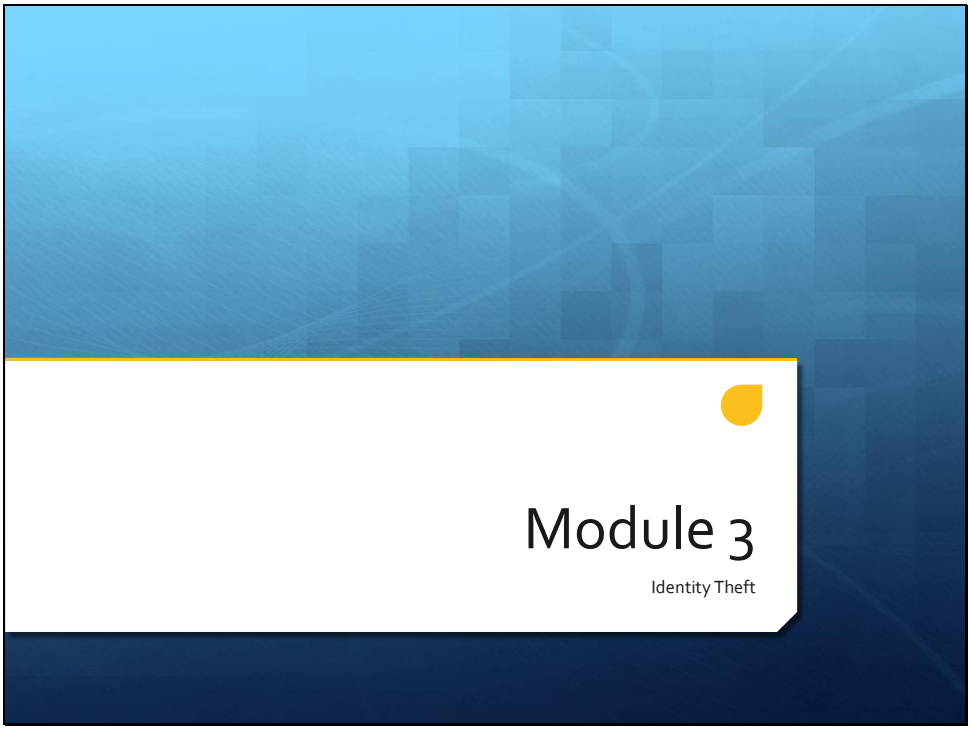
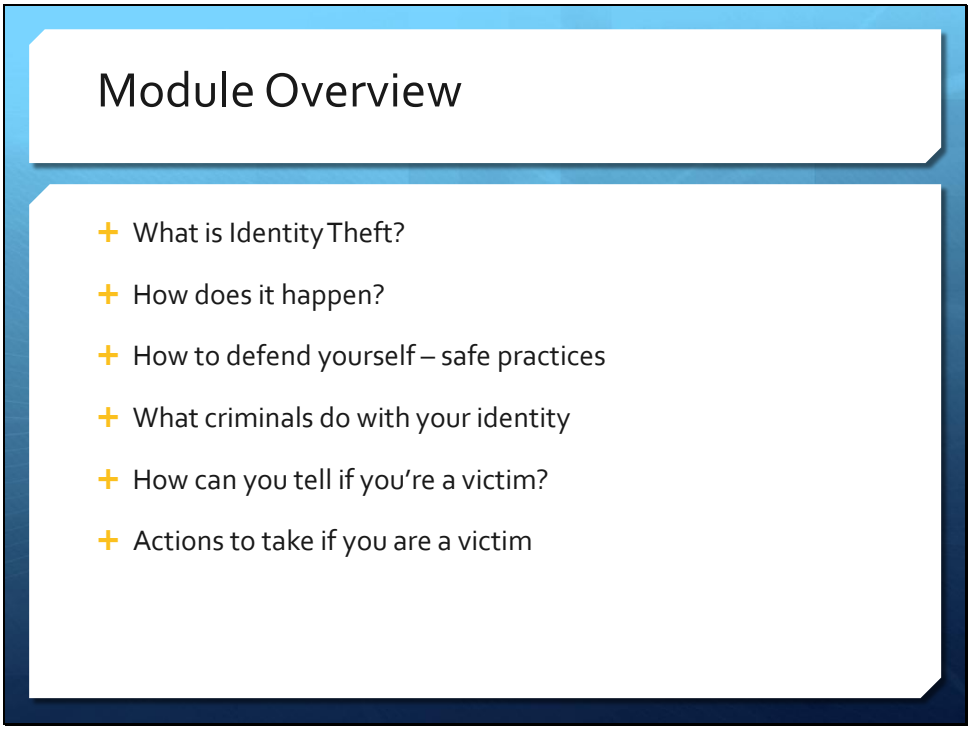
Security Awareness

