Identity Theft

Iowa Identity Theft Victim Assistance Coalition

Bill Brauch
Director

What is the Identity Theft Victim Assistance Coalition?

- The Coalition was formed in 2017.
- It was originally funded through a US Department of Justice grant obtained by the Iowa Organization for Victim Assistance ("IOVA")
- IOVA was formed in 1983 as a non-profit, 501(c)(3) organization to educate Iowans regarding victim rights issues. IOVA comprises victims of crime, witnesses, victim advocates, concerned citizens and related agencies and organizations.

More about the Coalition

The following agencies, organizations, schools, and entities are members of the Iowa Identity Theft Victim Assistance Coalition:

- The Iowa Attorney General's Consumer Protection Division
- The Iowa Insurance Division
- Children and Families of Iowa
- AARP Iowa
- The Iowa Department of Transportation
- Iowa Legal Aid

More about the Coalition

- The Iowa Attorney General's Crime Victim Assistance Division
- The Iowa Bankers Association
- The University of Northern Iowa
- Iowa Sheriffs' and Deputies' Association
- The Iowa County Attorneys' Association
- Iowa Credit Union Foundation
- ISU Extension and Outreach
- The Iowa Department of Veterans' Affairs

More about the Coalition

- The United States Attorney for the Northern District of Iowa
- Iowa Department of Corrections – Office of Victim and Restorative Justice Programs
- Iowa Office of the Chief Information Officer
- IOVA
- Polk County Attorney's Office
- Iowa State Bank
- Iowa US Postal Inspectors

More about the Coalition

The Coalition's mission is to help our members better serve their constituents, customers, clients, and students by sharing our resources, information, and ideas.

- www.IowaIDTheft.org
- Group e-mails
- Regular group calls
- "Identity Theft Update"
- Facebook page
- In-person meetings and trainings

What do Americans commonly think of when they hear someone is a victim of “Identity Theft”?

- A thief obtained personal information about someone else;
- They tricked the victim into divulging the information or hacked into a database or did something else to steal it;
- They did it for **personal gain**; and,
- Identity Theft is a crime (yes, it sure is!).

