Identity Theft in Today’s World

April 11, 2018

Agenda

What are the Types of Identity Theft?

How does Identity Theft Happen?

What Can Your Credit Union Do?

How Can You Protect Your Identity & Your Members?
Identity theft claims 16.7 million victims.

Identity thieves stole $16.8 billion in total fraud losses from consumers.

Identity fraud victims spend an average of 104.6 hours resolving fraud.

What is Identity Theft?

- FDIC describes Identity Theft as a serious crime and occurs when someone uses information about you, without your permission.
Who is a victim of Identity Theft?

- Everyone

Who are the victims?

<table>
<thead>
<tr>
<th>Age Group</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>70 and Over</td>
<td>6%</td>
</tr>
<tr>
<td>60-69</td>
<td>14%</td>
</tr>
<tr>
<td>50-59</td>
<td>20%</td>
</tr>
<tr>
<td>40-49</td>
<td>20%</td>
</tr>
<tr>
<td>30-39</td>
<td>21%</td>
</tr>
<tr>
<td>20-29</td>
<td>15%</td>
</tr>
<tr>
<td>19 and Under</td>
<td>4%</td>
</tr>
</tbody>
</table>
Types of Identity Theft

- Social Security
  - Most valuable
  - Can be used by the criminal or sold
  - Access to forge documents/collect social security benefits

- Financial
  - Credit card or bank account information
  - Can be quickly maxed out
  - Tend to start with “test” transactions

- Driver’s license
  - May look like the perpetrator or person purchasing the card
  - Can damage your driving record/DUI

- Criminal
  - Access to your identity and charged with a crime/court appearances/fees

Types of Identity Theft

- Medical
  - Can be used to access your medical records and prescriptions
  - Can lead to access denied or medical decisions being made that can adversely affect your health

- Insurance
  - Typically medical insurance
  - Higher premiums/outstanding medical bills

- Synthetic
  - Discuss in more detail later as this is very prevalent

- Tax
  - Using information to get tax refunds

- Child
  - Using a child’s information
How does Identity Theft Happen?

• Shoulder surfing
• Stealing mail
• Sending spam
• Skimming
• Social media
• Dumpster diving
• Impersonation to get access to credit files
• Insider
• Social engineering/Phishing emails

What can be done with the information?

• False applications for loans and credit cards
• Fraudulent withdrawals from bank accounts – including lines of credit
• Fraudulent use of online accounts
• Obtaining other goods or privileges
Serious Consequences

- Ruin Credit
  - Housing
  - Employment
- You will be responsible.
- May have to Pay
- Even if you didn’t know

10 things to leave out of your wallet:

- Social Security Cards
- Birth Certificates
- Receipts
- Gift cards
- Extra credit cards
- Blank checks
- Passports
- Medicare cards
- Spare keys
- PINs and passwords
**What do the criminals steal?**

<table>
<thead>
<tr>
<th>PINs</th>
<th>Utility Bills</th>
<th>Tax Information</th>
<th>Insurance Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Names</td>
<td>Deposit Slips</td>
<td>Loan Applications</td>
<td>Vehicle Registration</td>
</tr>
<tr>
<td>Checks</td>
<td>Medical Cards</td>
<td>Customer Records</td>
<td>Social Security #</td>
</tr>
<tr>
<td>E-Mails</td>
<td>Dates of Birth</td>
<td>Benefit Documents</td>
<td>Prescription Information</td>
</tr>
<tr>
<td>Receipts</td>
<td>Parent Names</td>
<td>Credit Card Offers</td>
<td>Credit Card Statements</td>
</tr>
<tr>
<td>Addresses</td>
<td>Phone Numbers</td>
<td>Investment Reports</td>
<td>Bank Account #s</td>
</tr>
<tr>
<td>Passports</td>
<td>Driver’s License</td>
<td>Employee ID Badges</td>
<td>Access Cards and Codes</td>
</tr>
<tr>
<td>Passwords</td>
<td>Student ID Cards</td>
<td>Medical Information</td>
<td>Proprietary Information</td>
</tr>
</tbody>
</table>

**REMEMBER THE ACRONYM “SCAM” TO GUARD**

- **Be STINGY** with your personal information.
- **CHECK** your financial information regularly.
- **ASK** for three credit reports a year, one from each of the major credit reporting agencies.
- **MANAGE** the damage.
A crime wave in the making......

