DAVIS & HODGDON ASSOCIATES
CPAs ▪ PLC

Innovative
Entrepreneurial
Experienced

Identity Theft: Protecting Your Information

What is identity theft? Identity theft occurs when a crook steals pieces of personal identifying information, which may include a name, address, date of birth, Social Security number, or mother's maiden name to gain access to a person's financial accounts. Armed with this information, an identity thief may open new credit or financial accounts, buy cars, apply for loans or Social Security benefits, rent an apartment, or set up utility and phone service - in someone else's name. Some suggestions that may protect your personal data and reduce your exposure to identity theft are highlighted in this newsletter.

Identity Theft by the Numbers

Someone is a victim of identity theft every two seconds. In 2016, over 15.4 million U.S. adults were victims of identity theft.[1] Also, 2016 saw 4.4 Billion records compromised by data breaches.[2] According to recent news articles, police agencies are now saying that the fastest growing segment of identity theft victims are children.[3] Identity thieves have stolen over $107 billion in the past 6 years and the costs in 2016 alone were nearly $16 billion.[1]

[1] *"2017 Identity Fraud: Protecting Vulnerable Populations," Javelin Strategy & Research, 2017*

[2] *"Source: https://www.riskbasedsecurity.com/2017/01/2016-reported-data-breaches-expose-over-4-billion-records/*

[3] *Source: http://www.iii.org/fact-statistic/identity-theft-and-cybercrime*

Your SSN

Your Social Security number (SSN) is the key to cloning your identity. Therefore:

- Do not carry your Social Security card in your wallet. Avoid carrying cards that display your SSN — notably health insurance cards, unless needed to receive care.
- Never give your SSN, credit card number, or other personal data by phone unless you have an existing relationship with the business or agency AND you initiated the call using a verified phone number. Always verify the other party's authenticity.
- Avoid including your SSN on job applications. Provide it only when absolutely necessary — for tax, employment, and student records, stock and property transactions, etc.
- If a government agency requests your SSN, look for an accompanying Privacy Act notice indicating whether a SSN is required, how it will be used, and what happens if you don't provide it.

Your Bank Accounts

Frequent monitoring of your bank accounts will help to detect and stop fraud. Research indicates that the risk and size of fraud loss for consumers who frequently monitor their accounts online is lower than those who don't monitor accounts regularly online. Most financial institutions use online banking to provide free 24/7 access to your accounts.

Use e-mail alerts in your online banking account to notify you of account activity, such as bill pay transactions, balance thresholds, transaction size, and account transfers (both within your bank and between institutions).

Monitor and reconcile your check activity by viewing check images online. Many financial institutions offering checking accounts provide you with the ability to view the check images online. Regularly viewing these check images helps stop check fraud.

Reduce Paper Transactions

- Use online bill pay and e-bills to remove confidential information from the mail and improve tracking of payments. Many financial institutions now offer free online bill pay.
- For all your financial accounts, enroll in online statements and choose to receive your monthly account statements online instead of receiving a monthly paper statement. Research indicates greater than 10% of identity theft is caused by stolen mail or trash.

Mail and Marketing Lists

- Use a secure locking mailbox or a P.O. Box.
- Never place outbound mail (at work or at home) in an open, unlocked mailbox. Never leave mail in your car. During long absences, have mail held at the post office or have a trusted neighbor pick it up.
- Investigate immediately if expected bills or statements from financial institutions do not arrive on time. Be especially vigilant January through April when tax documents are sent.
- Never simply discard "pre-approved" credit offers you receive in the mail. Always shred them.

33 Blair Park Rd.
Williston, VT 05495

49 North Main St.
Rutland, VT 05702

info@dh-cpa.com
www.dh-cpa.com

IDENTITY THEFT

• To keep pre-approved credit offers from being sent to you, remove your name permanently from the mail offer lists by visiting www.optoutprescreen.com. You can also opt out by calling 1-888-5OPT-OUT (1-888-567-8688), but only for a five-year period.
• Add your name to the National Do-Not-Call Registry at www.donotcall.gov . Add your name to name-deletion lists used by nationwide marketers at www.dmaconsumers.org/consumerassistance.html.

