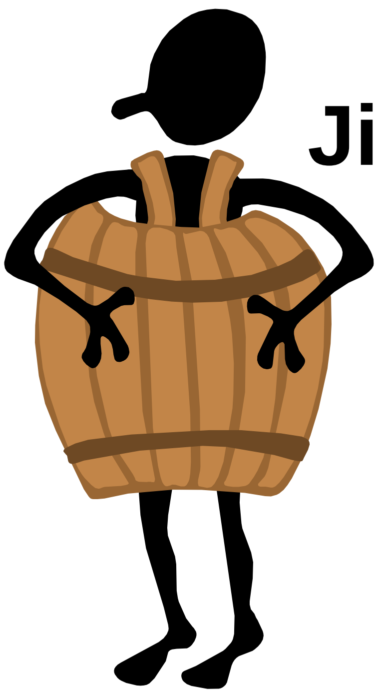
FRAUD & IDENTITY THEFT
"IDT"

TCOSCPA

Jim Small, CPA, MBA, CGMA

November 10, 2021



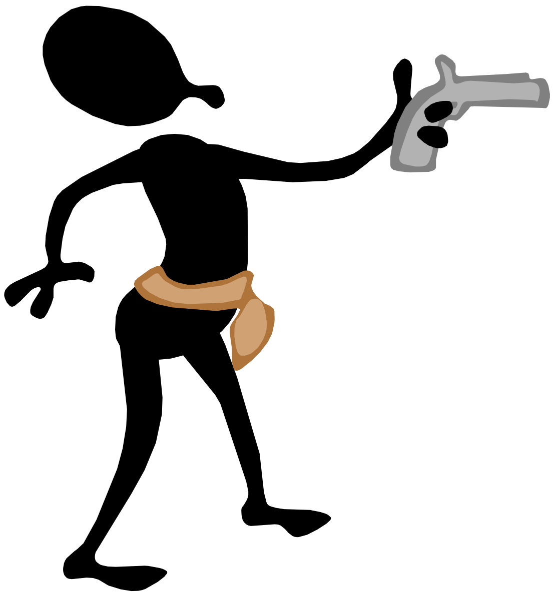
WHAT WE WILL LEARN

- Define identity theft – (“**IDT**”)
- Discuss why you should worry about it
- Examine how identity theft occurs
- Look at how identity theft has emerged
- Discuss what is being done about identity theft
- Look at ways to protect yourself
- Implications for CPAs and their clients

WHAT IS ID THEFT?

<u>Identity theft ("IDT")</u> is a crime of stealing key pieces of someone's identifying information, e.g.:

- Name,
- Address,
- Social Security number,
- Birth date, and
- Mother's maiden name
- Account PIN numbers and passwords



