Identity Fraud: Protecting Your Identity Between Work and Play
Ryan Sothan, Outreach Coordinator
Nebraska Department of Justice, Office of the Attorney General
Consumer Protection and Anti-Trust Division

What is Identity Theft?
- "Someone obtaining your personal identifying information without your knowledge in order to commit fraud or theft."
- Personal identifying information includes your:
  - Name
  - Date of Birth
  - Social Security Number
  - Driver's License Number
  - Bank Account and Credit Card Numbers
  - Other financial account information (including PINs and passwords)
On the Rise

- Identity Theft is the leading consumer complaint.
- Dollar amount stolen in 2016: $16 billion.
- Driven by 40% increase in Card-Not-Present Fraud.
- U.S. consumers impacted: 15.4 million.
- A new identity fraud victim every 2 seconds.
- Consumer information misused an average of 48 days.
- Amount stolen over the past six years: $128 billion.
  - $34,790 stolen per minute, or enough to pay for four years of college in just four minutes.

Javelin Strategy & Research, 2016 Identity Fraud Study, February 2017

How Victims Information is Misused
January 1 - December 31, 2015

- Credit Cards: 33
- Phone & Utilities: 13
- Bank Accounts: 12
- Employment or Tax-Related: 34
- Government Documents or Benefits: 7
- Loan or Lease: 7
- Other: 16

Federal Trade Commission, Released March 2017
Other includes: Miscellaneous, Uncertain, Internet/Email, Data Breach, Evading the Law, and eight other classifications below 1.0%

Get 5.99% guaranteed with no annual fee!
2016 and 2017 Verizon Data Breach Investigations Reports

Executive Summary

Data Breaches by Industry
January 1 - December 31, 2016

- Financial: 24
- Healthcare: 15
- Information: 6
- Other: 6
- Professional: 6
- Public: 12
- Retail/ Accommodation: 19

Other includes: Education, Manufacturing, Unknown, and a host of individual industries each accounting for less than 2% of all data breaches.
Verizon Data Breach Report: Findings

- “Cybercriminals are continuing to exploit human nature as they rely on familiar attack patterns such as phishing, and increase their reliance on ransomware where data is encrypted and a ransom is demanded.”
- “Most attacks exploit known vulnerabilities that have never been patched despite patches being available for months, or even years.”
- “The top 10 known vulnerabilities accounted for 85 percent of successful exploits.”
- “Eighty-one (81) percent of hacking-related data breaches leveraged using weak, stolen, or default passwords.”
- “Basic defenses continue to be sorely lacking in many organizations.”

2016 Data Breach Report: Findings

- “Our findings boil down to one common theme—the human element.”
- Despite advance in information security research and cyber detection solutions and tools, we continue to see many of the same errors we’ve known about for more than a decade now. How do you reconcile that?”

Bryan Sartin, Executive Director, Global Security Services
Verizon Enterprise Solutions
Prevention: 5 Key Principles

- **Take stock.**
  Know what personal information you have in your files and on your computers.

- **Scale down.**
  Keep only what you need for your organization.

- **Secure it.**
  Protect the information that you keep.

- **Pitch it.**
  Properly dispose of what you no longer need.

- **Plan ahead.**
  Create a plan to respond to security incidents.

[www.bulkorder.ftc.gov](http://www.bulkorder.ftc.gov)
Secure It:
Make Passwords Long and Strong

How many seconds would it take to break your password?

- 6 characters: .02 seconds
- 10 characters: 10.5 hours
- 6 characters plus symbol: 1.3 minutes
- 10 characters plus symbol: 54.5 years

Take the Password Test

How secure is your password?

Password: *********

1. Characters containing:
   - uppercase
   - lowercase
   - numbers
   - symbols

2._use()_lowercase()_upper_case()_numbers()_symbols()_39 centuries

Single Sign-On for Enterprise

Password Manager for Individuals

Get 5.99% guarantee with no annual fee!
How Do Thieves Steal an Identity?
- Steal wallets, purses, trash, even your mail
- Change your address at the Post Office
- Fraudulently obtain your credit report
- Unsecured Internet transactions
- Phishing
- Smishing
- Skimming
- Hacking

Who is the Thief?
The Identity Thief You Know
Identity theft victims who learn the thief’s identity most often say their personally identifying information was stolen by someone they know well—a relative, friend, neighbor or in-home worker.

Source: Javelin Strategy & Research
Phishing

- Also known as: Imposter Scam
- E-mail and frequent phone scam involving fraudsters posing as legitimate businesses.
- Use source authority and official looking e-mails to trick you into divulging your personal information.
- To protect yourself:
  - Treat all unsolicited requests for financial information and personal data as suspicious.
  - Independently contact business to find out if subject of e-mail or phone call is legitimate.
Phishing / Imposter Scam
Straight Talk from the IRS

NewEssentials
- Webpage
- Mobile App
- IRS Line
- Phone
- Email
- Twitter
- Facebook
- YouTube
- IRS.gov
- Alerts
- Scam

News
Scam Calls and Emails Using IRS as Bait
Forested

- Scammers using the IRS as a bait. They take different forms. The most recent scam involves phone calls that appear to be from the IRS, telling people they owe money and saying they will file a lien on their property if they do not pay.
- The IRS will never call you at home or send you an email saying you owe money. If you are unsure, call the IRS at 800-829-1040.
- The IRS will never ask you to pay with a credit card.
- The IRS will not ask for your credit card number over the phone.
- The IRS will never ask you to deposit money into your bank account.
- If you think you may have been a victim, call the IRS at 866-908-7857.

