Computer Workshop Series

Identity Theft Prevention Tips

May 2013

Dennis Martin

Demartek

This presentation is available at http://www.demartek.com/Demartek_Identity_Theft_Prevention_Tips_Speaking_Event.html

Agenda

- Identity Theft – What is it?
- Paper Document Handling
- Telephone Privacy
- Computer Security
- Laws, Regulations and Insurance
- Sources of Additional Information

Identity Theft – What is it?

- Identity theft is also known as:
  - ID theft
  - Identity fraud

- Identity theft is the act of stealing your personal information and using it without your permission
  - Usually with intent to commit financial fraud

Who is Affected?

- Victims include all categories of people
  - Age, economic background, race, gender

- In some cases, it can be weeks or months before the victims realize it happened

Who Commits it?

- Petty Thieves
  - Looking to steal your information in order to apply for credit in your name or purchase merchandise or services in your name
- Organized Crime
  - Sophisticated fraud operations
  - Can be international in scope

Security vs. Convenience

- Security and Convenience are inversely related
  - Higher security results in less convenience
  - Higher convenience results in less security

Security and Risk Management

- What are the threats?
- Which threats are the most likely to occur?
- What can be done to mitigate these threats?
- How much time, money and effort are you willing to devote to mitigating specific threats?

Disclaimer

- The steps discussed in this presentation cannot guarantee that you won't have your identity stolen, but will reduce the risk of this occurring

- I personally practice these steps

Your Trash, Privacy and ID Theft

- U.S. Supreme Court Case: ***California vs. Greenwood***, 486 U.S. 35 (1988)
  - The Fourth Amendment does not prohibit the warrantless search and seizure of garbage left for collection outside the curtilage of a home
  - There is no reasonable expectation of privacy for anything you put in your garbage
  - This garbage is readily accessible to members of the public
- "Dumpster Diving" is one ID theft technique

Paper Document Handling

- Get a good shredder
  - ***Strip-cut*** (not very good, in my opinion)
  - ***Cross-cut*** (better), small pieces
  - ***Micro-cut*** (best), tiny pieces, most expensive
  - Many also handle staples, credit cards, CDs/DVDs
  - Most have a limit to continuous run time

Shredding Guidelines

- There should be no trash or recycled paper leaving your residence that includes your name, address or other personal information that is legible
  - Shred these documents before discarding
  - Also shred the envelopes from statements, etc.

