Identity Theft
and
Strategies for Crime Prevention

Objectives

- What is identity theft?
- Why worry about it?
- How does it happen?
- Why has identity theft emerged?
- What is being done about it?
- What can I do about it?

What Is Identity Theft?

- One person, using information gathered from some source, takes on the identity of another person without permission and conducts a variety of activities using that identity.
- The intent is to use that identity for personal gain, generally with the intent to defraud others.

What Is NOT Identity Theft?

- Someone using your credit card with your knowledge and consent to make a purchase
- Someone properly exercising a legally granted power of attorney on your behalf
- Someone making up a fake name and signing into a hotel. This may be a crime, but it's not identity theft.

Why Worry About Identity Theft?

- It is the fastest-growing crime in the nation.
- More than 10 million people are victimized by it each year, the most victimized group being those between the ages of 19 and 29.
- It can cost an average of 80 hours and more than $1,400 to clear up a simple case of identity theft that is caught early.

Why Worry About Identity Theft? (cont.)

- Some victims lose many thousands of dollars as well as their good credit rating and consumer reputations.
- It costs our economy $40 billion or more each year.

(Source: Federal Trade Commission Synovate Study 2003, www.ftc.gov)

Why Worry About Identity Theft? (cont.)

- Deterrence and apprehension are not yet effective. Prevention is the best defense.
- There are jurisdictional problems concerning where the crime occurs.
- It is an attractive crime to criminals because of its low risk and high return.

How Identity Theft Works

STEP 1—Getting the Identity

- The thief or thieves look for information in any number of ways:
  - Discarded documents in the trash
  - Receipts from purchases
  - Lost or stolen wallets or purses
  - Online “phishing” for personal data
  - Stolen mail from mailboxes
  - Thieves are thinking of new, inventive ways every day.

How Identity Theft Works

STEP 1—Getting the Identity (cont.)

- Some thieves go “wholesale” by getting lists of information on individuals through computer hacking, theft, or bribery.
- The information may be resold to other crooks or used numerous times by the original thief or thieves.
- Profits may be used to support additional criminal activities such as drugs and terrorism.

How Identity Theft Works

STEP 2—Exploiting the Identity

- With the information that becomes available, the thief may have false IDs made:
  - A state driver's license with the thief's picture and the victim's name
  - Non-driver's state license
  - Social Security card
  - Employer ID
  - Credit cards

How Identity Theft Works

STEP 2—Exploiting the Identity (cont.)

- The thief may simply begin leveraging one piece of information to obtain or establish other information or assets. These may include
  - New credit card accounts
  - State or local licenses
  - Accounts with utility companies, apartment leases, or even home mortgages

How Identity Theft Works

STEP 3—Discovering the Theft

- The thief continues to build a "persona" using the victim's name, good credit, and even good character references. The thief never pays the bills, but the victim is left with a bad name and ruined credit.
- Eventually, the victim tries to get a new credit account and is turned down, gets a bill for a credit card he or she never owned, or starts getting calls from bill collectors.

How Identity Theft Works

STEP 3—Discovering the Theft (cont.)

- The thief might abandon the victim's identity because he or she has "spoiled" the name of the victim (e.g., with a criminal offense or bankruptcy).
- When the crime or ruined credit is discovered, the victim is left to clean up the mess.

How Identity Theft Works

STEP 4—Reporting and Restoring

- The victim reports it to the local police and to the nation's major credit bureaus.
- The victim asks the credit bureaus to note the identity theft crime on his or her credit report.
- The victim may need to consult with a local victims' assistance agency or an attorney for specific steps necessary in a given state.

How Identity Theft Works

STEP 4—Reporting and Restoring (cont.)

- The victim also files a complaint through the Federal Trade Commission registry at www.ftc.gov.
- The victim completes an ID theft affidavit, available in www.ftc.gov's identity theft section.

Frequently Asked Questions

Where and How Do They Get My Information ?

- Telephone calls asking you to “update records”
- Theft of incoming bills, which show your account number
- Theft of outgoing mail and bill payments

Where and How Do They Get My Information? (cont.)

- Redirection of stolen mail, where the thief files a change of address on your credit card bills
- "Phishing" in which the sender sends out an email or pop-up message that looks like it came from a real bank or credit card company and asks for identifying information. Legitimate groups will never do this.

Where and How Do They Get My Information? (cont.)

What is “phishing”?

- The Internet is a new, convenient, and trusted way to do business that has allowed criminals to create illegitimate emails or pop-up messages posing as your bank, credit card, or utility company.

Where and How Do They Get My Information? (cont.)

What is “phishing”? (cont.)