FOUR KEY IDT POINTS

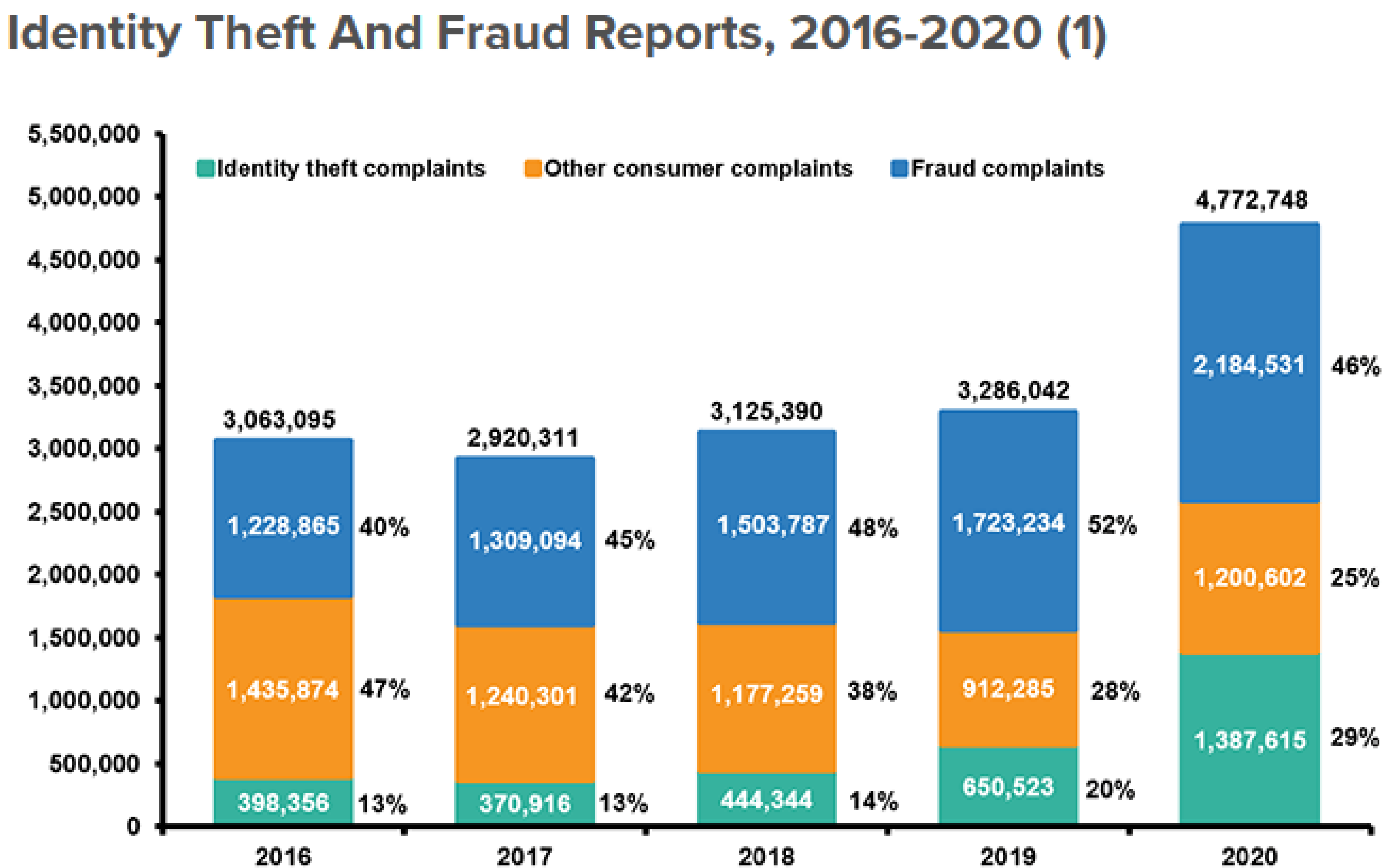
- People are <u>not</u> helpless in protecting themselves from identity theft.
- Consumers generally do <u>not</u> bear the brunt of the loss with credit cards.
- Internet use does <u>not</u> increase risk of identity fraud <u>if you are careful</u>.
- Seniors are <u>not</u> the most frequent targets of identity thieves.