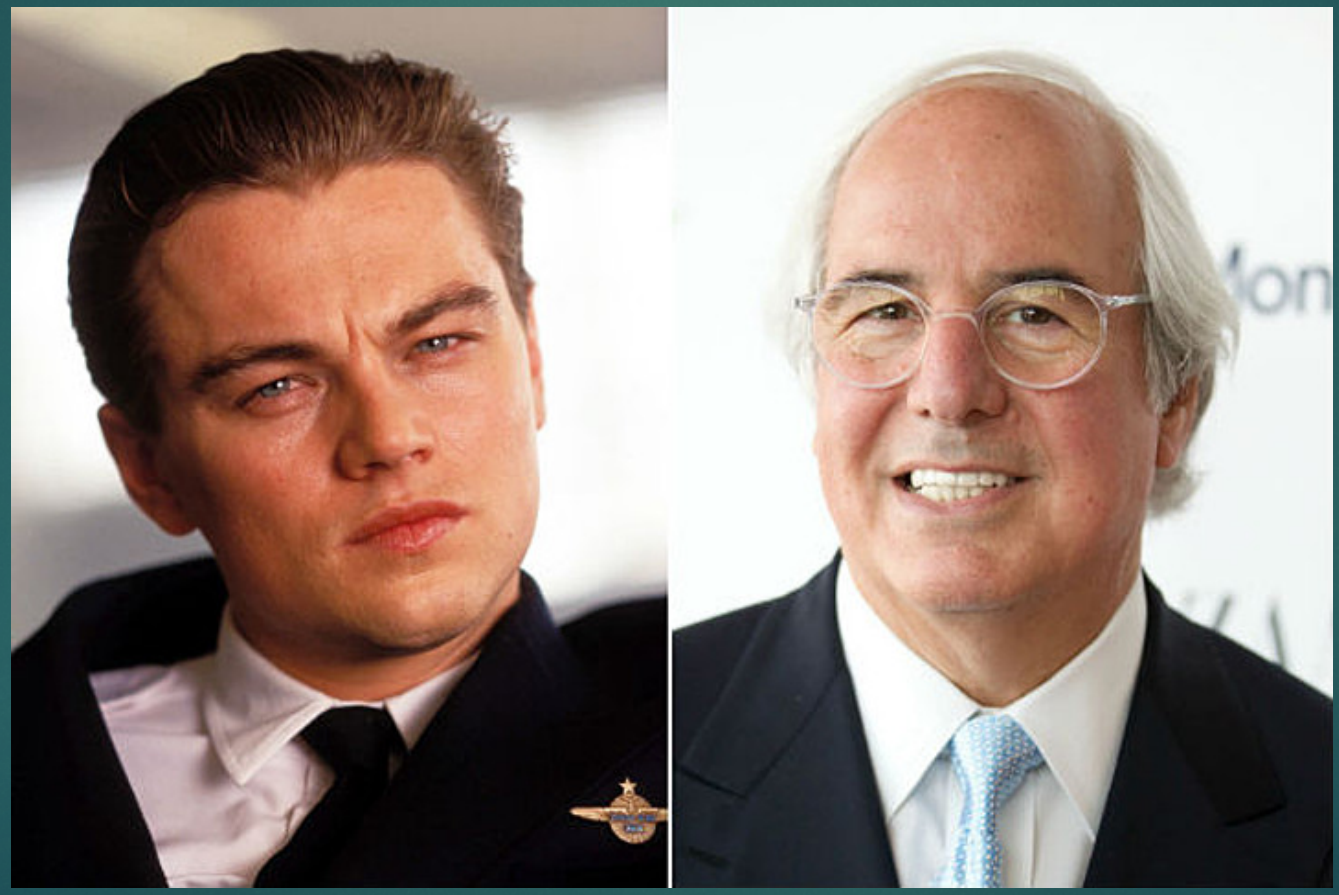
Did the Computer Age Spawn Identity Theft? (Not so much!)

- Abraham's son Isaac married Rebekah. Isaac and Rebakah had sons, Esau and Jacob.
- Isaac intended to give Esau his "blessing"-- inheritance.
- Jacob and Rebekah wanted different.
- Esau and Jacob looked the same, but Esau had substantially more body hair.
- Isaac was nearing death and Esau was travelling. Rebekah and Jacob stole some of Esau's clothes and placed goat fur carefully on his exposed skin and went to Isaac.
- Isaac was skeptical, but the son before him looked, smelled, and felt like Esau. Blessing granted.

Frank Abagnale

- Fraudulently cashed $2.5mn in checks over 50 years ago.
- Posed as a doctor, pilot, and lawyer (passed the LA bar and got a job at the LA AG's office at 19).
- Now he has a security consulting firm in DC and has been an FBI consultant on identity theft.

Frank Abagnale, Catch Me if You Can.



How does the law define Identity Theft?

- Iowa law defines Identity theft as follows:

  A person commits the crime of Identity Theft if the person fraudulently uses or attempts to fraudulently use identification information of another person, with the intent to obtain credit, property, services, or other benefit.

  Iowa Code Section 715A.8.

What is “identification information of another person” under IA law?

- Common pieces of information:
  - Name
  - Address
  - Phone number
  - Date of birth
  - Bank account numbers—checking, savings, demand deposit
  - Social Security number
  - Drivers license or non-operator ID card number
  - Credit card number

What is “identification information of another person?”

- But it also includes less commonly-considered information, including, but not limited to:
  - Student identification number
  - Military identification number
  - Alien identification or citizenship status number
  - Employer identification number
  - Signature
  - Electronic mail signature
  - Electronic identifier or screen name

What is “identification information of another person?”

- And we’re not done yet:
  - Biometric identifier
  - Genetic identification information
  - Access device
  - Logo, symbol, trademark
  - Place of employment and employee identification number
  - Parent’s legal surname prior to marriage

Who are today's ID Thieves?