Trash and Shredding

• Shred anything that contains your name, address, or other sensitive data before discarding, using a crosscut shredder - including invoices, receipts, statements, personalized pitch letters and envelopes, catalogs, and pre-approved credit offers.
• Don't discard sensitive documents at work unless you're sure they'll be shredded properly.
• Take your trash out immediately before it is due to be collected.

Your Checks

• Never let merchants write your SSN on your checks. It's illegal in many states and it puts you at risk.
• Do not have your SSN, driver's license number, or home phone number printed on your checks. If you have a P.O. Box, use that instead of your home address.
• The next time you order checks, have only the initials of your first name, followed by your full last name printed on them. If someone takes your checkbook, they will not know if you sign your checks with just your initials or your first name, but your bank will know how you sign your checks.
• Put your work phone number on your checks instead of your home phone.
• Pick up new checks at the bank instead of having them mailed to your home address.
• Don't leave outbound envelopes containing payments in a home or office mailbox for pickup, in a car, or in any other place where they might be stolen. Checks can be altered and cashed, and provide the thief with your account information. Be sure to carry these with you until you can deposit them into a USPS mailbox or bring them directly inside the post office.

Credit, Debit, and ATM Cards

• If a new or reissued credit card that's being mailed to you does not arrive on time, contact the issuer immediately.
• Minimize the number of credit cards you use, and carry only one or two at a time. Cancel unused accounts to reduce your exposure. However, be aware that canceling credit cards may affect your credit score adversely.
• Review your credit card statements, bank statements, and phone bills (including mobile phones) carefully each month for unauthorized use.
• Sign new credit cards immediately - before someone else does.
• Keep a list or photocopies of credit cards, bank accounts, and investments in a secure place (not your wallet or purse). Include account numbers, expiration dates, and phone numbers for customer service and fraud departments, so you can contact them quickly.

Your Wallet or Purse

At work, always store your wallet or purse in a safe place. Avoid carrying the following items in your wallet/purse:

- Your Social Security card (or your dependents' cards)
- Your birth certificate
- Your passport
- Your military identification card (required of military personnel)
- A driver's license or insurance card with your SSN (or that of a family member)
- A list of your banking information (PINs, logins, passwords, or account numbers)
- Receipts with your full credit card number displayed
- Paychecks or pay stubs
- Deposit slips
- More than two credit or debit cards
- Any card that might store your SSN or other sensitive data on a magnetic stripe, such as a gas card, electronic hotel key, or employee ID.

Credit Reports and Credit Files

- Check your credit reports as frequently as possible, at least twice a year. Under the FACT Act, U.S. consumers are entitled to one free credit report each year from each of the three major credit bureaus. For details, visit www.annualcreditreport.com or call 877-322-8228.
- Enroll in credit monitoring to track changes to your credit file. Enroll in fraud monitoring (non-credit database monitoring) to be warned of attempts to alter or acquire your identity data.
- Check your Social Security statement each year for signs of fraud. The Social Security Administration mails this statement to adult SSN holders about three months before their birthday.

Shopping and Application Forms

- Never toss credit card receipts into a public trash container. Always take them with you and shred them at home. Carry receipts in your wallet, not in the bag, so you don't mistakenly throw them out.
- Never leave transaction receipts at ATM machines, on counters at financial institutions, or at gasoline pumps.
- When signing a credit card receipt, note whether your entire account number is displayed, or merely the last four digits. If the entire number shows, cross it out before leaving the signed receipt behind.
- When paying a bill with a credit or debit card, always keep the waiter, cashier, or bartender in view. Pocket-sized "skimming" devices can capture your credit card information for later use.
- When filling out applications for loans, credit, mobile phones, or other services, find out how the company stores and disposes of your data. If you aren't convinced that your information is safe, take your business elsewhere. Some auto dealerships, department stores, car rental agencies, and video stores treat customer applications carelessly.

Web Sites and E-mail

- Do not provide credit card numbers or personal information on any web site if you aren't sure the site is authentic. Choose companies with secure transactions and strong

privacy and security policies (the “lock” icon appears at the bottom of the screen).
- Never open spam and other e-mail from unknown sources — it may contain viruses or other programs that make your computer vulnerable to intrusion.