Module 03 – Identity Theft

Slide 1



Slide 2

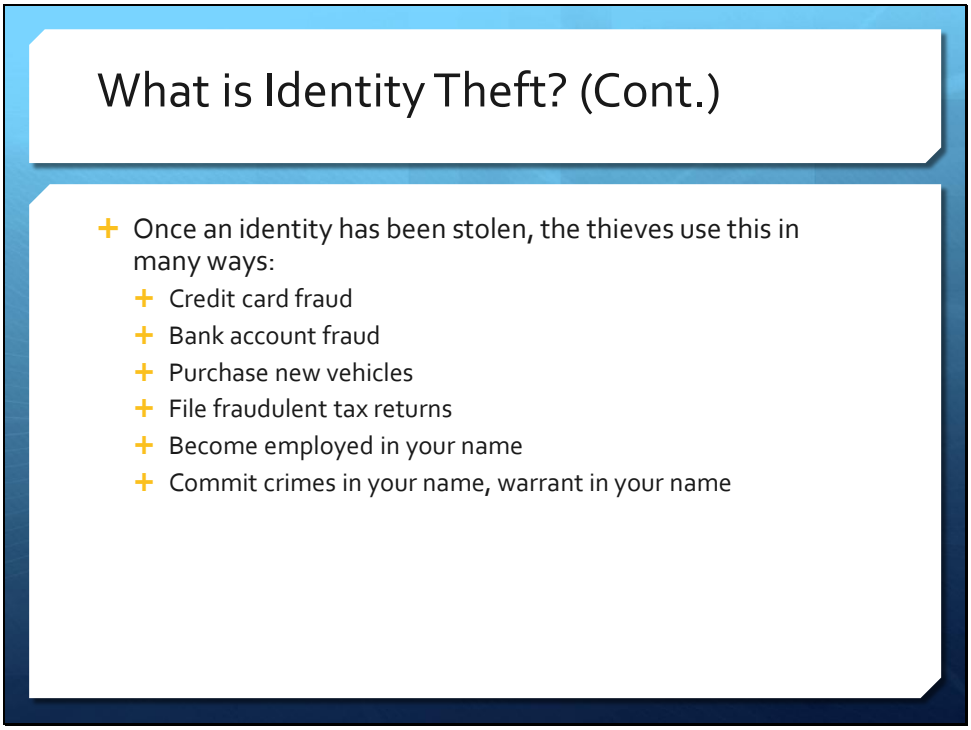

Module Overview
What is Identity Theft?
How does it happen?
How to defend yourself – safe practices
What criminals do with your identity
How can you tell if you're a victim?
Actions to take if you are a victim

Slide 3

What is Identity Theft?