- An acquaintance, friend or family member.
- Domestic rings
- International rings
- Amateur hackers
- Drug dealers
  - Because they don't want ownership in their names. Also, as an alternative to drug dealing.
- Data brokers
  - The "middle-men" of data breach information. ID thieves sell to them post-breach/hack. They then bundle the information and sell it online to other groups.

What might an ID thief do with someone's personal information?

- Obtain a loan or credit card
- Apply for a job
- Apply for a residential lease
- Rent a car
- Apply for insurance
- Apply for utility services
- Access financial accounts to steal money
- File for the victim's income tax refund
- Con another person – such as through a "romance scam"

What might an ID thief do with someone's personal information?

- Avoid arrest or greater penalties (due to their past record under their real or past purported names) by using some of the victim's identification information when arrested or detained
- Obtain government benefits
- Gain admittance to a college or university
- Obtain a driver license or a license to engage in a profession or specialty
- Obtain medical services
- Avoid detention due to immigration status

How do ID thieves get hold of someone's personal information?

- **THEFT:** A family member, friend, or burglar goes through a victim's purse, wallet, or your house or car looking for credit cards, Social Security Numbers, DL numbers, prescription data, etc.
- **HACKING**: Theft of personal data from government or companies via online hacking or theft of thumb-drives or physical hard drives. Either way, the thieves acquire sensitive info from databases.
- **PHISHING**: Using some sort of attractive lure to induce a victim into providing personal information "voluntarily." Think about the spam email you get, if you were to actually engage with it by, for example, opening an attachment that unleashes a "worm," that's phishing and you're the fish who's been hooked.

How do ID thieves get hold of someone's personal information?

- **SPOOFING**: related to phishing. These are disguised messages where victims share information because of the appearance of legitimacy. Phone numbers and websites are commonly "spoofed" to look legitimate or at the very least cover up the traceability of the origination of the call or email. They use the victim's 3-digit phone # prefix.
- **SHOULDER SURFING**: Simple, but it happens. Thieves—often in public areas—watch for people that are not as guarded with their personal info. Perhaps a person is making an online purchase while waiting at an airport or in a bank line, and the perpetrator sees it, captures the data, and goes on to use it.
- **SKIMMING**: Stealing personal information from another by capturing stored information on a data storage device created or obtained by the thief, e.g., gas pump skimmers.

How do ID thieves get hold of someone's personal information?

- **DUAL SWIPING**—ex. of this is where the restaurant server captures credit card info with a hand-held e-skimmer. Organized rings of merchant employees that have stolen millions doing this.
- **PEN AND PAPER**—Unsophisticated, but it happens. Hand over a card to a merchant's employee and they write down everything they need to know and use it online.
- **DUMPSTER DIVING**—just what it sounds like, but it can be a euphemism for searching your trash for documents related to credit offers or bank accounts.

How do ID thieves get hold of someone's personal information?

- Trickery via deceptive phone call or e-mails that result in a victim divulging his or her personal information.

Consequences for Victims

Substantial inconvenience and stress and, maybe, some expense.

- Having to report it.
- Having to contact creditors, financial institutions, credit card issuers.
- Having to freeze credit reports.
- Having to deal with debt collectors calling about debts that are in a victim's name but are not theirs.
- Having to deal with legal actions filed against them.

Consequences for Victims

- Having to take time off from work and from family and other activities to deal with it.
- Having to pay money to a lawyer if the victim is sued based on a bogus debt.
- Dealing with fear of further victimization and stress.
- Shame - maybe hiding it from family.

Consequences for Victims – Some Good News!

- A victim's financial liability for bogus credit card charges is limited by federal law – one of Americans' best friends, the Fair Credit Billing Act!
- Responsibility for unauthorized use cannot be more than $50. As a practical matter these days, it's $0. Card issuers write off the charges.
- If loss of card is reported before fraudulent use, $0 responsibility by law.