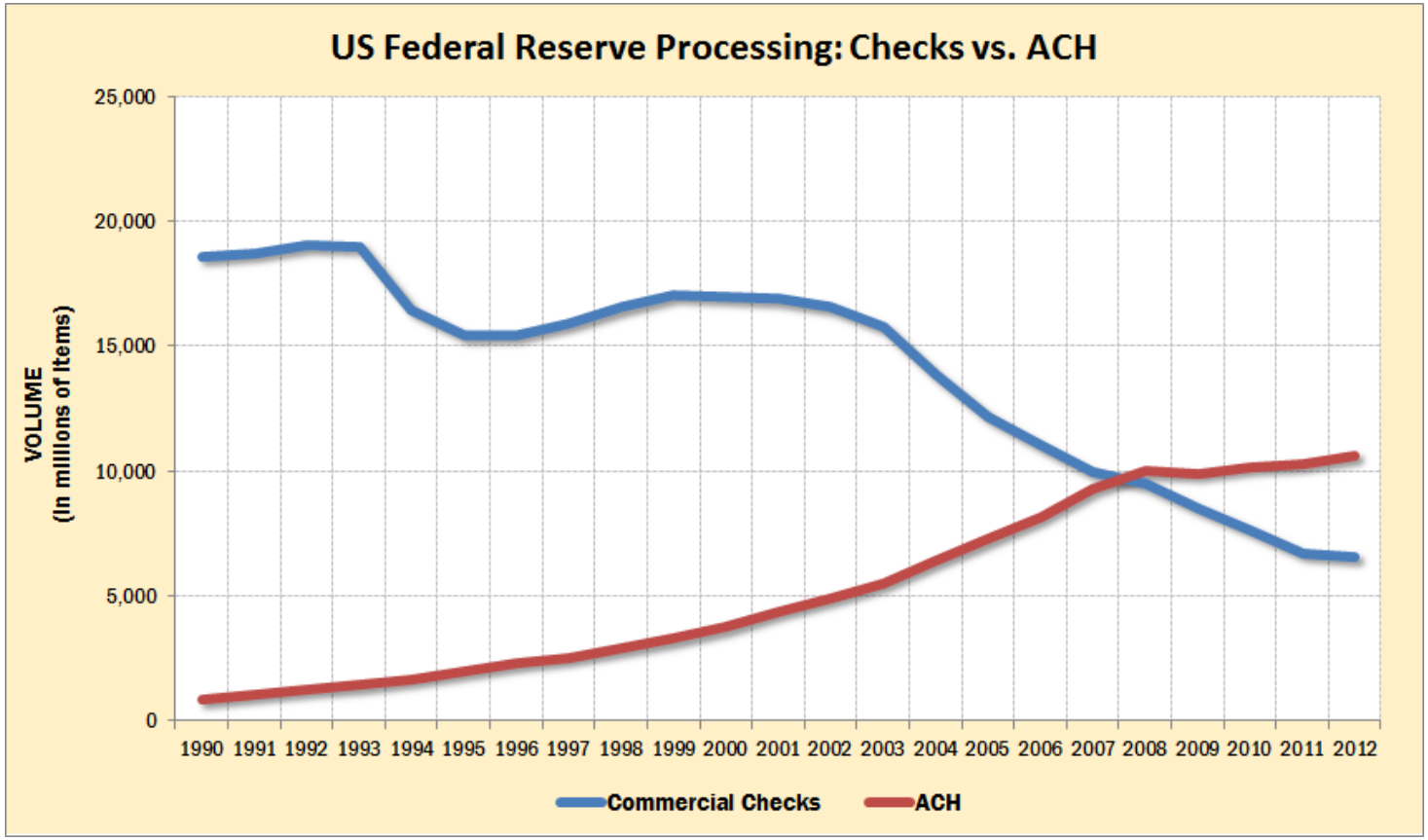
Outgoing Mail

- Take all out-going mail to the post office or package delivery office to avoid mail-tampering
  - Identity thieves look through mailboxes, looking for anything with financial or personal information

DO NOT MAIL

- Get removed ("opt-out") from mailing lists
  - US Direct Marketing Association (DMA) http://www.DMAchoice.org
  - Credit Card offers https://www.optoutprescreen.com
  - Credit offers – reply with "***permanently remove me from your mailing list***"

Banking – Checks vs. ACH



Source: U.S. Federal Reserve – http://www.federalreserve.gov/paymentsystems/default.htm

Secure Check Handling

- Keep checks in a secure location
- Use “high-security” check features
- Do NOT have your social security, driver’s license or other government ID printed
- Some people only have first and middle initials printed on checks
- Write with indelible ink – avoid check washing
- When sending checks in the mail, use security envelopes or wrap with extra sheet of paper
- Banks can have new checks delivered to branch if your home mailbox is not secure

Credit & Debit Cards

- Sign with permanent ink
  - Unsigned cards are not valid
- Do not lend cards to friends or relatives
  - Banks will either consider that these charges are yours, or some banks will close the account
- Keep in secure location
  - Frequent thefts: glove box of car and unattended at work
- Check your bank statements regularly
  - Online is usually up to date, often same-day
- Give your travel plans to your bank

Credit Freeze and Fraud Alerts

- If you suspect that somebody might be trying to establish credit in your name, request a “credit freeze” or “fraud alert” with credit card reporting companies
- “Credit Freeze” prevents credit reporting company from releasing your credit report without your consent
  - Enforced by various state laws
  - Even you will have to take extra steps to obtain credit
  - You must file this separately for each credit reporting company
  - You must file to release it (“thaw”)
- “Fraud Alert” is a temporary, cautionary flag on your credit file that encourages lenders to take extra precautions

Social Security Numbers

- Do NOT carry your social security card
  - Needed only for employment verification
  - Keep in a secure location
- SSN is **CONFIDENTIAL**!
  - Should NOT be printed on documents, IDs, etc.
  - Do not advertise or give out your SSN (few exceptions)
  - US Military DD 214 may have SSN publicly available – there are procedures to redact
- Social Security Administration sends a yearly statement – check the amounts
  - http://www.socialsecurity.gov/myaccount/

Telephone Privacy

- Telephone directories and your information
  - Main listing – everything public and sold
  - Non-listed (“unlisted”) – not in printed directory but available through directory assistance (411)
  - Non-published (“unpublished”) – not in printed directory, not in 411, and not sold
- DO NOT CALL
  - National: https://www.donotcall.gov/
  - Colorado: https://www.coloradonocall.com/
  - Most US States have a “do not call” website

Children

- In addition to protecting your own identity, parents and guardians should take steps to protect the identity of their children
  - In some divorce cases, a parent who has bad credit may use the child's identity to obtain credit or services such as utilities, etc.
  - Secure your child's social security number and other important documents
  - Teach your children the importance of keeping certain information private

Break Time

Upcoming Workshops

- June 2 – How to Build a Computer
  - We will explain the major components of a computer and build a computer during the workshop. No experience is necessary.

