Preventing Identity Theft
Seminar Overview

• What is identity theft?
• How do crooks get our personal information?
• When do you have to give out your SSN and when can you avoid giving it out?
• How can you protect yourself from fraud?
• What are the Warning signs that you may be a victim?
• Where can you go for help?
• How can Georgia United Credit Union help?
Identity theft is when someone uses your:

- Name
- Social Security number
- Other identifying information

... without your permission, to establish new accounts *in your name*. 
How many victims?

• 2016: $16 billion stolen from 15.4 million people
  *Javelin Strategy & Research, Feb. 2016*

• 40% rise in card-not-present (CNP) fraud
  *Javelin Strategy & Research, Feb. 2016*

• Up to 400,000 children each year (ABC News)

• 13% of all complaints to FTC
  *Consumer Sentinel Network Data Book for 2016*
Data breaches

- BC / BS / Anthem – approx. 80 million customers
- Equifax – approx. 143 million consumers
- Other – Arby’s, Gmail, Yahoo, Kmart, Verizon...
Impact on victims

- **Damaged** credit record
- **Loss** of job opportunities
- **Refused loans**

To resolve problems, average victim spent an **average of six months and 200 hours of work**. Phone calls, written correspondence, keeping track of creditors, responding to letters, working with credit bureaus and law enforcement agencies, etc – FTC via Identity Hawk (2017)
Who’s vulnerable?  All of us!
What do crooks do with your personal information?

• Change billing address
• Open new accounts
• Get loans, cars, phone service
• Authorize electronic transfers
• File bankruptcy
• Give your name during arrest
• ...all in your name!
How is your personal information stolen?

While you’re out ... Stolen wallet, shoulder surfing, skimming
At home ... “Friendly” theft, dumpster diving, unlocked mailbox
Through businesses you use ... Data breach, hacking
By trickery ... Phishing, vishing, social networking site fraud
Data breaches

What type?

▪ Existing account
▪ Potential for unauthorized new accounts

What if you’re a victim?

▪ Request fraud alert, order credit reports, monitor
▪ Consider security freeze
Variations on an ID theft theme
Spamming—Sending unsolicited email indiscriminately to multiple mailing lists, individuals, or newsgroups.

Spoofing—Creating a replica of a legitimate Web page to fool you into submitting personal, financial, or password data.

Phishing—Luring victims to a fake website through spam. Data breach victims are targeted.
Email Red Flags

Beware email red flags:

“Dear Visa customers” or “Dear friend”

“This is an urgent problem”

“Your account will be shut down unless you reconfirm billing information”

“Click on the link in this message”
Protect yourself from phishing attacks

• Don’t click links in emails
• Look for https:// in URL
• Update antivirus software and firewall
• Avoid e-mailing financial information
• Password-protect tax returns
• Report it!
Beware card skimming

**Who? How? Huh?**
- *Thief* attaches skimmer over card slot
- *Device* gleans info from magnetic stripe
- *Wireless camera* videotapes you punching in PIN
- *Thief* drains your account

**Tips:**
- *Suspicious? Walk away*
- *Report suspicious activity*
- *Check statements*
- *Memorize pin*
Your computer may be infected with spyware if it …

• Slows down, malfunctions, displays repeated error messages
• Won’t shut down/restart
• Serves up pop-up ads
• Displays Web pages/programs you didn’t intend to use
• Sends emails you didn’t write
Protect your computer

- Download.cnet.com
- Lavasoft.com
- Onguardonline.gov
- Killdisk.com

HANDOUT: Protect Your Computer
Protect your computer
Mobile device Safety Tips

• Password-protect it with “strong” passwords
• Install security software; download updates
• Enroll in back-up/wiping program
• Limit activities while using public Wi-Fi
• Read fine print before downloading apps
• Install “phone finder” app; report lost phone immediately
Social networking safety tips

• Don’t post exact birth date/place
• Don’t post address, phone, email
• Don’t post embarrassing photos
• Talk about trips—after you return
• Control access—*use privacy settings*
Tips for protecting Social Security number

• Ask “Why do you need it?”
• Keep it off driver’s license
• Don’t use last 4 digits as PIN
• Don’t have SSN preprinted on checks
• Don’t let clerks handwritten it on checks
• Don’t carry it in wallet unless you need it that day
Warning signs you may be a victim of ID theft

• Oftentimes, there aren’t any!
• Statements contain fraudulent charges
• Get bills from unfamiliar companies
• No mail for several days
• Computer is slow, won’t shut down or restart
• Collection agents call
• Denied credit
No warning signs?

• Check your credit report anyway!
  • 2 free/year from each bureau
  • Look for accounts you didn’t authorize
  • Check for accuracy; file disputes

• Beware emails, websites offering “free” credit reports
  • Don’t give SSN just to get free report
If you’re a victim ...

• Fraud alert—get free credit reports
• ID Theft Hotline—call 877-IDTHEFT
• ID theft affidavit—close affected accounts
• Certified letters, return receipt requested—keep copies.
• Police report—give copies to creditors
Resources - links

• https://identitytheft.gov/

• annualcreditreport.com
Questions?