

Identity Theft and Fraud

What Every Graduating Senior Needs to Know about Protecting Your Identity

Mary McDougall **Marsha Yelick CFA (retired)**

Vail Public Library F**inancial Programs Consultant**

mmcdougall@vailgov.com **myelick@estesvalleylibrary.org**

970-479-2186 **970-586-8116 Ext 831**



**What is identity theft?**

 

Identity theft occurs when someone wrongfully acquires and uses your personal information. Personal information can include many things but is commonly:

* Your name
* Address
* Phone number
* Credit card numbers
* Driver’s license number
* Insurance card
* Paycheck stubs
* Social Security number
* Banking information (account numbers/ATM or debit card numbers/PIN)
* Passwords

18 million Americans or approximately 7% of the population over age 16 were victims of identity theft in 2014, according to the Bureau of Justice Statistics. This means 1 in every 14 people were victims; a new victim every 2 seconds. Identity theft resulted in the loss of $16 billion or about $3,000 per incident, with a median loss of $100 per victim.

**Why would someone want my identity?**



* To commit financial fraud
* To commit documentation fraud
* To sell your identity to someone else who wants to commit fraud

HOW VICTIMS' INFORMATION IS MISUSED, 2014 (1)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

| **Type of identity theft fraud** | **Percent** |
| --- | --- |
| Government documents or benefits fraud | 38.7% |
| Credit card fraud | 17.4 |
| Phone or utilities fraud | 12.5 |
| Bank fraud (2) | 8.2 |
| Attempted identity theft | 4.8 |
| Employment-related fraud | 4.8 |
| Loan fraud | 4.4 |
| Other identity theft | 21.8 |

 |

(1) Percentages are based on the total number of complaints in the Federal Trade Commission’s Consumer Sentinel Network (332,646 in 2014). Percentages total to more than 100 because some victims reported experiencing more than one type of identity theft.
(2) Includes fraud involving checking, savings and other deposit accounts and electronic fund transfers.

Source: Federal Trade Commission.

**Why me?**



* Identity thieves want personal information from others for varying reasons, and therefore everyone is a potential target - not just people with good credit and a lot of money.
* College students and recent high school graduates (that’s you!) are especially at risk….but why?
* For many, this is the first time that you have been on your own and responsible for managing your own lives and financial responsibilities
* You are busy and distracted
* You are inundated with a flurry of paperwork as you begin college or a job, and much of it will have personal information on it.
* SENIOR CITIZENS are also high risk for identity theft. They are often trusting of others. They may not check accounts as often as they should. They may keep on hand significant amounts of cash or other assets. They may keep quiet about any of the financial transactions.

**How do thieves get my information?**

Types of identity theft attacks include:

 

* Dumpster diving
* Phishing (email), vishing (calling), smishing (texting), spoofing (fake websites)
* Hacking
* Data breach –either from outside of an organization or an “inside job”
* Stealing a wallet or purse
* Stealing mail
* Internet – personal information taken from web sites
* Fraudulently obtaining your credit report
* Skimming
* Shoulder surfing

**How can I protect my identity?**

1. **Guard information online**
* Guard user names and passwords. Clear them, change them frequently, guard them, avoid using them on public computers, don’t share them with anyone, don’t write them down. Make them hard to guess – use combinations of letters, numbers and symbols; phrases from a favorite/book/movie. Get creative!
* Make strong passwords. Don’t use obvious words or series of numbers or letters; use characters; avoid words found in the dictionary; don’t use the same password for multiple accounts.
* Maintain anti-virus and anti-malware software.
* Don’t open links on unknown emails.
* Limit the personal and financial information that you store online. When possible, decline to save financial information and account numbers on websites.
* Be careful with unsecure Wi-Fi. Don’t do personal banking on public Wi-Fi.
* Lock your computers and phones.
* Don’t send account numbers or Social Security numbers by unsecure email. If you do not have secure email, ask the institution that you are sending the information to how to get it to them securely. Use a phone or fax if you have to.
1. **Don’t over share on social networking sites.** Be careful

about what and how much personal information you put out there. Don’t include your full birthdate, information that allows someone to know your mother’s maiden name, or info that could be used to answer other common security questions.

1. **Beware of the dorm room or shared apartment!** Although

you want to feel relaxed in your new home, dorm rooms are notoriously open to many people, some of whom may not necessarily be your true friends when it comes to looking out for your best interests.



1. **Keep personal documents in a secure place.** Or leave

them at home with parents if possible.

1. **Ignore credit card offers, and don’t sign up at a table or**

**booth on campus.** Don’t be tempted by the offer of free stuff! Go directly to the company’s secure website using your secure computer to apply.

1. **Guard your Social Security Number!!!!** Don’t carry your

SS card with you. Give it out only when absolutely necessary! There are legitimate situations in which you will be required to provide it, but if you are asked to give it, it is OK to question why it is needed before providing it.

1. **Ask your college or employer** **what they do to protect**

**the personal information that they have for you.** If they use SSNs as student or employee IDs, ask to have another identifying number assigned instead.

1. **Use credit cards to pay for online purchases instead of**

**debit cards.**  Credit cards provide better protection under the law for unauthorized usage.

1. **Beware of phishing scams that look like legitimate**

 **correspondence from your bank or other service provider.**

 Do not enter personal information unless you are certain that

 you are on the legitimate site. If in doubt, contact the

 institution directly in a different manner – you initiate the

 contact.