Underrated News:
IRS Now Using Private Debt Collectors

- IRS sending letters to taxpayers alerting them that their accounts are being turned over to private debt collectors.
- The private companies will then send letters to the taxpayers before calling.
- No one will hear from a private collection firm unless they have unpaid tax debts dating back several years and have already heard from the IRS multiple times about this debt.

- The collection firms are:
  - CBE Group (Cedar Falls, IA)
  - Conserve (Fairport, New York)
  - Performant (Pleasanton, CA)
  - Pioneer (Horseheads, New York)
Legitimate Change - But Watch Out for Imposter Scam Calls

Social Security Numbers to be Removed From all Medicare Cards Beginning April 2018

- The “Social Security Number Removal Initiative” (SSNRI).
- **Beginning April 2018**, Centers for Medicare & Medicaid Services (CMS) will start mailing out new Medicare cards to all 58 million beneficiaries.
- New Medicare Beneficiary Identifier (MBI) will replace the SSN-based Health Insurance Claim Number.
- New number will be eleven (11) alphanumeric characters long.
- Each person enrolled in Medicare will be assigned a new MBI and mailed a new Medicare card.
- **You do not need to verify or confirm your information** nor do you need to pay to receive your new card. Also, all contact will be by U.S. Mail ONLY.
- The MBI is confidential like the SSN and should be protected as Personally Identifiable Information.
- Transition period from April 1, 2018 and running through December 31, 2019. During this time, both the SSN-based claim number and new MBI number will be accepted.
Skimming

- You give your credit card to the waiter at a restaurant.
- Your server runs your charge card through as usual but also runs it through a “skimmer” which collects your credit card information.
- Server receives (on average) $50 per card in exchange for information collected.
Equifax Data Breach
Sensitive Personal Information Exposed for Majority of American Adults

- Breach lasted from mid-May through late July. Hackers accessed names, Social Security numbers, birth dates, addresses and driver’s license numbers.
- Hackers also stole credit card numbers for approximately 209,000 people and dispute documents with personal identifying information for approximately 182,000 people.
- Visit Equifax’s website, www.equifaxsecurity2017.com to find out if your information was exposed.
- Click on the “Am I Impacted?” tab and enter your last name and the last SIX digits of your Social Security number. The site will tell you if you’ve been affected.
- Other steps to take to help protect yourself:
  - Check your credit reports; look for recent inquiries you do not recognize as made by you;
  - Consider placing a Fraud Alert or, better, a Security Freeze on your files;
  - Monitor existing credit card and bank accounts closely for charges you don’t recognize;
  - Change or strengthen your passwords on all financial accounts e.g. bank accounts, credit and debit cards, e-commerce sites, brokerage accounts, etc.
Security Freeze

- Written directive prohibiting the release of your credit report and credit score without your express authorization.
- Must request in writing by certified mail. Do so with all 3 credit bureaus.
- $3 to freeze and/or temporarily thaw.
- ICW: Monitoring free credit report, equivalent of brand name identity theft protection.

*N.R.S. 8-2601 to 8-2615 Credit Report Protection Act. 8-2603. Security freeze; request*
For your free credit report, here's what the web site looks like at: AnnualCreditReport.com

Other Simple Steps to Secure Your Digital Home

- **Secure your Wi-Fi Network.**
  Change the factory-set default password and username. Your router should use the latest security protocol (WPA2-PSK).

- **Keep a Clean Machine.**
  Keep your security software, operating system, and web browser on all of your Internet–connected devices updated.

- **Share with Care.**
  Limit the amount of personal information you share online and use privacy settings to avoid sharing information widely. Wait to post pictures from trips and events.
Identity Theft

Identity theft occurs when someone fraudulently uses your personal information, such as your name, date of birth, social security number, or other identifying data, to gain access to financial or other personal information. Identity theft can cause severe financial damage, credit damage, and other personal harm.

Protecting Your Identity

It’s important to keep your personal information secure. Here are some tips to help prevent identity theft:

- Keep your personal data secure.
- Shred old bank statements carefully and safely.
- Protect your bank statements and other financial information.
- Check your credit report regularly.
- Use a secure method of payment when making transactions online.
- Use strong passwords and update them regularly.
- Be cautious of email scams and phishing attempts.
- Keep your identification and other important documents in a safe place.

Detecting Identity Theft

If you suspect you have been a victim of identity theft, take the following steps to protect yourself:

- Contact your bank or credit card company immediately.
- Report the fraud to the Federal Trade Commission (FTC) by filling out their online fraud report or calling 1-877-438-4338.
- Place a fraud alert on your credit reports.
- Report the fraud to the FTC by filling out their online fraud report or calling 1-877-438-4338.
- Contact your bank or credit card company immediately.
- Report the fraud to the Federal Trade Commission (FTC) by filling out their online fraud report or calling 1-877-438-4338.
- Place a fraud alert on your credit reports.

Security Freeze

A security freeze, also known as a credit freeze, prevents creditors from accessing your credit report to make a new account. This can help protect against identity theft. Here’s how to set up a security freeze:

- Contact one of the three major credit bureaus (Equifax, Experian, or TransUnion) and request a security freeze on your credit report.
- Provide your personal information, such as your name, address, and Social Security number, to the credit bureau.
- The credit bureau will mail you a security freeze kit.
- Follow the instructions in the security freeze kit to sign and return the forms.

Economics

For More Information, Contact

Nebraska Department of Justice
Doug Peterson, Attorney General
Consumer Protection Division
2115 State Capitol Building
Lincoln, NE 68509
Phone: (402) 471-2682
Fax: (402) 471-0006
Consumer Protection Hotline: (800) 727-6432
E-mail: ago.consumer@nebraska.gov
Web Site: ProtectTheGoodLife.Nebraska.gov