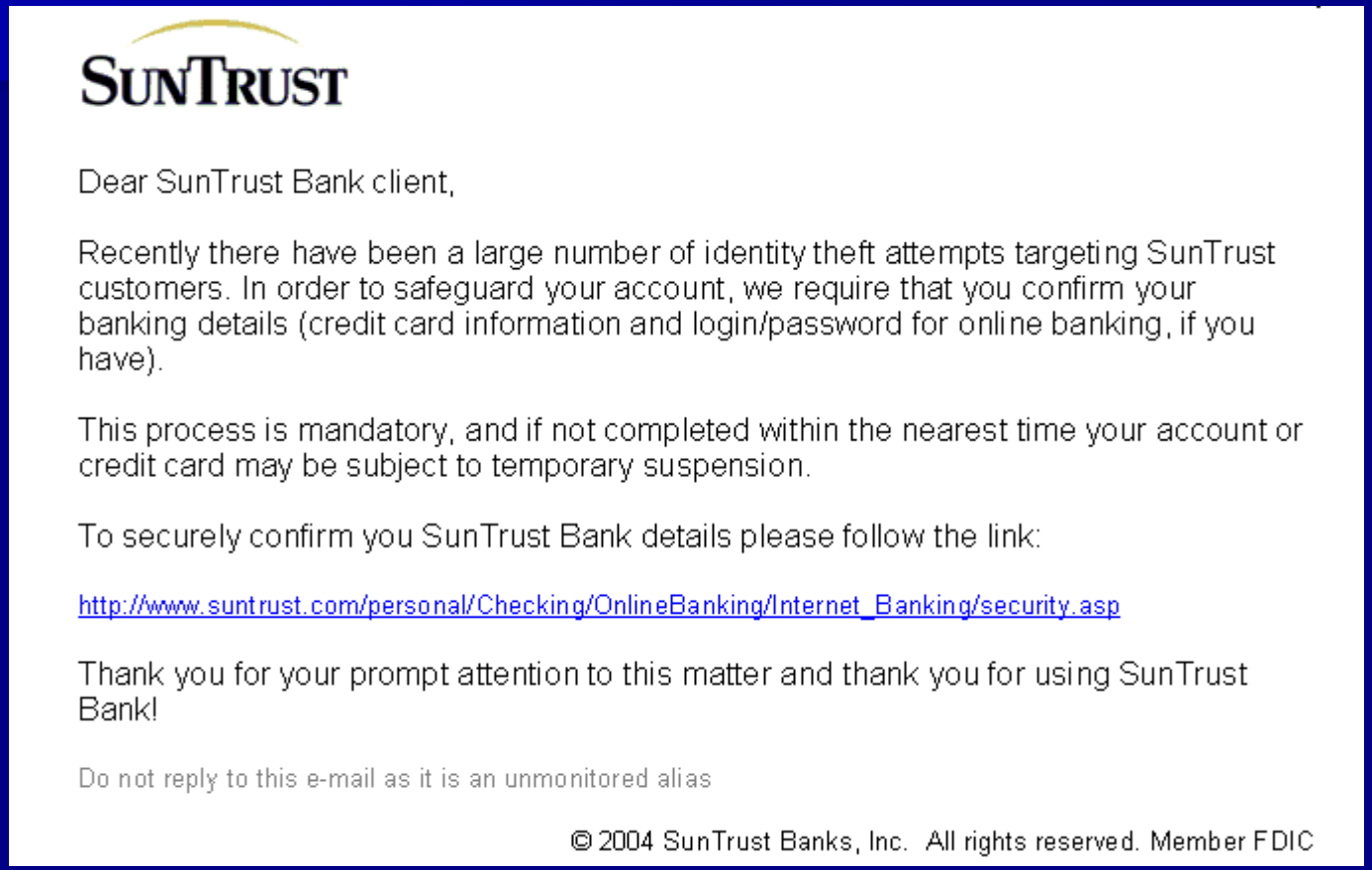
- They create a phony reason why you need to give them your personal information (e.g., bank routing number, Social Security number).
- They use the ease of online transactions to their advantage, hoping you will be fooled.

Where and How Do They Get My Information? (cont.)

More places…

- Going through trash to recover bills
- Credit card receipts that you discard or toss out with a shopping bag
- Noticing a bill you tossed in a public trash can
- Second impressions of credit cards
- Casual use of Social Security numbers and other similar identifiers

Sample “Phishing” Email



SUNTRUST

Dear SunTrust Bank client,

Recently there have been a large number of identity theft attempts targeting SunTrust customers. In order to safeguard your account, we require that you confirm your banking details (credit card information and login/password for online banking, if you have).

This process is mandatory, and if not completed within the nearest time your account or credit card may be subject to temporary suspension.

To securely confirm you SunTrust Bank details please follow the link:

http://www.suntrust.com/personal/Checking/OnlineBanking/Internet_Banking/security.asp

Thank you for your prompt attention to this matter and thank you for using SunTrust Bank!

Do not reply to this e-mail as it is an unmonitored alias

How To Avoid a “Phishing” Scam

Tips from the FTC:

- If you get an email or pop-up message that asks for personal or financial information, do not reply or click on the link in the message. Legitimate companies don’t ask for this information via email.

How To Avoid a “Phishing” Scam (cont.)

Tips from the FTC:

- If you are concerned about your account, contact the organization using its legitimate telephone number or open a new Internet browser and type in the company’s correct web address.

How To Avoid a “Phishing” Scam (cont.)