Source: Javelin Strategy and Research 2006 Identity Fraud Survey Report

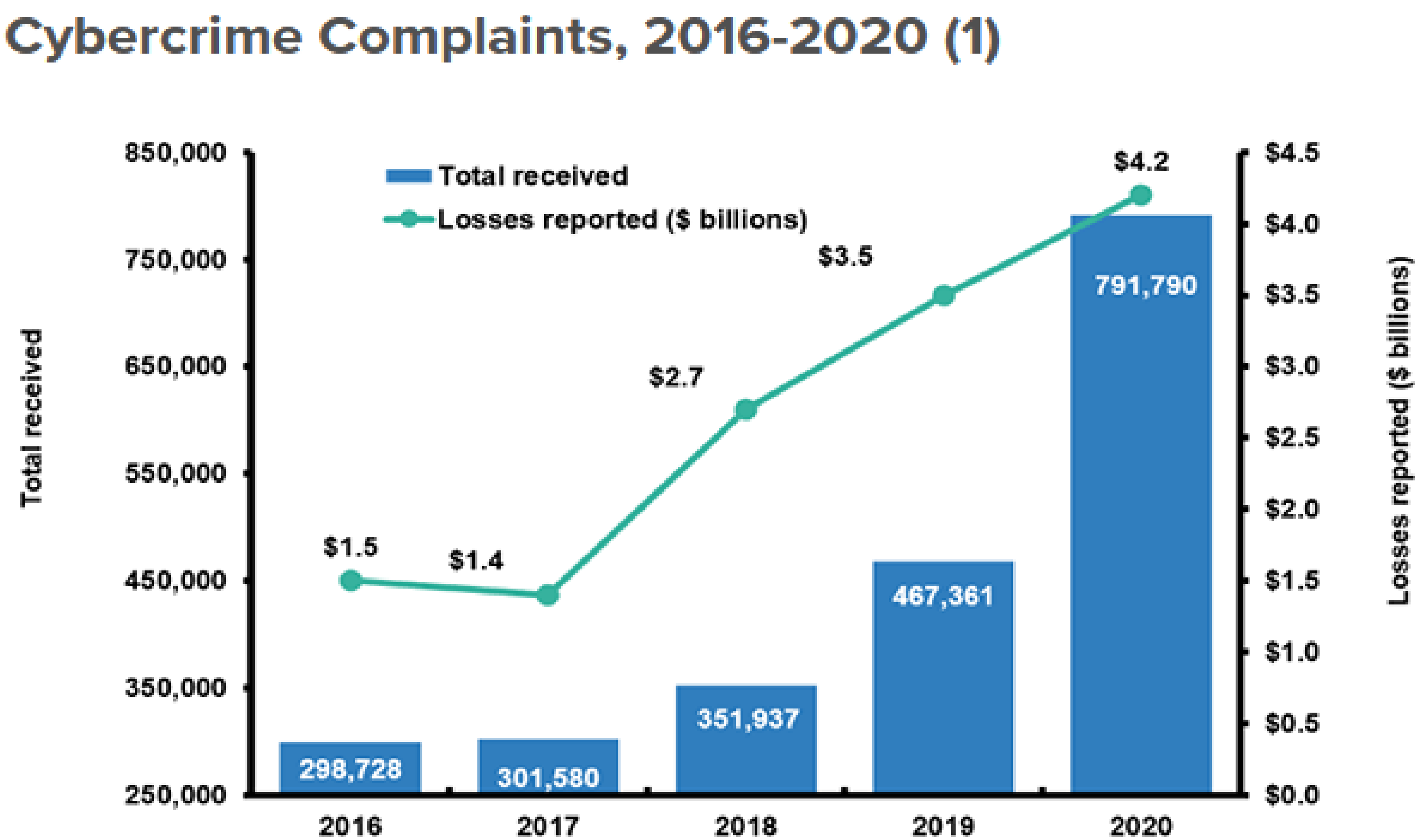
KEY STATISTICS

- Fastest growing crime in America (300% per year) estimated 80% goes unreported
- Perceived: low risk & high profit
- Further facilitates other crimes
- Increasing gang involvement
- Identity theft is of greater concern to adults with older children at home (45%) than those with younger children at home (27%).

KEY STATISTICS – FTC



CYBERCRIMES



(1) Based on complaints submitted to the Internet Crime Complaint Center.

TYPES OF IDT

Top Five Types of Identity Theft, 2020 (1)

Type of identity theft	Number of reports	Percent of total top five
Government benefits applied for/received	394,324	32.0%
Credit card fraud—new accounts	365,597	29.7
Miscellaneous identity theft (2)	281,434	22.9
Business/personal loan	99,667	8.1
Tax fraud	89,391	7.3
Total, top five	**1,230,413**	**100.0%**

SCAM TACTICS and TRIGGERS

HOW IDT OCCURS

- They steal wallets, purses, cell phones
- They scan & clone data on credit cards
- They steal your mail or divert your mail to another location
- They rummage through your trash, or the trash of businesses, for personal data in a practice known as “dumpster diving.”
- They fraudulently obtain your credit report

BEC – BUSINESS EMAIL COMPROMISE

- Scam targeting businesses who conduct wire transfers with suppliers abroad
- Impersonate CEO or other executive requesting a money transfer
- Bogus Invoice Scheme
- Attorney impersonation
- Data theft for future attacks from HR or accounting staff

PHISHING

Email phishing can be difficult to distinguish from legitimate emails. In this example, notice:

1. **Non-Wells Fargo email address:** The email address of the sender does not include the wellsfargo.com domain name, but instead uses "wells-fargo.info".
2. **Urgent call to action:** The email conveys urgency by saying, "you need to update your account today for security purposes" to convince you to take action.
3. **Suspicious URL:** The email contains a link that appears to be legitimate, but leads to a fraudulent website. You should preview a URL before clicking on it. If you're using a computer, hover over the link with your mouse, and the URL will show in the bottom left of your browser window. On an iPhone®, you can tap and hold the link and the URL will appear in a pop-up box. **Beware:** URLs beginning with "https" can also be used for phishing.