- Never click on a link in an e-mail claiming to come from a financial institution or business, and never provide personal or account data in response. The e-mail may be a fake sent by “phishing” scammers.
- When entering personal information online, even on well-known web sites, watch for signs that you’ve been redirected to a “cloned” replica site where your data can be captured without your knowledge (a fraud technique called “pharming”). Such signs include odd error messages, unexpected page design or content, or other strange site behavior.

Computers and Networks

- Install a firewall on your home computer to keep hackers out — especially if you connect to the Internet by DSL or cable modem. Install virus protection and keep it updated. Some viruses are designed to send sensitive data to identity thieves from your computer.
- Before disposing of a computer or hard drive, remove data using a strong “wipe” utility program. Do not rely on the “delete” function to remove files containing sensitive information.
- If possible, encrypt sensitive data that is sent or stored in digital form.
- Always store personal files and data securely in your home, especially if you have roommates, employ outside help, or have service work done in your home. (This applies to paper as well.)

Passwords and PINs

- Never use the last four digits of your SSN, your mother’s maiden name, your birth date, your middle name, your child’s name, your pet’s name, or anything else that’s easily discovered or guessed. If your financial institution uses the last four digits of your SSN as your default PIN, change it.
- Memorize all your passwords. Combine letters and numbers and change your passwords frequently. Don’t record them on anything you carry in a wallet or purse. Ask financial institutions to add extra security to your account by requiring an additional code or password.
- Password-protect computer files that contain sensitive personal or account data.
- Shield your hand at an ATM or when making long distance calls with a phone card. Shoulder surfers may be nearby with binoculars or cameras. Avoid giving personal data by phone in a public place.

Smartphones

Smartphone users are almost 33% more likely to be the victims of fraud.
- Set passwords on the home screen to prevent unauthorized access.
- Remember that others can hear your phone conversations; do not reveal important information in a public place.
- Do not save log-in information on online banking sites, email, or other places that may have critical information.
- Review apps before purchasing. Malicious apps can steal sensitive information.

Other Important Tips

- Beware of mail or telephone solicitations that offer prizes or awards—especially if the offer asks you for personal information or financial account numbers.
- When you are writing checks to pay on your credit card accounts, DO NOT put the complete account number on the “For” line. Instead, just put the last four numbers. The credit card company knows the rest of the number, and anyone who might be handling your check as it passes through all the check processing channels won’t have access to it.
- Photocopy the contents of your wallet or purse. Do both sides of each license, credit card, etc. You will know what you had in your wallet and all of the account numbers and phone numbers to call and cancel. Keep the photocopy in a safe place. You can also carry a photocopy of your passport when you travel.
- Federal law allows credit bureaus to sell your personal information for marketing purposes to banks and credit card companies. The same law requires most financial institutions to provide a privacy notice and a chance to opt out of having your information sold when you apply for an account or a loan and gives you the right to opt out in general. Make sure you do so. Go to http://www.ftc.gov/privacy/protect.shtm for more information, and call 888-5-OPT-OUT to opt out. This automated call takes only a few minutes. You will be asked for your name, address and Social Security number. You can opt out for two years or permanently.
- Caller ID is a useful option to have so that you know who is calling you.

If You Suspect You Are the Victim of Identity Theft

- Contact your financial institutions and request they flag your accounts. Instruct them to contact you immediately if there is unusual activity on your accounts.
- File your complaint online with the Federal Trade Commission, at https://www.ftccomplaintassistant.gov/ or call their Identity Theft Hotline at 877-IDTHEFT. The FTC has counselors to assist identity theft victims with resolving financial and other problems that can result from this crime.
- Record the names and phone numbers of people with whom you discussed your case and retain all original reports and supporting documents. Keeping accurate and complete records are a big step toward helping you resolve your problem.
- To report fraud, call or go to the following websites:

Equifax: 800-525-6285; http://www.equifax.com/
Experian: 888-397-3742; http://www.experian.com/
TransUnion: 800-680-7289; http://www.transunion.com/

Understanding Your Credit Score

Your credit score might be the most important number that you don’t understand.

Credit scores – the arcane calculations pored over by everyone from mortgage lenders to auto dealers to decide how much they’re willing to lend – are growing in importance as

their use spreads beyond traditional lenders to wireless-service providers, insurance companies, and even employers.