- Identity theft is when someone uses your personal information, such as your name, Social Security Number, credit card number, and so on, without your permission to commit or attempt to commit fraud or other criminal action
- This can be more than financial:
  - Online identity
  - Defamation
  - Cyber attacks

Slide 4

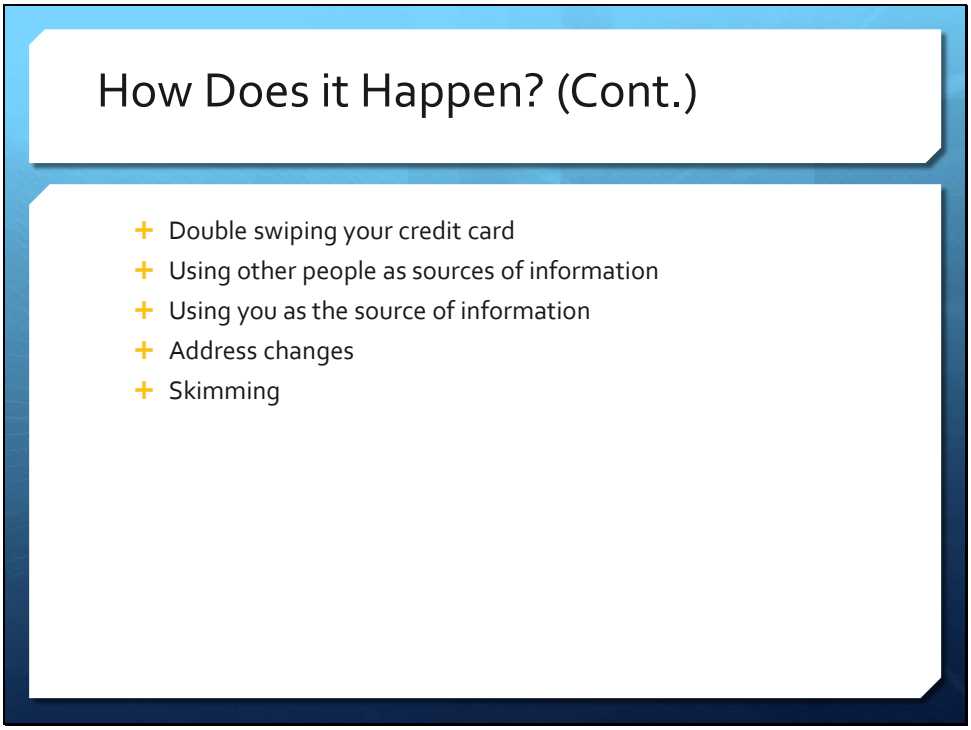

What is Identity Theft? (Cont.)
Once an identity has been stolen, the thieves use this in many ways:
Credit card fraud
Bank account fraud
Purchase new vehicles
File fraudulent tax returns
Become employed in your name
Commit crimes in your name, warrant in your name

Slide 5

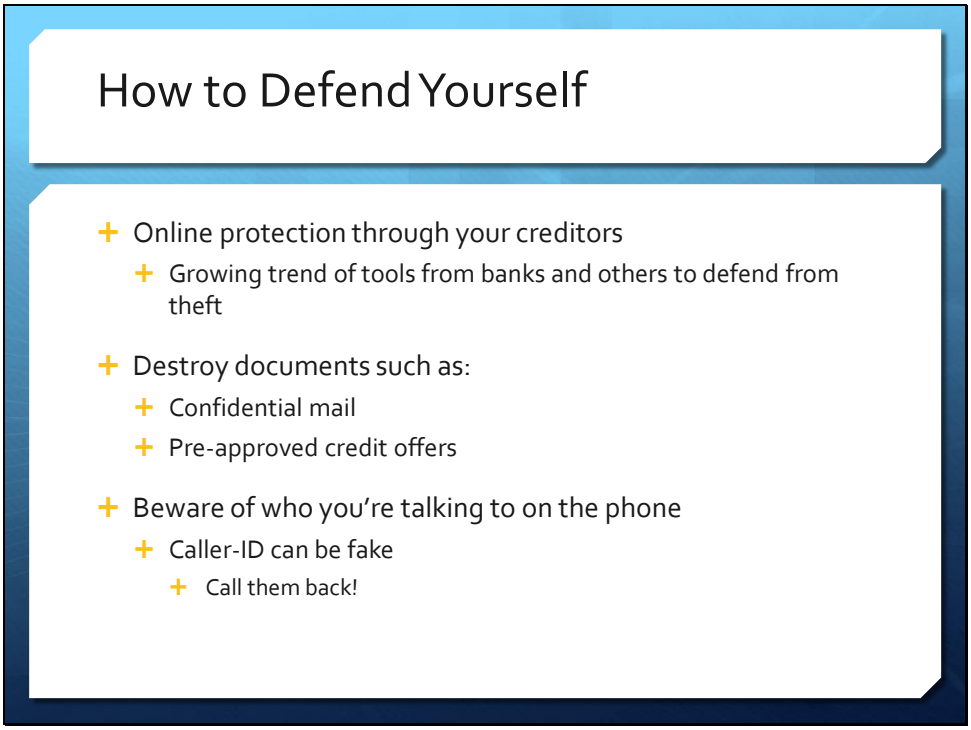
How Does it Happen?

