Identity Theft
March 2017

Improving your odds

Purpose

- To alert you to the causes of Identity Theft
- To provide resources where you can learn about the subject
- To outline steps you can take to lesson your risks

Background

- It all started with an article in Wired Magazine
- I became curious
- I then made some phone calls
  - My bank
  - A Financial Institution
  - My Credit Card company, etc.
- I then started my research
  - How do you know when you're done?

Started noting typical activities

- Ordered from catalog at a store
- Swiped credit card at the market & gas station
- Bought a book at Amazon
- Rented a car on Maui
- Paid for meal at restaurant with credit card
- Conducted online banking
- Checked credit card balance on line
- Received insurance statements in the mail
- Given a receipt with full credit card # visable

Fraud versus Identity Theft

- Fraud is when you grab someone's credit card, you steal their wallet, you use their credit card to buy things.
  - Not on the rise so much
- Identity theft is more complex, because you're taking people's identifiers, particularly their name and their Social Security number, and applying for credit in their name. So it's more behind the scenes.
  - On the rise
  - Easy, low risk

Per NPR.COM

How is it done?

- Dumpster diving
- Stealing your mail or wallet/purse
- Skimming your credit card
- Phishing
- Obtaining your Credit Report illegally
- Business record theft – an office is robbed
- Diverting your mail
- Spyware and Keylogger

Some statistics

- Bank failures causing Phishing to flourish
  - 465 bank failures last 4 years
- 314,248 Complaints reported to IC3
  - Internet Crime Complaint Center
- California ranked #1 in 2011
  - 34,000 complaints, $485 million loss (that has been reported)

Avoid being a victim

- Throw away your phones
- Toss out your PC and iPad
- Don’t use your mailbox
- Destroy your wireless network
- Put your wallet in a safety deposit box
- Don’t fill out any forms at your doctor’s office
- Burn your filing cabinets
- Now – you may stand a chance
- Cancel your Facebook account

Unbelievable – I think not

- One consumer took an unsolicited credit card offer, ripped it up, reassembled it, and then submitted it to a bank with a change of address. The bank issued the card and sent it to the new address, thus demonstrating that a thief could easily use even a torn-up offer to commit fraud.
- The owner of a dog had signed up for a free e-mail account in his pet's name and later received a pre-approved credit offer for a Clifford J. Dawg.

Tips #1

- Avoid paper statements by mail
- Keep SS and Medicare cards & Tax Returns locked up
- Use strong passwords – avoid dictionary words
- Use Credit Card with your photo on it
- Review your Credit Report every 4 months*
- Review all accounts online frequently
- Don’t use SS number to log into any site
- Never give out any personal information (impossible)
- Change passwords frequently
- Log off password manager when away from your PC

Tips #2

- Don’t leave a wallet or phone in your car
- Put as little information as possible on your checks
- Use virtual credit card numbers when merchant is in doubt
- Avoid debit cards
- Use a unique credit card for automatic deductions
- Don’t post vital information online (Facebook)
- Opt out of receiving offers of credit in the mail*

Tips #3

- Place Fraud Alerts on your account*
  - Only need to do one bureau
- Freeze your credit*
  - Must do at all 3 bureaus
- Read all of the information here
- Review Credit Report Monitoring Services here
- Read how to reduce risks here
- Update your PC religiously
  - Anti-virus, Flash, Windows
- Generate your own security questions

Tips #4

- Scan PC with anti-malware programs often
- Backup all data on your PC frequently
- Shred all paper with any vital info on it
- Call your Credit Card company and bank and ask them what protection they provide
- They also provide paid protection which you may or may not need
- Don’t store any passwords on your PC
- Use an unique Recovery email address for Gmail

Credit Report Services

- Companies like LifeLock and IdentityGuard
  - Don’t freeze your credit
  - Don’t place fraud alerts
  - Do notify you when there are changes to your Credit Report and many more things
  - Do provide free Credit Scores and Reports, some update this annually or quarterly

Typical fraud scenario

- My credit card was “skimmed” at a gas station in Palm Desert and my card was charged $179
- I was not liable for any charges but had to obtain a new card
- Basically, Credit Card companies and banks protect you against fraud
- Fraud is not the major threat

Typical Identity Theft scenario

- A shopper walks into a BestBuy and opens a credit card in my name
  - This is identity theft
  - What happens next depends on what preventative measures you took
- Someone opens a line of credit in your name
  - How do you find out?

What steps could have been taken?

- Placed a Fraud Alert with major credit bureaus before the fraud was attempted
  - “Should” prompt BestBuy to contact you first
- Placed a Credit Freeze with the credit bureaus
  - BestBuy now unable to run a credit check
  - Even you can’t apply for a Macy’s credit card to save 15%
  - Now - no one can open a line of credit!

Alerts and Freezes may be an answer

- Fraud Alert - any creditor that is asked to extend credit is asked to contact the consumer by phone and verify that the credit application was not made by an identity thief. The merchant may or may not do this.
- Credit Freeze or frequently referred to as a Credit Lock or Security Freeze - prevents anyone from accessing your credit making it virtually impossible for anyone to open a line of credit, new credit card, etc. in your name.

What to do if you're victimized

- File a report with the FTC at https://www.ftccomplaintassistant.gov/. You can also call them at 1-877-438-4338
- File a police report and take the FTC report with you
- Call credit card company and bank, etc.
- Follow all of the steps listed at https://www.privacyrights.org/fs/fs17a.htm.
- Read the document titled Taking Charge at http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf.
- Visit Identity the Theft Resource Center (ITRC) at http://www.idtheftcenter.org/.

Basic “Do it Yourself” plan

- Place Fraud Alert
- Place Credit Freeze
- Practice the tips included above

- For additional piece of mind subscribe to Identity Theft Protection Service – either paid or free (AAA)

What I did

- Tried a subscription to 2 Identity Theft services
- Created stronger passwords
- Placed Credit Freeze with all 3 bureaus
- Placed Fraud Alert with 1 bureau
- Made sure Apple ID used unique email address
- Made sure Gmail recovery email address is unique
- Signed up for AAA free credit monitoring
  - They offer free Resolution Service 877-440-6943
  - They also offer a Lost Wallet service

Conclusions

- The more steps you take, the more you are inconvenienced
  - ***Security versus convenience is the big tradeoff***
- Freezes, Fraud Alerts and Credit monitoring plus staying vigilant will help quite a bit

Important Contacts

- Internet Crime Complaint Center (IC3)
  - www.ic3.gov
- Federal Trade Center
  - http://www.consumer.ftc.gov/features/feature-0014-identity-theft
  - http://www.ftc.gov/ or 877.382.4357
- US Postal Inspection
  - https://postalinspectors.uspis.gov/

Important Contacts

- Department of Consumer Affairs
  - www.dca.ca.gov or 800-952-5210
- CA Dept. of Real Estate
  - www.dre.ca.gov or 213-620-2072
- Department of Justice site
  - http://www.justice.gov/criminal/fraud/websites/idtheft.html
- Financial Industry Regulatory Authority
  - www.finra.org

Important Contacts

- American Express: 800-297-7672
- Discover Card: 800-347-2683
- MasterCard: 800-622-7747
- VISA: 866-434-6854
- Social Security Administration: 800-772-1213
- Password strength information here
- OnGuardOnline here