- Sophisticated identity theft rings continue to evolve
  - 1970s – evolved as students would assume stolen identities to stay past the expiration of a student visa
- Global black market for identity data
  - Recent commercials – grocery check out lane or vending machine
- Increased involvement by organized crime
- Increased involvement by street gangs

Synthetic Identity Theft

- Definition – fraud that involves the use of a fictitious identity
- Combining real and fictitious information to create a new identity
- Used to get credit, driver’s licenses, passports, etc
Synthetic Identity Theft

• Use SSNs of deceased and children
• On the rise over the past five to seven years
• Study by Carnegie Mellon’s CyLab discovered that children’s SSNs are 51 times more likely to be used in synthetic fraud than adults

How much is your identity worth?

• Social Security number: $1
• Credit or debit card (credit cards are more popular): $5-$110
  ▪ With CVV number: $5
  ▪ With bank info: $15
  ▪ Fullz info: $30
  Note: Fullz info is a bundle of information that includes a “full” package for fraudsters: name, SSN, birth date, account numbers and other data that make them desirable since they can often do a lot of immediate damage.
How much is your identity worth?

- Online payment services login info (e.g. Paypal): $20-$200
- Loyalty accounts: $20
- Subscription services: $1-$10
- Diplomas: $100-$400
- Driver’s license: $20
- Passports (US): $1000-$2000
- Medical records: $1-$1000*
  - *Depends on how complete they are as well as if it’s a single record or an entire database
- General non-Financial Institution logins: $1

Note: Prices can vary over time and prices listed below are an estimation and aggregation based on reference articles and hands on experience of Experian cyber analyst the last two years.
Your identity is a steal on the Dark Web. Here are what the most common pieces of information sell for:

- Social security number: $1
- Online payment services login info (e.g., PayPal): $20-$200
- Credit or debit card (credit cards are more popular): $5-$110
- Drivers license: $20
- Loyalty accounts: $20
- General non-financial institution login: $1
- Subscriptions services: $1-$50
- Medical records: $1-$1000**

**Net sales:**
- With CVV number: $15
- With card info: $30
- Full info: $70

Deter - Detect - React

- Keep your records safe
- Shred
- Collect your mail
- Only when absolutely necessary
**Deter - Detect - React**

- Use strong passwords
- Secure Websites
- Do not respond
- No Public PC
- Security Software

**Detect**

- Read
- Watch
- Check
- Request
Detect - What to look for?

- Look for:
  - Misspelled words on websites or in emails
  - If poorly grammar usage is being there
  - Asking for more information than normal
    - SSN
    - PIN
    - Date of Birth
  - Missing security verifiers – HTTP not HTTPS

Deter - Detect - React

Don’t Get Caught!

- Look for the 's' in 'https' or 'http'.
- The lock indicates a secure web connection.
- The ‘Real Name of the site’ is important.
- Add the lock!
Deter - Detect - React

- Quick
- Deliberately
- Seriously

Deter - Detect - React

- Call the credit card company
  - Close Accounts
  - Security/Fraud Department
  - Follow-up in writing
  - Proper documentation
Deter - Detect - React

- File an Identity Theft Report
  - Identity Theft Affidavit
    - FTC
  - Police Report

Breaches

1 in 4 consumers are data breach victims
1 in 5 breach victims experience fraud
$901 mean fraud cost to consumers
Breaches

• Equifax – announced September 7, 2017
  ▪ 143 Million could be affected
  ▪ Breach potentially occurred between mid-May and July of this year. Discovered by Equifax on July 29 and announced September 7.
  ▪ Names, social security numbers, birth dates, addresses and the numbers of some driver’s licenses