----- Forwarded Message -----
From: Wells Fargo Online <OnlineSupport@wells-fargo.info> 1
Sent: Tuesday, April 6, 2021, 02:47:38 PM MDT
Subject: Please Review: Your Wells Fargo contact information

WELLS FARGO

Dear Customer,

You need to update your account today, for security purposes. 2

We're providing this notification for your account security, and additional action is required.

https://5x.to.mk/skfzpl
Ctrl+Click to follow link 3

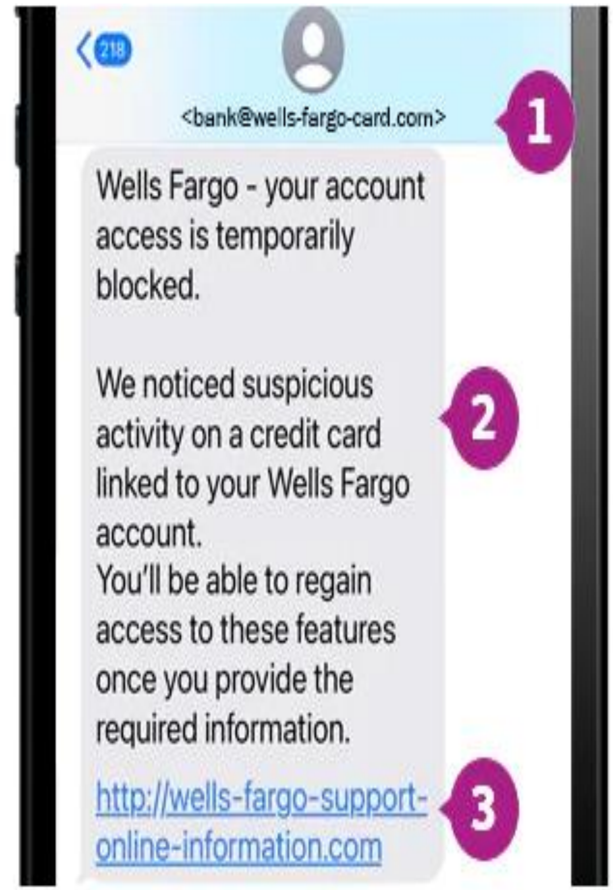
Keep in mind: please log on to wellsfargo.com.

Thank you for helping us serve you better.
Sincerely,
wellsfargo.com | Wells-Fargo Information Center.
Please do not reply to this automated email. To ensure a prompt response, send a secure email from your account.

SMISHING

Text phishing or "smishing" uses similar techniques as email phishing. In this example, notice:

1. **Suspicious sender:** The text was sent from an unknown phone number, instead of one of Wells Fargo's official short codes: 935-57, 937-33, 937-29, or 937-67.
2. **Unexpected request and unusual formatting:** The message includes an unexpected request to provide "required information" in order to regain access to your credit card.
3. **Suspicious URL or phone number:** The text message contains a link to a non-Wells Fargo URL, which could be a fraudulent website. Always preview a URL before clicking on it. On a mobile phone, press and hold the link and the URL will appear in a pop-up box. Phishing texts may also include a fraudulent phone number. Do not call the number in a suspicious text. Call the number on the back of your card or the website to verify the request.



WARNING SIGNS OF IDT

- Billing statements or collection calls for credit cards you never applied for
- Your credit card bill doesn't come at all
- Your billing statement includes charges you didn’t make
- Your credit card is unexpectedly declined for being over the limit or you are unexpectedly denied for a credit card or loan

IDT LAWS

- The Identity Theft and Assumption Deterrence Act, enacted by Congress in <u>October 1998</u> is the federal law making identity theft a crime.
- Violations of the Act may be investigated by the U.S. Secret Service, the FBI, the U.S. Postal Inspection Service, and SSA's office of the Inspector General. Federal identity theft cases are prosecuted by the U.S. Department of Justice.

WHAT THEY DO WITH ID

- Open credit card accounts in your name, using a false address.
- Establish phone or wireless service in your name.
- Open bank accounts and write bad checks in your name.
- Take out loans in your name.
- File medical claims in your name

A LITTLE QUIZ

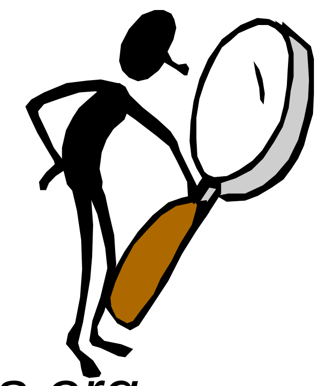
- I receive several offers of pre-approved credit every week (5)
- If you do <u>not</u> shred the offers (5)
- I carry my Social Security card in my wallet (10)
- My driver's license has my SSN on it (10)
- I do <u>not</u> have a PO Box or locked, secured mailbox (5)
- I use an unlocked, open box at work or at home to drop off my outgoing mail (10)
- Don't reconcile your bank and CC statements (5)