Consequences for Identity Thieves

- **Criminal Penalties – Iowa Code Section 715A.8**
- Class C Felony - If the value of the credit, property, services, or other benefit exceeds $10,000. (Penalties = No > 10 years imprisonment and a fine of from $1000 to $10,000.)
- Class D Felony – If said value exceeds $1000. (Penalties = No > 5 years imprisonment and a fine of from $750 to $7,500.)
- Aggravated Misdemeanor – If said value is $1000 or less. (Penalties = No > 2 years imprisonment and a fine of from $625 to $6,250.00)

Consequences for Identity Thieves

Private Right of Action For Identity Theft – Iowa Code Section 714.16B

- A person who suffers a pecuniary loss resulting from identity theft, or a financial institution on behalf of an account holder victim, may bring an action against the perpetrator to recover:
- Greater of $5000 or 3x actual damages; plus

Consequences for Identity Thieves

- Reasonable costs incurred due to the identity theft, including all of the following:
  - Costs for repairing the victim's credit history or credit rating;
  - Costs incurred for bringing a civil or administrative proceeding to satisfy a debt, lien, judgment, or other obligation of the victim; and,
  - Punitive damages, attorney fees, and court costs.

Iowa Laws Related to Identity Theft

Consumer Credit Security – Iowa Code Chapter 714G

Amended in the 2018 Legislative Session (SF2177). Requires a credit reporting company to freeze a consumer's credit report upon the consumer's request. There can be no fee for the credit freeze. The companies must also temporarily lift security freezes at no charge upon consumer request. Became effective July 1, 2018.

Certain aspects of the new amendments went into effect 1-1-19, such as mandating that the companies accept consumer requests made via means other than certified mail, including telephone, first class mail, and secure electronic methods.

Iowa Laws Related to Identity Theft

- Violations of Chapter 714G are violations of the Iowa Consumer Fraud Act, Iowa Code Section 714.16. The Consumer Fraud Act is enforced by the Attorney General.
- There is no private remedy for violations of chapter 714G.
- However, under chapter 714G, in an action by the Attorney General under section 714.16 for a violation of chapter 714G the Attorney General may seek to recover the greater of $500 or actual damages for each consumer affected by a violation. (unusual provision)

Iowa Laws Related to Identity Theft

Protected Security Freeze (Minors and others) – Iowa Code Section 714G.8A.

- Contained within chapter 714G, this section permits an adult to require credit reporting companies to create a credit report for the adult's minor child under 16 years of age and to freeze that credit report.
- Protected consumers under the law also include an incapacitated person and protected persons for whom a guardian or conservator has been appointed.

Iowa Laws Related to Identity Theft

Protected Security Freeze (Minors and others) – Iowa Code Section 714G.8A.

- The protected consumer may request that the freeze be lifted if he or she submits proof to the consumer credit agency that the previously submitted proof of authority to act on the consumer's behalf to seek imposition of the security freeze is no longer in effect.
- Consumer credit agencies may not charge for the placement or removal of a security freeze under this section.

Iowa Laws Related to Identity Theft

Iowa's Privacy Breach Statute – Iowa Code chapter 715C

Requires anyone possessing a consumer's "personal information" in connection with a business, vocation, occupation, or volunteer activity that was subject to a breach of security:

- Give notice to consumers whose personal info was breached.
- Follow certain notice requirements as to method and timing.
- There are certain exceptions, including for entities subject to and who comply with rules adopted under Title V of the Gramm-Leach-Bliley Act. (Privacy Notices & Safeguards.)
- AG can seek actual damages for a consumer (unusual).

Iowa Laws Related to Identity Theft

Unauthorized Computer Access – Iowa Code section 716.6B

1. A person who knowingly and without authorization accesses a computer, computer system, or computer network commits the following:

- a. An aggravated misdemeanor if computer data is accessed that contains a confidential record, as defined in section 22.7, a trade secret, or operational or support data of a:
  - public utility, as defined in section 476.1,
  - rural water district incorporated pursuant to chapter 357A or 504,
  - municipal utility organized under chapter 388 or 389, or
  - public airport.

Iowa Laws Related to Identity Theft

- b. A serious misdemeanor if computer data is copied, altered, or deleted.
- c. A simple misdemeanor for any access which is not an aggravated or serious misdemeanor.

