By Vickie Chavers-Bruso

Presented at CSC Fall Board Meeting

October 17, 2020

Identity Theft is a big problem.

Before 1935 when the Social Security Act passed peoples identity was determined on their name and face. Now we are faced with the internet technology and telecommunications In 2015 Colorado was 13 in reported cases..

**Types**

**Criminal** they get arrested using the other person’s information and get released on bail. When they do not show up a bench warrant is issued. The victim of identity theft is arrested.

**Medical identity theft**. Most victims are not aware of this until premiums go up or treatment is disallowed. Under current law, many victims do not have the right to review their medical records or correct errors. You have to watch if you go to purchase identity theft insurance some of them do not cover thus type of identity theft.

**Automobile insurance identity theft** is used by people with DUIs for example so they can have insurance.

Life insurance identity theft is when a person says they are the beneficiary produces a fake death certificate and gets paid the proceeds of the policy. The person finds this out by either seeing they are dead on their credit report or getting arrested for using credit cards of the deceased person.

**Child Identity Theft** after all they have a blank slate.

**Professional Identity Theft**

**Business Identity Theft**

**Financial Identity Theft** is the most common form.

**Other types** of Identity fraud are, identity cloning, synthetic identity theft (is where they obtain a person’s social security number and then fabricate personal information) government benefits fraud, government documents fraud, employment fraud, utility fraud bankruptcy fraud and tax return identity theft.

The ways they get your information are mail theft, stolen wallet or purse, phishing, (sending emails that appear to be legitimate) whaling( get a lot of information at one time ie Target) vishing(over the phone), pharming(a virus or malicious software is secretly loaded) , shoulder surfing, social media data mining, credit /debit card skimming, hacking, pretexting (convincing a victim that information is needed to complete a transaction or that someone is trying to access their account) dumpster diving, fraudulent recruiter scam( they receive an email with a link to a website that when it is loading downloads malicious software. Once on the site the victim is presented with an application to complete.) fraudulent employment scam, internet dating scams, internet auction and fake retail schemes, a foreign government letter, long lost relative, advance fee scams, charity frauds, lottery frauds, corporate prize scam, spoofing (email looks like it is from a legitimate source), skimming (like gas pumps or atm machines) cell phone cameras, cell phone cloning (within 3 feet if it is turned on), fake census workers, obituary surfing, free public Wi-Fi networks, malware, data breaches

**Detecting Identity theft**

Check your credit report. Look at the accounts listed. Correct? Excessive inquiries? Is your name correct? Address? Employers?

Unrecognized withdrawals from bank or brokerage accounts?

Missing Mail bills or account statements?

Receive unsolicited credit cards.

Getting calls from debt collectors for unknown debts.

Receiving surveys on items you have not purchased.

Receiving 1099’s or W-2’s for work you did not perform or prizes you did not receive

Receiving from your insurance company explanation of benefits you did not receive

Not able to access financial accounts online or notification of password changes you are unaware of

Credit applications denied for no apparent reason

**Steps to take to TRY to prevent identity theft for individuals**;

1. DO NOT give out personal information.
2. Something that is too good to be true IS TOO GOOD TO BE TRUE (MR. RIGHT, DEALS, JOBS NOT APPLIED FOR,UNREALISTIC INCOME STREAMS, ETC)
3. If they say you have to act now…RUN the other way.
4. Do not reply to emails even to tell them remove me from your list or click on links. of unknown sources .If your bank or anyone else wants you to contact them go to your bookmarked link or type in the website you are aware of.
5. Check out companies with the Better Business Bureau before contracting with them.
6. The IRS will never ask for personal information by email or phone .
7. Use a cross cut shredder to get rid of anything with personal information, financial information or credit card or loan applications sent in the mail.
8. Never provide your PIN number.
9. Do not carry your social security card.
10. Review any medical insurance documentation you receive regarding services.
11. Check your credit report every four months rotating
	1. Equifax [www.equifax.com](http://www.equifax.com) 1-800-525-6285
	2. TransUnion [www.transunion.com](http://www.transunion.com) 1-800-680-7289
	3. Experian [www.experian.com](http://www.experian.com) 1-888-397-33742
12. Install good antivirus software on your computer and phone and keep it up to date.
13. Install a firewall.
14. Do not use public WIFI
15. Password protect your cell phone.
16. Make sure before you give credit card information on the computer make sure the website address has https:// My computer antivirus shows a lock closed for good sites. “https” means it has a security certificate issued.
17. Guard your social security number
	1. Remove your social security number from your driver’s license
	2. Ask Why do you need my social security number?
	3. How do you protect my social security number?
	4. What will happen if I do not give it?
18. Use separate passwords for each application.
	1. Do not just use a word easy to remember or guess for a password
	2. Do not use a word with numbers at the end for a password.
	3. Never use names or birth dates or account numbers for a password.
	4. Change your passwords often
	5. The longer the password the better. 12 to 14 character.
19. Use 2 factor authentication for all online financial accounts.
20. Backup your system.

**Mitigate Damages**

1. Notify the bank and credit card companies.

2. If you have identity theft insurance notify them.

3. Contact a credit bureau and put a fraud alert on. You only have to contact one they will alert the others. Or you can use annualcreditreport.com

4.File a report with the Federal Trade Commission [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)

5.File a police report.

6. File From 14039 Identity Theft Affidavit with the IRS.

7. If the theft involved the internet file a complaint with Internet Crime Complaint Center at [www.ic3.gov/default.aspx](http://www.ic3.gov/default.aspx)

8. For mail theft report to US Postal Service local Postal inspector.

Maintain a log of everyone you speak with note the date and time on each entry.

Keep copies of all correspondence .