- This isn't all "electronic" theft
  - Dumpster diving
  - Shoulder Surfing (with cell phones)
  - Subterfuge
    - Phishing
    - Pharming
  - Actual theft of property
    - Home
    - Laptop
    - Cell phones
    - PDAs

Slide 6


How Does it Happen? (Cont.)
Double swiping your credit card
Using other people as sources of information
Using you as the source of information
Address changes
Skimming

Slide 7

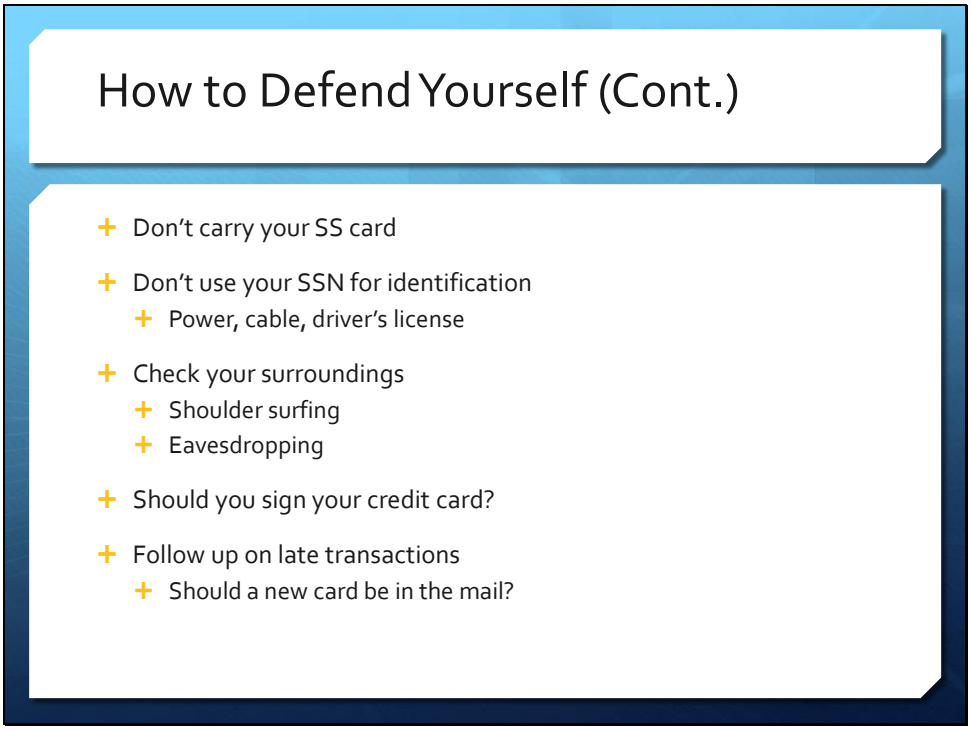

How to Defend Yourself
Online protection through your creditors
Growing trend of tools from banks and others to defend from theft
Destroy documents such as:
Confidential mail
Pre-approved credit offers
Beware of who you're talking to on the phone
Caller-ID can be fake
Call them back!

Slide 8

How to Defend Yourself (Cont.)