**10) Monitor your bank accounts and credit card statements.**

 Check them regularly and within the time frames allowed for

 disputing charges. Look for flags – unusual/large amounts,

 locations that are not near you, retailers or providers that are

 unfamiliar to you. Look also for small amounts at unfamiliar

 retailers or providers – these may be “test” charges run by the

 thief to see if the account is active, or to avoid detection for as

 long as possible.

**11) Monitor bills that you receive in the mail.** Don’t leave

them lying around. Pay attention to billing cycles and follow up

 if a bill does not arrive on time.

**12) Verify your mailing address with the post office and**

 **financial institutions.** Thieves may change your address with

 these institutions so that you are not receiving mail notices from

 them regarding unusual activity or late payments.

**13) Monitor your credit report.** You are entitled to a free credit

report every year from each of the three credit reporting

 agencies (Equifax, Experian, TransUnion). Use

 annualcreditreport.com to get a free one – beware of other

 providers who are not free or may be scams. Review the credit

 report for normal/abnormal tradelines and activity. Look for

 accounts or credit cards that you did not open. Learn how to

 read your credit report!

**14) Monitor your credit score.** Changes in it can indicate that

something new or something negative has been reported on

 your credit report . Your credit score (your Fair Isaac Corp

 score or FICO score) is a three-digit number between 300 and

 850 calculated from a formula that is designed to gauge your

 creditworthiness. Higher is better. It takes into account:

 payment history; amounts owed; years of credit; new credit;

 types of credit (mix of types of loans that you have).

**15) Shred sensitive documents.** Don’t fall prey to Dumpster

divers! Shred everything – even some junk mail can have your

 information in it that can be stolen. Shred pre-approved credit

 card offers. Only retain paper copies of information that you

 have to retain, such as tax records.

**16) Manage your mail.** Put outgoing mail in post office

collection boxes rather than unsecure mailboxes; pick up your

 mail regularly, especially if you receive it in an unsecure box;

 put a hold on your mail if you are going on vacation.

**17) Watch your wallet and purse.** Don’t leave them unattended

in public places, or lying around in a dorm or workplace. Minimize what you carry in them and carry only what is absolutely needed. Keep duplicate records of the contents of your wallet.

**18) Stay abreast of new information on scams and identity**

 **theft techniques in the news.** It is a crime that is continually

evolving with technology and trends.

**19) Keep receipts.** Although this may not help in prevention, it

may help in resolving a problem if your identity is stolen.

**20) Shield your hand when entering your PIN at an ATM or**

 **entering account numbers on a phone, keypad, etc.** Don’t

provide others with opportunity to see what you are doing.

**21) Don’t keep PINs with ATM/Debit cards!**



**How would I know if my identity has been stolen ?**

Some clues….

 

* Bank account statements reflect activity that you did not do.
* You are denied credit for reasons that don’t match your understanding of your financial position or creditworthiness.
* You start getting bills from companies that you do not recognize.
* You receive calls from collection agencies or creditors for an account that you do not recognize.
* You see unusual entries on your credit report.
* You receive notification from your bank that your online password or mailing address has been changed (and you didn’t change it).
* You stop getting mail from your bank that you normally receive.
* You receive calls from creditors saying you are approved or denied for credit that you haven’t applied for; or you get statements for credit cards that you do not have.

**What can happen if my identity is stolen?**

* Thieves can use your identity to:
	+ get a new driver’s license
	+ open bank or credit accounts
	+ apply for loans using your identity and credit history
	+ apply and get jobs in your name
	+ rent an apartment
	+ make retail purchases; get utilities in your name; get counterfeit checks or negotiate counterfeit checks in your name; use your name if they are arrested.
* You may have personal liability. For credit cards, regulations limit personal liability to $50 per card for unauthorized use; for ATM/debit cards, regulations limit personal liability to $50 if reported within 2 days, or $500 if reported within 60 days. For checks, put stop payments on checks to limit liability.
* Victims can spend months, years, and thousands of dollars trying to clean up their identity and credit. Fraudulent use of your identity can prevent or compromise your ability to get a job or get a loan or banking account. It’s a big deal!



**What should I do if my identity is stolen?**  

* Act immediately!
* Contact any affected entity or institution – bank, credit card company, government agency, or IRS in the case of SSN. Banks will close the affected accounts and set up new ones with new numbers for you.
* You may be asked or required to file a police report.
* Keep a record of all correspondence, phone calls including date, contact person, and any specific comments or actions to be taken.
* Contact one or more of the three consumer credit reporting agencies. The contacted company is required to contact the other two bureaus. Tell them that you are an identity theft victim and ask them to place a “fraud alert” on your file (will prevent thief from opening additional accounts using your personal information). You may want to consider a credit freeze (prevents anyone from accessing your credit report and prevents all credit approvals – even if you are the one applying).
* Get a copy of your credit report. You can request it when you call the consumer credit reporting agency.
* Continue to monitor your credit on an ongoing basis – once a thief has your identity, they have it forever.

CONGRATULATIONS ON YOUR

 GRADUATION!



**From the Staff at Vail Public Library and**

**Common Cents for Colorado**