2. The prosecuting attorney or an aggrieved person may institute civil proceedings against any person in district court seeking relief from conduct constituting a violation of this section or to prevent, restrain, or remedy such a violation.

Terminology is defined in Iowa Code section 702.1A

Iowa Laws Related to Identity Theft

Illegal Use of a Credit Card – Iowa Code section 715A.6.

- Includes not just theft, but reaches "unauthorized use."
- Violations are crimes – a class C felony if the value of the property secured or sought to be secured by using the card is > $10,000. Class D for over $1000 up to $10,000. Aggravated misdemeanor if $1000 or less.

Iowa Laws Related to Identity Theft

Illegal Use of Scanning Device or reencoder. Iowa Code Section 715A.10. A Class D Felony

- To use a scanning device to access, read, obtain, memorize, or store, temporarily or permanently, information encoded on a credit card without permission of the authorized user & with intent to defraud the authorized user.
- To use a reencoder to place info on the credit card without authorization & with intent to defraud the authorized user.

Iowa Laws Related to Identity Theft

- **Computer Spyware and Malware Protection – Iowa Code Chapter 715**
  - Makes it a crime for a person who is not an owner or operator of a computer to transmit computer software to such computer knowingly or with conscious avoidance of actual knowledge, and to use such software to engage in a variety of sharp practices in an attempt to take over, disable, or extract certain personal information from another person's computer.
  - Violations are aggravated misdemeanors, but the penalty increases to a class D felony if the violation results in pecuniary losses exceeding $1000 for a victim.

Federal Laws relating to Identity Theft

- Identity Theft and Assumption Deterrence Act prohibits "knowingly transfer[ring] or us[ing], without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law." 18 U.S.C. § 1028(a)(7).
- The mandatory minimum penalties is 2 years imprisonment. The US Sentencing Commission issued a report in 2018 on ID theft sentences: https://www.ussc.gov/research/research-reports/mandatory-minimum-penalties-federal-identity-theft-offenses

Federal Laws relating to Identity Theft

- Schemes to commit identity theft or fraud may also involve violations of other statutes such as credit card fraud (18 U.S.C. § 1029), computer fraud (18 U.S.C. § 1030), mail fraud (18 U.S.C. § 1341), wire fraud (18 U.S.C. § 1343), or financial institution fraud (18 U.S.C. § 1344).
- Each of these federal offenses are felonies that carry substantial penalties – in some cases, as high as 30 years' imprisonment, fines, and criminal forfeiture.

Federal Laws relating to Identity Theft

Fair Credit Reporting Act, 15 USC § 1681 *et. seq*.

- Provides a variety of rights to consumer victims, some of which are cited herein. It also imposes a variety of duties on creditors.

What You Can do for Victims

The Coalition's Victim Handout

- Highlights the immediate and near-term steps victims should take to deal with identity theft.
- Urges them to be organized and to retain good records.
- Provides victims specific referral information.

What You Can do for Victims

The handout tells victims to:

- Close or freeze accounts which were accessed.
- Call local law enforcement to report it and obtain a police report.
- Tell the investigating officer that the victim wishes to apply for an Iowa Identity Theft Passport. (Iowa Code section 715A.9A).

- Continued -

What You Can do for Victims

- **<u>The handout further advises victims to:</u>**

- **<u>Contact the three major credit bureaus</u>.** Victims should ask that a "***security freeze***" be placed on their credit reports and ask for their free credit report.
  - A security freeze will stop someone else getting new credit in the victim's name.
  - Security freezes are now free of charge.

- Continued -

Urge Victims to:

<u>Mail the below four items</u>

1. The FTC ID Theft Affidavit
2. The police report
3. Victim's Iowa Identity Theft Passport (if obtained)
4. A letter disputing the fraudulent charges

To the Following

1. **To all three major credit bureaus, and**
2. **To all creditors and collection agencies showing or collecting the fraudulent charges.**

Urge Victims to do all of the following in the dispute letter:

1. Identify the victim
2. State which accounts are disputed
3. State that the victim had nothing to do with the charges on the accounts
4. Request that the accounts be blocked from the victim's credit report
5. Go to Identitytheft.gov to find a sample letter.

