It’s not going away…

Identity Theft

San Francisco Bay ISSA 03/12/2014

First, the Scary Statistics…

From Bureau of Justice Statistics www.bjs.gov 2012

- About 7% of persons age 16 or older were victims of identity theft in 2012.
- The majority of identity theft incidents (85%) involved the fraudulent use of existing account information, such as credit card or bank account information.
- Victims who had personal information used to open a new account or for other fraudulent purposes were more likely than victims of existing account fraud to experience financial, credit, and relationship problems and severe emotional distress.
- About 14% of identity theft victims experienced out-of-pocket losses of $1 or more. Of these victims, about half suffered losses of less than $100.
- Over half of identity theft victims who were able to resolve any associated problems did so in a day or less; among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems.

How Does Your Identity Get Stolen?

- With little more than a SSN, thieves can apply for and obtain credit in your name.
- Often all that's required to make changes to an existing account is the last four digits of one's SSN, their DOB and home phone number.
- Once a thief makes changes to your bank/credit card accounts (i.e., address, email, phone number changes) your cash and credit can be accessed without your knowing it.
- Thieves know that many department stores allow customers who have forgotten their store credit card to do an account look up by SSN alone in order to make in-store purchases.
- Often the thief will use your identity to authorize other users to access accounts or make purchases with your store credit line.

How Do Thieves Obtain Your Personal Information?

- By stealing mail from your mailbox including credit card/bank statements, utility bills, w2s and unsolicited applications for pre-approved credit.
- By sifting through trash and recycled computer media for statements, receipts and other paperwork with personal details.
- From employees who work for institutions with access to your personal information including banks, car dealerships and doctor's offices. There is a black market for completed credit applications.
- Lost or stolen wallets or purses.
- Skimmer devices on credit/debit card readers.
- By search public records and accessing personal data you provide on social networking sites (DOB, phone number, address, etc.).
- Email phishing and social engineering attacks by phone.

Telltale Signs your Identity has Been Compromised

- Unexpected purchases on credit card and debit statements.
- Calls from creditors asking to verify information on an application for credit received in your name or containing your SSN.
- Frequent calls from an unknown number or area code or otherwise invalid phone numbers that appear on your phone's caller ID.
- New, unexpected credit cards in the mail!
- Alerts from monitoring agencies, assuming you subscribe to one.

Steps To Take If Your Identity Has Been Stolen

- Start a journal. Note dates and times of events. Track hours spent and expenses .
- At the first sign of fraudulent activity, contact your bank and creditors using the numbers provided on the back of the cards.
- Immediately file a Fraud Alert with any one of the three main credit bureaus (Equifax, Transunion, Experian), they will notify the other bureaus of the alert and activate a 90 day fraud alert.
- Contact the FTC and file a Fraud Report.
- File a report with your local police department, you can likely do this online very easily.
- Request a free copy of your credit report from all three bureaus using Annualcreditreport.com.
- Ask each bureau to remove any inquiries or other information generated by the fraudulent use of your personal information. Provide them with a copy of the Police Report # and PD contact information and ask that they work with the police in the investigation.
- Call any creditors who are listed on the report under “inquires”. If an account was already opened it can take up to 90 days to appear on the report.

Minimizing Your Risk for Identity Theft

- Be proactive – review online banking and credit card statements often; you may catch something before your bank or creditor does.
- Subscribe to a monitoring service such as lifelock.com.
- Shred ALL personal paperwork.
- Request that your banks and creditors implement a “special password” that you share with them and that must be provided by anyone attempting to make changes to any account information.
- Use obscure answers to online security questions (i.e. Where did you go to elementary school? Answer: Purple).
- Department stores commonly allow customers to look-up their account number by simply providing a name and SSN. Request that creditors block this option from your account. Consider canceling cards with creditors who refuse.

Who to Contact if You Are a Victim of ID Theft

- The Federal Trade Commission offers a plethora of information about identity theft, from how to avoid it to how the respond once you discover you've become a victim. Following are several links to the FTC and the three credit bureaus you should be aware of:

  - http://www.consumer.ftc.gov/features/feature-0014-identity-theft
  - http://www.consumer.ftc.gov/topics/protecting-your-identity
  - https://www.annualcreditreport.com/index.action
  - https://www.experian.com/fraud/center.html
  - http://www.transunion.com/personal-credit/credit-disputes/fraud-alerts.page
  - http://www.equifax.com/answers/set-fraud-alerts/en_cp

What Improvements Can We as Service Providers Make?

- Stop relying on SSNs as a defacto means of customer authentication.
- Provide better “secret password” support on accounts, avoid relying on so heavily on SSN. Don’t wait until the customer reports fraud to enable these options.
- Require stronger authentication requirements for changes to existing accounts, be more thorough when sending change notifications.
- Stop using caller-ID/ANI as an authentication factor, these numbers can be faked.
- Allow for personalized security options when the account is opened (e.g. “would you like us to require you visit our store/branch to make a change of address or phone number?).