- Don't have a single point of theft
  - Take credit cards with you as you need them
  - Don't carry them all together
- Verify your credit reports
- Use different passwords for your accounts
  - This can be difficult but worth the effort

Slide 9

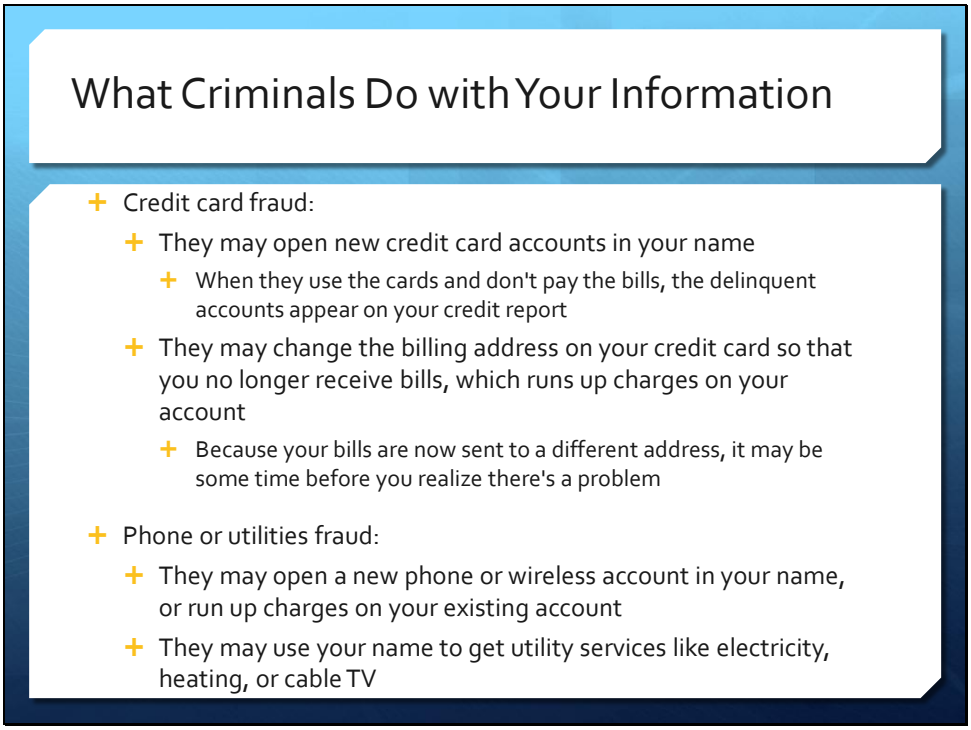

How to Defend Yourself (Cont.)
Don't carry your SS card
Don't use your SSN for identification
Power, cable, driver's license
Check your surroundings
Shoulder surfing
Eavesdropping
Should you sign your credit card?
Follow up on late transactions
Should a new card be in the mail?