Computer Passwords – Bad

- Bad passwords
  - Blank – no password is inviting theft
  - Simple – little thought to create or guess
    - Ex.: secret, password, admin, god, 123456, abc123
    - There are lists of common (“stupid”) passwords
    - Automated attack tools try these common passwords
  - Default – any vendor-supplied, easy to discover
  - Personal information – anything based on:
    - Names of family members, pets, birthdays, favorite sports team, musician, special license plates

Passwords – Best Practices

- Good password: letters & numbers & symbols
  - 8 or more characters
- Separate and unique passwords for each:
  - Financial (bank, investments, etc.)
  - Social media (Facebook, LinkedIn, Twitter, etc.)
  - Email accounts (gmail, yahoo, hotmail, etc.)
  - Retail (Amazon, airlines, etc.)
- Identity thieves will hack one account in order to try to hack others

Computer Protection

- Must-haves
  - Anti-virus software
  - Anti-spyware software
  - Firewalls (hardware and software)
- Best practices
  - Keep current with security patches
  - Delete web browser “cookies” periodically
    - Some browsers have “privacy” mode, blocks cookies
    - Browsers can block cookies from specific sites

Data Protection

- Make backup copies of your data!
  - Your data is worth far more than your computer
  - I keep data on a separate drive from the O.S.
- If you are selling or donating computer equipment, be sure to fully delete your data before that equipment leaves your control
  - Previous workshop on May 5, presentation: http://www.demartek.com/Demartek_Presents_Data_Destruction_Methods.html

Phishing

- Criminals attempting to convince you to give your data using deceptive emails & websites
  - "Please confirm your account"
  - "Somebody has a crush on you"
  - "Advance Fee" scams (Nigerian 419 and Lottery)
  - Work from Home scams ("Money Mule")
  - Child pornography scams
  - Jury duty scams

Spear-Phishing

- Targeted emails that appear to have been sent by somebody you know (boss, family member, supplier, etc.)
  - Criminals do some research on you specifically to use subject lines that you might be more likely to open

Smishing & Vishing

- Smishing: Phishing via SMS (text messaging)
- Vishing: Phishing via voice mail
- “Your ATM card has been suspended”, call this number to resolve or confirm information
- Mobile users are more likely to submit information to a bad site (my opinion: “gullible”)
- If you get one of these, call your bank’s real telephone number, not the one in the message you received

Websites

- Always use secure http (“https://”) for websites where you have accounts
  - Banks, Financial institutions
  - Facebook, LinkedIn, Twitter, Pinterest
  - Email: gmail, yahoo, hotmail
  - Retail: Amazon, airlines, etc.
- HTTPS pages will have the padlock symbol in the browser address bar

Data Breach Laws & Regulations

- These laws and regulations require direct or public disclosure of data breaches
  - California Security Breach Information Act, SB 1386, effective July 1, 2003
    - Most other US States have passed similar laws
  - US Federal Reserve Board ruling, effective March 23, 2005
  - US Federal Trade Commission “Red Flag Rules”, effective July 8, 2008

Identity Theft Insurance

- Insurance policies offered by
  - Insurance companies as an endorsement to a homeowner or renter policy, or as stand-alone policy
  - Some banks and employers
- Provide coverage to reimburse expenses to recover from identity theft
  - Does not cover monetary losses from ID theft
  - Some expenses may require prior consent

More Resources

- Federal Trade Commission
  http://www.consumer.ftc.gov/features/feature-0014-identity-theft
- FBI
  http://www.fbi.gov/about-us/investigate/cyber/identity_theft
- Privacy Rights Clearinghouse
  https://www.privacyrights.org/Identity-Theft-Data-Breaches
- Most US State websites for Department of Consumer Affairs or Attorney General

Demartek Resources

- Demartek Identity Theft Prevention Tips and Commentary Report
  - Available in English and Spanish
  - http://www.demartek.com/Demartek_Identity_Theft_Prevention_Tips_and_Commentary.html
- Current version published in 2009, updated version planned for 2013

Thank You!

Dennis Martin, President
dennis@demartek.com
www.linkedin.com/in/dennismartin

Demartek

(303) 940-7575
www.demartek.com
http://twitter.com/Demartek
www.youtube.com/Demartek
Skype: Demartek

To learn more about Demartek:

- Download the Aurasma App (Android/iPhone)
- Search and follow "Demartek"
- View image below with viewfinder.

*also on the back of Dennis' business card

Powered by: AURASMA