren’t delivered.
What Can You Do To Prevent It?

- Don’t leave mail for pickup in an unlocked mailbox.
- Check your credit report at least once a year. (www.annualcreditreport.com)
- Monitor your online financial accounts frequently.
- Sign your new credit and debit cards promptly.
- Do not keep PIN numbers attached to credit, debit or ATM cards.
  - If you are a member of a military unit who is on active duty, consider placing an active duty alert on your credit report. The active duty alert can prevent pre-screened offers of credit and insurance from being sent while you are away on active duty.

*Note: To opt out of receiving pre-approved credit card offers altogether, call 1-888-5OPTOUT.*
Tools To Use

A micro-cut shredder
A Uni-Ball Signo Gel 207 Pen
Protect Yourself: Phone Fraud

- Recognize how to identify the most common telemarketing scams.
  - Foreign Lotteries
  - Veteran Scams
  - Gift Certificate Scams
  - Jury Duty
  - Stolen Account Numbers
  - Medicare Part – D
  - College Credit Card Offers

- Report phone fraud to the FTC at www.FTC.gov or 877-FTC-HELP.

- Register your phone number on the National Do Not Call Registry at www.DoNotCall.gov or 888-382-1222. Registering can help limit the number of telemarketing calls you receive, so you can be more alert to calls you do get.

- Be aware that scammers will typically make high pressure statements, express urgency, and may get agitated if you start asking a lot of questions.

- If it sounds too good to be true, it probably is.
Protect Yourself: Skimming

- Check your accounts on a regular basis to be sure there are no unusual purchases or withdrawals. This is the most important thing you can do to protect yourself, as skimming devices can be difficult to detect.

- Closely monitor anyone who handles your card. If possible, don’t let them out of your sight with your card.

- Keep low limits on your cards. This will restrict the amount of money available to the thieves.

- Look at the ATM before using it. Be wary of anything about the ATM that looks out of the ordinary. If it doesn’t look right, don’t use it.

  - If your card is not returned after the transaction or after pressing cancel, contact the bank or financial institution involved immediately.
    - Watch out for people who try to “help” you at an ATM or other POS terminal.
    - Hide your hand as you enter in your PIN to prevent a camera from recording your keystrokes.
Protect Yourself: Mobile Devices

- Treat your mobile device with the same level of care as you would a credit card. If it is lost or stolen and you have not protected it adequately, you may be at risk.
- Password protect your mobile device.
- Store your mobile device in a safe place.
- Do not send confidential information in email or text messages (e.g., account numbers).
- Delete messages that contain account information, including account balances, and any alerts you receive on a regular basis.
- Only download information (photos, ring tones, video clips, etc.) from trusted sources.
- Follow the same rules you use on your computer with respect to opening email and attachments. Install anti-virus software on your mobile device.
- If you are concerned about the sites you are accessing from your mobile device, turn on the “show URL” or “show address bar” option so that you can see the actual site addresses to ensure they start with “https.”
Protect Yourself: Online

- Do not download or install software unless you know and trust the vendor 100%.
- Be very cautious about who you give your email address to.
- Use strong passwords.
- Do not enter sweepstakes or contests.
- Never open emails or attachments from email addresses you do not know.
- Never click on links in emails from email addresses you do not know.
  - Consider using disposable email accounts when filling out forms on the Web.
  - Learn how to recognize phishing emails.
Protect Yourself: Keep Your PC Clean

- Use a personal firewall and security software.
- Always keep your computer's operating system and security software updated.
- Run a full system scan of your computer weekly.
- Clear out cookies and other tracking data on your PC regularly.
What If You Become A Victim?

- Contact the financial institution(s) or the companies where information about you has been used and let them know you are a victim of identity theft.

- Contact the credit reporting agencies to report identity theft and request they place a fraud alert on your account. You only need to contact one. The first agency you contact will contact the other two.

- Contact the police department to report the crime. Be sure to request a copy of the report.


- Keep good records of who you talk to, summaries of conversations and documentary evidence of the crime.

For additional information about account fraud and identity theft, visit the Identity Theft Resource Center at [www.idtheftcenter.org](http://www.idtheftcenter.org) or the Fifth Third Privacy and Security Center at [www.53.com/security](http://www.53.com/security).