Slide 10

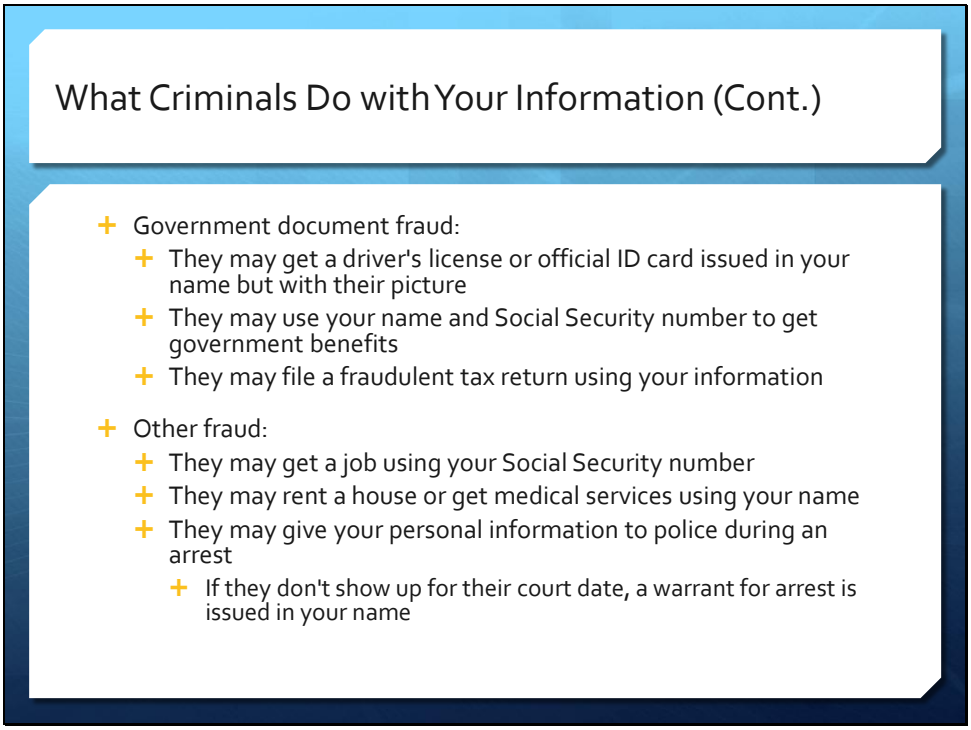
How to Defend Yourself (Cont.)

- Beware of online credit card use
  - It is safe, if you're prepared
  - Later we'll talk about SSL/Encryption options
- Know what your creditor offers for your protection

Slide 11


What Criminals Do with Your Information
Credit card fraud:
They may open new credit card accounts in your name
When they use the cards and don't pay the bills, the delinquent accounts appear on your credit report
They may change the billing address on your credit card so that you no longer receive bills, which runs up charges on your account
Because your bills are now sent to a different address, it may be some time before you realize there's a problem
Phone or utilities fraud:
They may open a new phone or wireless account in your name, or run up charges on your existing account
They may use your name to get utility services like electricity, heating, or cable TV

Slide 12


What Criminals Do with Your Information (Cont.)
Government document fraud:
They may get a driver's license or official ID card issued in your name but with their picture
They may use your name and Social Security number to get government benefits
They may file a fraudulent tax return using your information
Other fraud:
They may get a job using your Social Security number
They may rent a house or get medical services using your name
They may give your personal information to police during an arrest
If they don't show up for their court date, a warrant for arrest is issued in your name

Slide 13

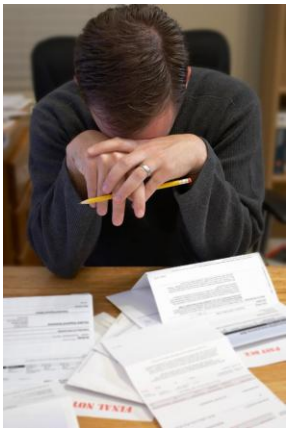
What Criminals Do with Your Information (Cont.)

- Bank/finance fraud:
  - They may create counterfeit checks using your name or account number
  - They may open a bank account in your name and write bad checks
  - They may clone your ATM or debit card and make electronic withdrawals your name, draining your accounts
  - They may take out a loan in your name