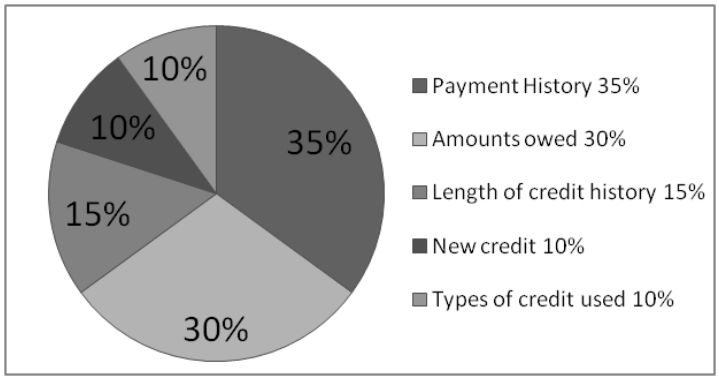
A person's score is basically a picture of one's credit-worthiness at a particular moment, based on a wide array of data. It includes information about loans and credit accounts, along with a tally of who has accessed the report, as well as a list of court documents and other matters, such as bankruptcies, liens or foreclosures.

As the use of credit scores proliferates, financial service companies are rolling out an assortment of products and services to try and help consumers track their credit score. For example, myFICO is a credit-score tracking service that sends emails or text-messages to customers whenever their FICO score (the standard credit score) fluctuates outside of a set range. (www.myfico.com)

The costs of having a bad credit score add up fast. Scores range from 300 to 850 with 700 or so marking the point below which it can be tougher to get the best price on a loan. For instance, on a $150,000 30-year mortgage, a person with a score of 639 would face annual payments nearly $2,000 higher than someone with a score of 760, according to Fair Isaac.

What's in Your Score

FICO Scores are calculated from different credit data in your credit report. This data is grouped into five categories as reviewed below. The percentages in the chart reflect how important each of the categories is in determining your score.



These percentages are based on the importance of the five categories for the general population. For particular groups - for example, people who have not been using credit long,- the importance of these categories may be somewhat different.

For consumers, this increases the importance of understanding the tricks for improving your score. The most important way to raise a credit score is a no-brainer: pay bills in full and on time. In fact, your history of making payments accounts for 35% of your overall FICO score. Missing payments or submitting the minimum due each month will lower scores. It is important to be vigilant on bill paying, because it can take a long time to recover from a missed or late payment.

The second biggest priority for anyone looking to improve their score is to maintain a low "credit utilization" level. This refers to the balance-to-limit ratio on credit accounts or the percentage of available credit being used for each card. The credit-utilization level falls under a complicated category referred to as "amounts owed," which comprises 30% of the FICO score. That means maxing out credit cards will send a score plummeting. In fact, simply using 50% or more of a limit can cause problems. For example, a consumer who has four credit cards with a $2,000 credit line on each, it isn't wise to carry a balance of more than $1,000 per card. In other words, it is better to carry smaller balances on several cards than to pile everything onto one card.

The third most important strategy, which makes up 15% of the score, is to build up a lengthy credit-using history. This means it's usually better not to close out all those old cards, as keeping them open adds to the credit record. Moreover, keeping otherwise dormant accounts active will help lower the balance-to-limit-ratio, as the limits are factored into the credit-utilization formula.

The final 20% of the score is divided equally between two categories: new accounts and diversification. Unlike keeping old accounts open, taking out new lines of credit raises red flags because it makes the consumer look riskier. Consumers get credit for having a variety of loans, so its better to have an assortment, including installment plans like auto loans or mortgages, than just simply credit cards. Creditors feel that consumers well versed in a variety of credit types post a lower risk.

As credit scores are based on information in credit reports, it's important to check reports to make sure they're accurate. Often credit reports can omit important information and sometimes they contain errors or accounts fraudulently opened by an identity thief. Be warned: Correcting errors requires patience, follow-through and lots of correspondence.

Conclusion:

As the information in your credit report changes, so does the importance of any factor in determining your score. What's important is the mix of information, which varies from person to person, and for any one person over time.