Urge Victims to:

Notify all financial institutions they have an account with that they are a victim of identity theft:

- Use new passwords – not a victim's mother's maiden name or other personal information that may have been stolen – on any new accounts opened.
- Close outdated accounts, making sure to ask that old accounts be processed as "account closed at consumer's request," not "card lost or stolen." When the latter is reported to credit bureaus, it can be interpreted as blaming the victim for the loss.
- Carefully monitor mail and credit card bills and immediately report any new fraudulent activity to credit grantors.

Urge Victims of Tax ID Theft to:

- Call IRS Identity Protection Specialized Unit at 800-908-4490 ext. 245.
- Fill out Form 14039, the Identity Theft Affidavit.
- Follow other steps of what to do if the person is a victim of ID theft, generally.
- Be prepared to work with IRS through resolution, which can take a long time.

Protect Personal Information to Avoid Identity Theft

- Freeze credit reports!
  - Freezing credit reports makes it really tough for identity thieves to open accounts or get credit cards or loans in a person's name.
  - As of July 1, 2018, Iowans may freeze their credit reports for free with all credit reporting agencies. **DO IT**!
  - Iowans also may remove their credit freezes for free and reinstate their credit freezes for free.

Protect Personal Information to Avoid Identity Theft

- Do not ever divulge personal information to someone who calls or e-mails “out of the blue!”
- Use random passwords, different passwords for every account, and change them regularly.
- Check one credit report every four months for free – www.AnnualCreditReport.com, rotate between the 3 major credit reporting agencies. Each must provide a free report annually.

Protect Personal Information to Avoid Identity Theft

- Read all bills like a hawk! ID thieves like to test whether an account is active by charging very small dollar amounts.
- If a consumer doesn't recognize a charge, they should check with others in the home and then call and write their credit card issuer to challenge charges that they believe are not theirs.

Protect Personal Information to Avoid Identity Theft

- Fight "phishing" - don't take the bait.
  - Scam artists "phish" for victims by pretending to be banks, stores or government agencies. They do this over the phone, in e-mails and in the regular mail. Consumers should not respond to any request to verify an account number or password. Legitimate companies do not request this kind of information in this way.

Protect Information to Avoid Identity Theft

Never click on links in unsolicited e-mails, texts, Messenger messages, or Internet pop-ups

Protect Personal Information to Avoid Identity Theft

- Consumers should be discouraged from accessing financial accounts on public wifis. Checking a bank balance on a laptop, smartphone or tablet while connected to the coffee shop's wifi is a terrible decision!

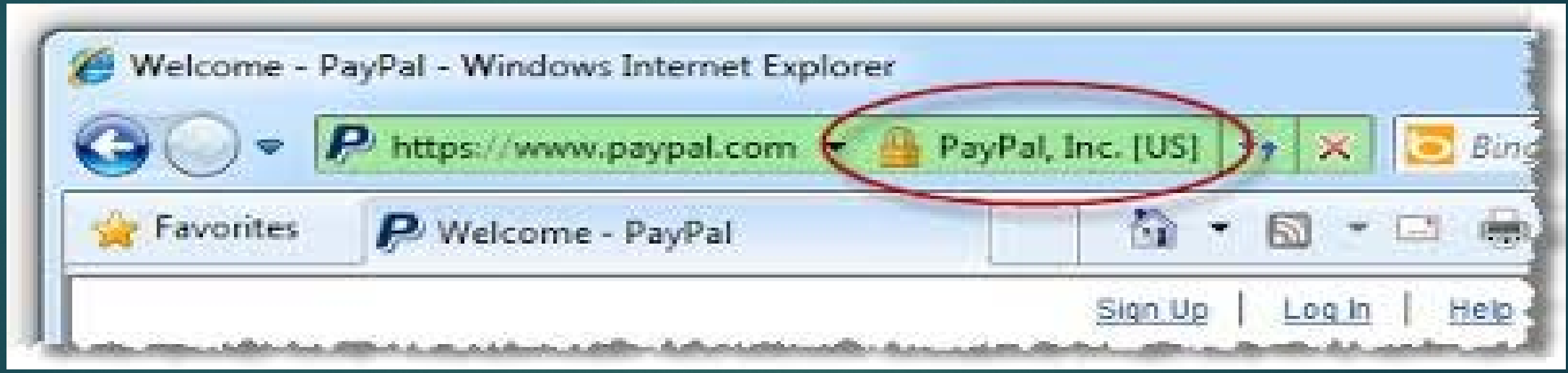
- Consumers should be careful what they post on Facebook and other social media. Posting photos while on vacation in Florida may constitute an invitation to burglarize.