More tips from the FTC

- Don’t email personal or financial information. If you initiate a transaction and want to provide your personal or financial information through an organization’s website, look for indicators that the site is secure.

How To Avoid a “Phishing” Scam (cont.)

More tips from the FTC

- A “lock” icon on the browser’s status bar or a URL for a website that begins “https:” (the “s” stands for “secure”) indicates that you are on a secure site.
- Unfortunately, no indicator is foolproof; some phishers have forged security icons.

How To Avoid a “Phishing” Scam (cont.)

- Use antivirus software and keep it up-to-date. Some phishing emails contain software that can harm your computer or track your activities on the Internet without your knowledge. Antivirus software scans incoming communications for troublesome files. Look for antivirus software that recognizes current viruses as well as older ones, can effectively reverse the damage, and updates automatically.

How To Avoid a “Phishing” Scam (cont.)

- A firewall helps make you invisible on the Internet and blocks all communications from unauthorized sources. It’s especially important to run a firewall if you have a broadband connection. Finally, your operating system (e.g., Windows or Linux) may offer free software “patches” to close holes in the system that hackers or phishers could exploit.

Why Is ID Theft on the Rise?

- Computers have made record-keeping faster but have removed human analysis, making it easier for someone to steal an identity or pose as another person.
- More and more transactions are being handled electronically, and that trend is continuing to increase dramatically.
- More computer hackers now go for monetary returns, not for the thrill of conquering another computer.

Why Is ID Theft on the Rise? (cont.)

- Mobility means that many of us shop in stores all over our community, the region, or the country, so we are more anonymous than ever.
- Many of us find it hard to believe that ID theft could happen to us, even though millions are victims each year.

What Can We Do About It?

- Consumer education, like the information we're sharing today, helps you reduce your risk of becoming a victim.
- Education is an ongoing process as new techniques emerge.
- Information about prevention and ways to stop ID theft spread quickly as well.

What Can We Do About It? (cont.)

- New ways are being found to tighten security on electronic payment systems and to detect “out of the ordinary” purchase patterns.
- Some credit card payment systems now signal only the last four digits of your card number, so that someone who steals your receipt can’t steal your good name.

What Can We Do About It? (cont.)

- New shredders are coming onto the market, making thorough document destruction easier at home.

Who Is Vulnerable?

People who

- Keep their money in bank accounts
- Use credit or debit cards
- Generate trash with unshredded paper in it
- Casually toss credit card or other receipts into public receptacles
- Get personal bills by mail or electronically
- Don’t check their credit card reports and bank statements

Who Is Vulnerable? (cont.)

People who

- Don’t regularly check their credit bureau reports
- Have accessible mail boxes

Prevention

- Check your bank, credit card, and similar statements monthly. Make sure you receive them, and make sure the charges are yours.
- Immediately call your bank or credit card company if you don’t receive your bill.

Prevention (cont.)

- Consider registering with the Direct Marketing Association to refuse any unsolicited credit offers.
- NEVER provide account information over the Internet or the telephone unless you originated the call and unless you are absolutely certain of the party you are speaking to.

Prevention (cont.)

- Rip up receipts if you will not need them for warranties or returns.
- Shred any unwanted credit, loan, or credit card offers – or at least cut them up with scissors – before putting them in the trash.

Prevention (cont.)

- Do not give out your real name or other personal information in Internet chat rooms. Use a screen name.
- Do not authorize others to use your credit cards. They may not take the same care that you do.
- Deposit mail in a U.S. Postal Service mailbox.
- Make sure your mailbox is secure.

How To Handle Identity Theft

- File a police report immediately.
- Notify the three major credit bureaus and each of your credit or debit card issuers of the identity theft, and ask that appropriate alerts and closures be filed.
- File a report with the Federal Trade Commission's Complaint Center, and obtain an ID theft affidavit, which is available online at www.ftc.gov.

How To Handle Identity Theft (cont.)

- Check credit reports, immediately report any incorrect activity, and ensure that a fraud alert is still active on your account.
- Carry copies of documents with you – the police report, the affidavit, and any other formal records that attest to your identity – in case of emergency.

How To Handle Identity Theft (cont.)

- Check court records in your general area for bankruptcies and for mortgage liens using your name. Many records are automated, which makes the job easier.

Encourage Everyone To…

- Review methods of handling personal information
- Take prevention strategies to heart – and encourage others to do so
- Speak out about the need for preventive action and laws that protect identity theft victims

Online Resources

- Federal Trade Commission: www.ftc.gov
- Department of Justice: www.usdoj.gov/criminal/fraud/idtheft.html
- Better Business Bureau: www.bbb.org
- United States Postal Service: www.usps.com

Online Resources

- Many nonprofit organizations are committed to promoting prevention and recovery from identity theft. Here are a few:

  www.idtheftcenter.com/index.shtml

  www.identitytheft.org/

  www.privacyrights.org/identity.htm

National Crime Prevention Council

1000 Connecticut Avenue, NW,
Thirteenth Floor
Washington, DC 20036
202-466-6272
www.ncpc.org