A LITTLE QUIZ

- I carry my military ID in my wallet at all times (10)
- I provide my SSN whenever asked, without asking questions as to how that information will be safeguarded (10)
- I have not ordered a copy of my credit report for at least 2 years (20)
- I do not believe that people would root around in my trash looking for credit or financial information or looking for documents containing my SSN (10)

QUIZ RESULTS

- **100+** - You are at a high risk – look out!
- **50 - 100** – Your odds of being victimized are about average but higher if you have good credit they can use
- **0 - 50** – You are in good shape. Don't let your guard down!



Privacy Rights Clearinghouse, www.privacyrights.org

PASSWORDS

- EU study of “office workers”
  - 16% used their name as password
  - 11% used favorite football team
  - 12% used the word “password”
- Never use a word that could be in any dictionary, names of places, or any proper nouns even spelled backwards
- Never use any of the above simply followed by a digit - Include upper and lower case, numbers, special characters

OTHER PC MEASURES

- Promptly apply system and product **patches**
- Run **anti-virus software** configured to update daily, and perform a full scan at least weekly
- Use a **firewall** (either software or hardware) and configure for the most restrictive setting that still allows you to do required work
- Select good, strong **passwords** and use different one on each site
- **Think** BEFORE you click or just don't click

WHERE VICTIMS SEEK HELP

- FTC – 3%
- Other Federal Agency – 5%
- State Dept of Motor Vehicle Admin – 7%
- State AG or State Consumer Agency – 8%
- Lawyer – 12%
- Credit Bureau – 22%
- Local Police – 26%
- Credit Grantor – 43%
- Did Not Contact Anyone – 38%

IF YOU ARE A VICTIM

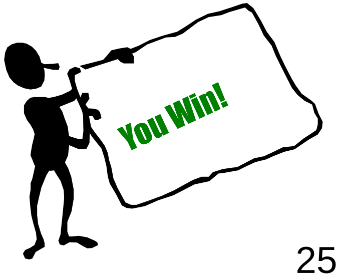
- If you are a victim, file a Police report with LOCAL Police or Police where identity theft occurred, if known
  – Get a copy and retain for your records
  – Get information on the assigned investigation and keep phone numbers available for verification
- Complete a free ID Theft Affidavit from the FTC
  – **www.ftc.gov/idtheft**

IF YOU ARE A VICTIM

- Contact ALL Creditors
  - Contact billing inquires and security department
  - Change passwords
  - Close unused or unnecessary accounts
  - Monitor activity closely
- Add a fraud alert to your credit report
  - Initial alert—90 days
  - Extended alert—7 years

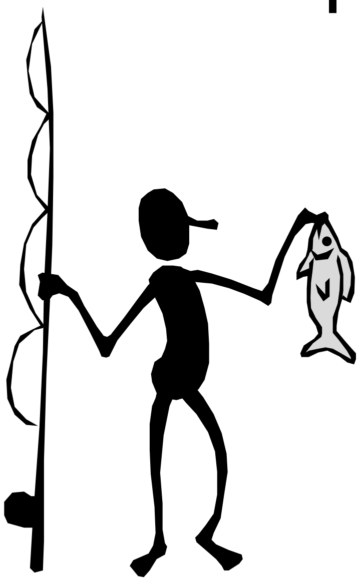
RED FLAGS of a PHISHING SCAM

- E-mails that direct users to a Web site to “validate” or “update” info
- E-mails warning accounts will be closed
- Grammatical errors and typos
- References to 9-11, the Patriot Act, etc.
- Return addresses at yahoo.com, juno.com
- Words Like “Urgent” and “Important”



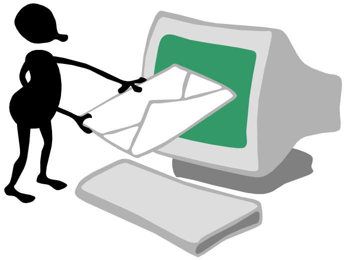
PHISHING SCAMS

- Wells Fargo, Chase and other major banks have examples of fraudulent emails on their websites
- Nigerian money transfer scams are quite common



OTHER INTERNET ISSUES

- Never send credit card data in an email - always be considered unsecured
- Don’t open email attachments without understanding that these are the largest cause of infections - your friend could have been infected and had their address book stolen
- Email is one of the largest sources of viruses, trojans and spyware
- Never open an eCard – spyware?