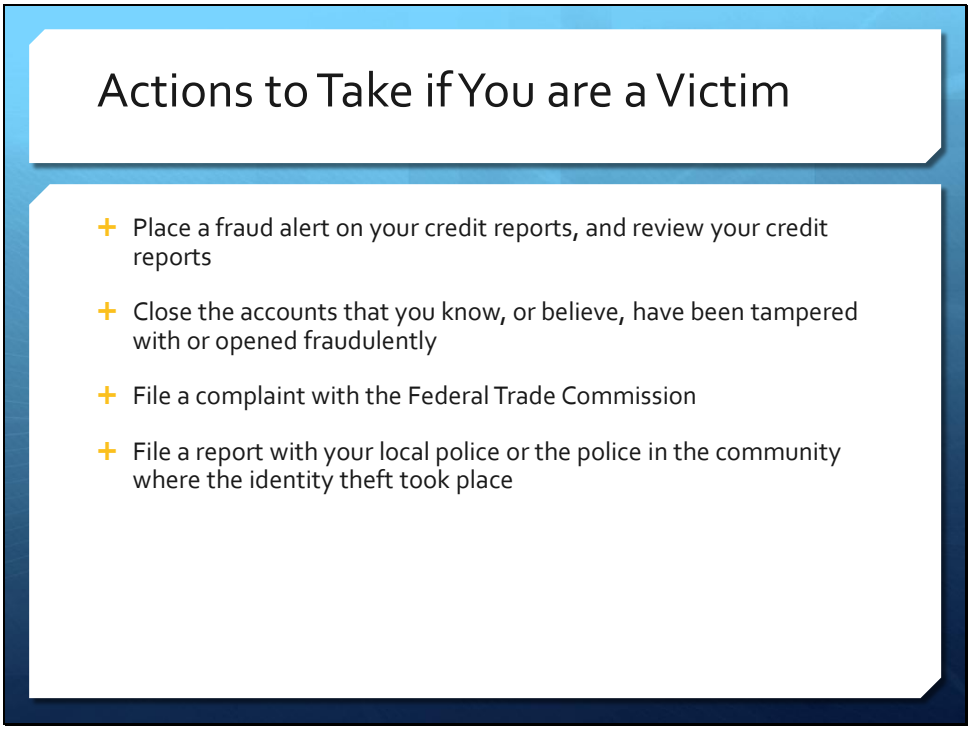
Slide 14

How Can You Tell if You're a Victim?

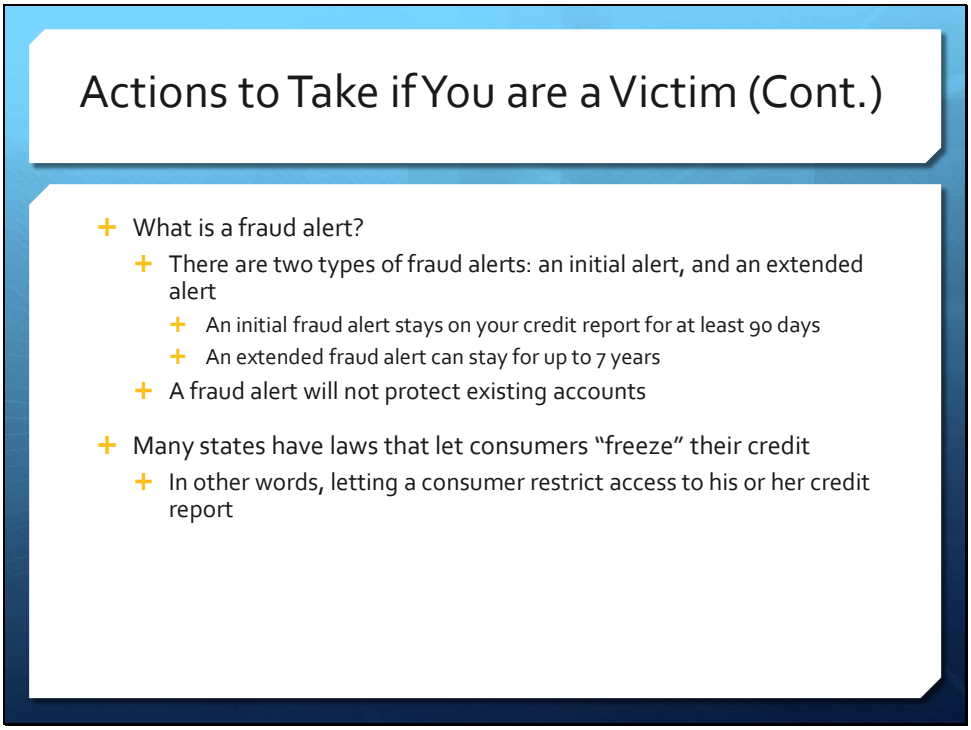
- Bills from unknown sources
- Charges on credit card statements
- Credit scores change
- W-2 form for unknown employer
- Police at your door!