Breaches

• Saks Fifth Ave/Lord & Taylor
  ▪ 5 million credit and debit cards stolen
  ▪ It continues to be investigated, but thoughts are it is the result of malware/phishing email campaign
Breaches

• Panera Bread
  ▪ Leak of millions of customer records including names, email addresses, physical address, birth dates and last four digits of credit cards
  ▪ Information was in plain text
  ▪ Records of customers that had signed up to order their food online

• Delta Air Lines/Sears Holdings/Best Buy
  ▪ Cyberattack hit third party service provider
  ▪ September 26, 2017 to October 12
  ▪ Used the third party provider to collect payment information
  ▪ Malware attack
  ▪ Very similar to the 2013 Target breach
  ▪ Be diligent when working with third party providers
Breaches

- Facebook
  - US FTC is investigating – 2011 settlement
  - Mark Zuckerberg, CEO, facing Congress this month
  - Up to 50 million (this number keeps increasing) users’ data was transferred to Cambridge Analytica
  - Originally collected from a Facebook app – “thisisyourdigitallife”
  - Ways to help protect your Facebook data
    - Delete it, Deactivate your account (like a freeze), minimize the apps you access within Facebook, using Facebook to login to other apps, sharing

Protect Yourself and Your Members

- According to CyberScout.com
  - Your identity is comprised of three types of information: financial, medical, and public documents/data. We refer to this trinity as your identity portfolio.

  - Identity is an asset—as valuable as cash in hand. And it’s easily compromised through theft or a data breach. You should give the same kind of care to your identity portfolio as you would an investment portfolio. Your identity should be nurtured, managed and properly protected.
Protect Yourself and Your Members

- According to CyberScout.com
  - Tips to protect credit and debit card
    1. Cut the cards
    2. Cancel unused accounts
    3. Watch for new cards
    4. Review your accounts and statement regularly
    5. Keep a list of accounts for record keeping
    6. Avoid using PIN based debit for purchases when traveling
    7. With unfamiliar merchants, use a credit card
    8. Run debit card purchases as credit

Protect Yourself and Your Members

- According to CyberScout.com
  - What to do when you get a data breach letter.......
    1. Read the notice carefully
    2. Review the potentially breached account
    3. Know exactly what is at risk
    4. If you are offered free credit monitoring, take it
    5. Pay extra attention to your account and billing statements
    6. Check your credit report
    7. Place a fraud alert on your credit file
Protect Yourself and Your Members

• According to CyberScout.com
  ▪ Social media
    1. Use strong passwords
    2. Be cautious when using public Wi-Fi
    3. Know exactly what is at risk
    4. Be wary of third party applications you are connecting to

What can your credit union do?

• Offer advice such as:
  ▪ Call the companies where you know the fraud occurred.
  ▪ Place a fraud alert and get your credit reports.
  ▪ Report identity theft to the FTC.
  ▪ File a report with your local police department.
What can your credit union do?

- Educate
- Fraud Related Systems
- Offer Identity Theft Protection

Identity Theft Protection options

- Whistleblower
  - Offer a third-party anonymous and confidential whistleblower reporting service
  - Gives staff the confidence to report what they are seeing
Whistleblower - internal fraud

- Examples of concerns and issues

- Embezzlement
- Bribery
- Falsifying contracts
- Accounting misrepresentation, theft
- Misuse of company property
- Ethics violations
- Discrimination
- Unfair labor practices

Fraud Management Services

- Services used to assist if you think or know your identity has been compromised
- Best if there is an assigned caseworker to help you through the process of “cleaning up” your identity
- Should include document replacement, educational resources and peace of mind
Fraud Management Services

- Proactive and reactive services
- Full-range of monitoring options
- A partner that is searching a variety of places/areas that your identity may appear without your knowledge

Fraud Management Services

- For the credit union:
  - A partner that will provide data breach protection and remediation services
  - Breach counseling, crisis management, notification guidance and general support

**Contact Sollievo to hear more about our trusted partner.**
Thank you!

Staci Wright, Senior Consultant, Fraud Services

swright@Sollievo.com
(855) 605-5664 ext 1204