Protect Personal Information to Avoid Identity Theft

- Users of Facebook and other social media need to check privacy settings to limit access to only folks who whey want to see their posts.
- Consumers should read notices they receive of privacy breaches and act on them. Free credit monitoring may help prevent loss of personal data.
- Never, ever enter personal financial data on a webpage, the address of which does not start “https”. An “http” page (without “s”) is not secure!

HTTPS? Padlock ?

- Hypertext Transfer Protocol Secure: Indication of authentication of the visited website and protection of the privacy and integrity of exchanged data.
- Padlock?



Protect Personal Information to Avoid Identity Theft

- Stop pre-approved credit offers.
  - Stop most pre-approved credit card offers. They make a tempting target for identity thieves who steal mail. Call toll-free 1-888-5OPTOUT (888-567-8688) to opt out of having a name included in credit bureau marketing lists.
- Ask questions.
  - Consumers should never be shy about asking how their personal information will be used before divulging it.

Protect Information to Avoid Identity Theft

- Shield computers and smartphone.
  - Protect personal information on computers and smartphones. Use strong passwords and change them regularly. Use firewall, virus and spyware protection software and update regularly.
  - Don’t install software without knowing what it is. Steer clear of randomly offered spyware. Download free software only from trusted sites.

Era of the ‘Security Breach’

- Equifax breach
  - 145.5 million Americans likely affected
  - Holy Grail of personal identifying information
- Target breach
  - Forty million credit and debit accounts implicated.
  - 70mn people had emails, phones and names stolen.

Era of the ‘Security Breach’

- Almost overnight, security breaches became normal. In 2017, 1,632 security breaches. In 2018, 1,244 security breaches. (ITRC)
- But, 2017 breaches exposed nearly 198 million records while 2018 breaches exposed over 446 million records!
- Anyone participating in the modern marketplace is vulnerable. (100s of orgs could have personal information about a person…e.g., businesses, health care, public institutions).

More on Passwords! They're a powerful avoidance...if created correctly.

- In 2013, a hacker stole and posted User Names and PWs from Adobe.com. Here's the most common Adobe PWs from that hack:
- 123456---~2 million
- 123456789---~500,000
- Password---~350,000
- 111111
- 123123
- Adobe123---~210k
- Abc123
- Adobe1

Tips to avoid Tax ID Theft

- Avoid carrying certain identifying documents like SS car or paperwork that has SSN.
- Only share SSN when absolutely required.
- Check credit report once a year.
- Protect personal computers with antivirus software, security patches and firewalls. Change PW regularly.
- Don't ever give personal info over the phone unless it is a known and trusted callder. The IRS never initiates contact with a phone call to a taxpayer.
- If you can, file early.

Tips for victims of Tax ID Theft

- Call IRS Identity Protection Specialized Unit at 800-908-4490 ext. 245.
- Fill out Form 14039, the Identity Theft Affidavit.
- Work with IRS through resolution, which can take months.
- Follow steps recommended for all ID theft victims.

Protect Personal Information to Avoid Identity Theft

- For more information:
  - The Iowa Attorney General's "How to Avoid Identity Theft" – "How to Avoid Identity Theft"
  - The Federal Trade Commission's tips on "protecting your identity" - https://www.consumer.ftc.gov/topics/identity-theft

Contacting Bill

- Call: 515-314-9591
- E-mail: Bill@IowaIDTheft.org

Website: www.IowaIDTheft.org

Caveat: This presentation is not legal advice. Contact your attorney for legal advice.