Slide 15


Actions to Take if You are a Victim
Place a fraud alert on your credit reports, and review your credit reports
Close the accounts that you know, or believe, have been tampered with or opened fraudulently
File a complaint with the Federal Trade Commission
File a report with your local police or the police in the community where the identity theft took place

Slide 16


Actions to Take if You are a Victim (Cont.)
What is a fraud alert?
There are two types of fraud alerts: an initial alert, and an extended alert
An initial fraud alert stays on your credit report for at least 90 days
An extended fraud alert can stay for up to 7 years
A fraud alert will not protect existing accounts
Many states have laws that let consumers "freeze" their credit
In other words, letting a consumer restrict access to his or her credit report

Slide 17

Contact Information

- Equifax Credit Bureau
  - 1-800-525-6285
- Experian Information Solutions
  - 1-888-397-3742
- TransUnion Credit Bureau
  - 1-800-680-7289
- Federal Trade Commission
  - 1-877-IDTHEFT (438-4338)
- Social Security Administration, Fraud
  - 1-800-269-0271

TransUnion

FEDERAL TRADE COMMISSION • UNITED STATES OF AMERICA • MCMXV

Questions and Answers

Review Questions:

1. You just learned that you have a new credit card being used in your name. You're more than likely a victim of what?
    A. Defamation attacks
    B. Identity theft
    C. Accounting malpractice
    D. Banking error

2. True or False: Stolen identities are only used for online theft or financial gain.
    A. True
    B. False

3. Which of the following would be non-electronic (not done by computer) types of social engineering? (Choose all that apply)
    A. Dumpster diving
    B. Phishing
    C. Phone calls
    D. Pharming

4. An identity thief just took a picture of your credit card when you pulled it from your wallet to use at the cashier's POS. What type of social engineering attack would that be?
    A. Dumpster diving
    B. Eavesdropping
    C. Shoulder surfing
    D. Theft

5. What method could be used to steal your credit card numbers for illegal use?
    A. Double swiping
    B. Skimming
    C. Address change notification
    D. All of the above

6. True or False: One of the best ways to get rid of your private documents would be through shredding.
    A. True
    B. False

7. You've learned that your company has been targeted in a recent social engineering attempt through telephone communications. To help lower risk of this attack, you should do which of the following on any suspicious call? (Choose all that apply)
    A. Alert the designated security team
    B. Call the police department
    C. Verify the phone number from caller-id
    D. Verify the phone number by calling that person back

8. True or False: It's ok to use the same password for all of your online accounts, just as long as it's a complex and long password.
    A. True
    B. False

9. How might you be able to determine if you're a victim of identity theft? (Choose all that apply)
    A. Undocumented charges to your credit card
    B. Changes to your credit report
    C. You can't really tell
    D. Phone calls from unknown creditors

10. What kind of fraud alert is capable of freezing your credit reports for about 90 days?
    A. Initial
    B. Starter
    C. Extended
    D. Monthly

Answer Key:

1. B
   This would be an example of identity theft.

2. B
   False. An identity thief could also impersonate you for the purpose of committing crimes in your name.

3. A, C
   Dumpster diving and making fake phone calls would be the non-technical side of social engineering.

4. C
   Shoulder surfing is just that, watching (or in this case photographing) actions/passwords/cards while trying to not be obvious in their actions.

5. D
   All of the above are great ways to steal someone's credit card information.

6. A
   True. Having a shredder will keep you safer from a thief dumpster diving and taking your personal information.

7. A, D
   Any suspicions should be reported immediately to your company's security response team. In the meantime, don't trust caller-id, as it's too easily spoofed. Instead, call them back at that number to verify they are at least potentially real.

8. B
   False. This is perhaps tricky because you may have heard me say that a long password is good, but you shouldn't reuse a password. Once one has been discovered, you have more accounts that could be at risk.

9. A, B, D
   These are all ways to determine if you're a potential victim and you should investigate any change of that nature.

10. A
    The option is referred to as an Initial alert.