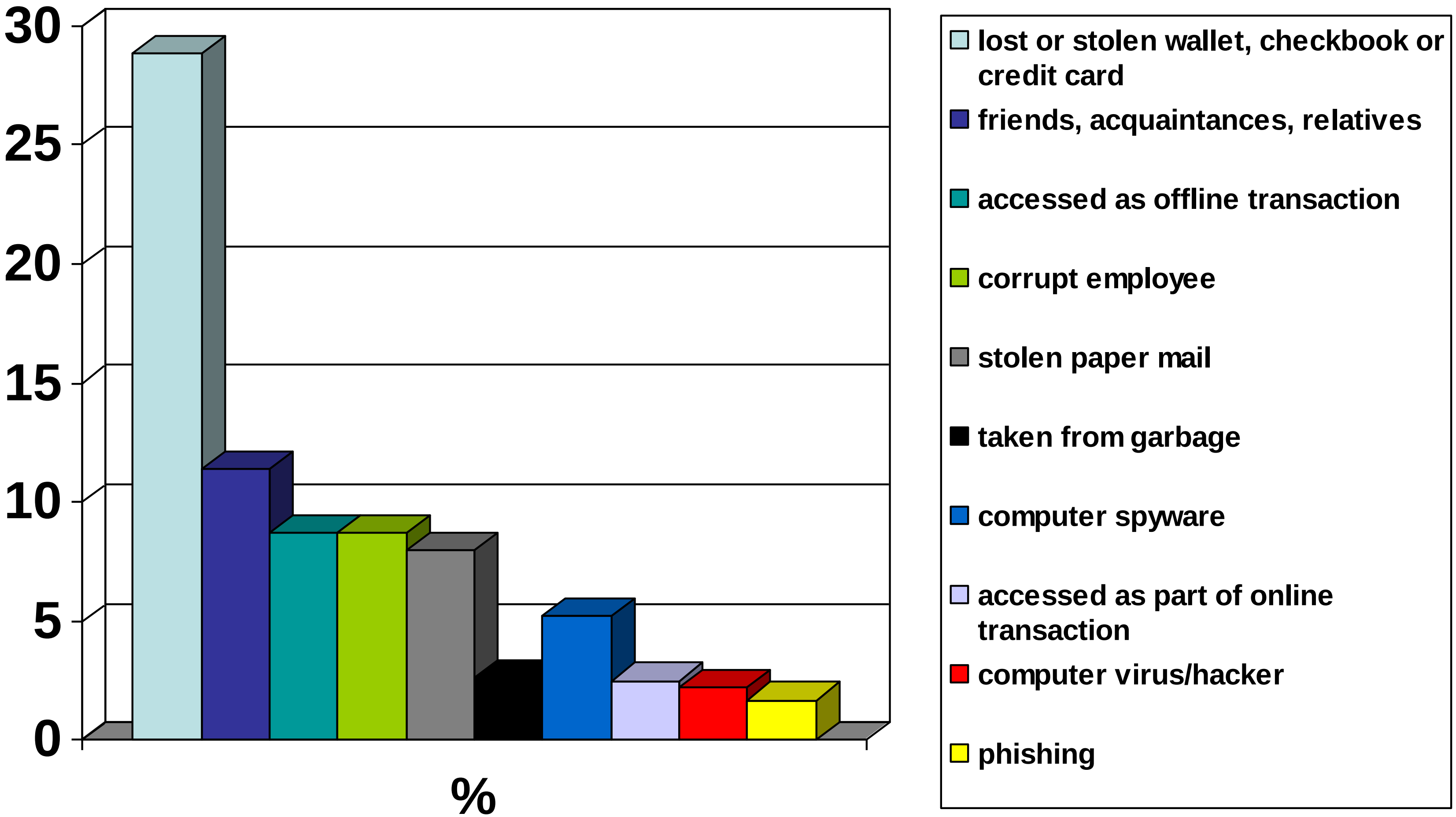
OTHER INTERNET ISSUES

- “Social Networks” like Plaxo, Friendster, Tickle and others help you remember addresses and phone numbers
- You risk your personal information, privacy and the information contained in your own computer’s address book the services will expose your information and possibly the information stored on your computer to misuse and theft
- Be careful of HTML email - it can contain web bugs

EMAIL ATTACHMENTS

- **Can you spot a safe attachment?**
  - USUALLY DEADLY - .ade, .adp, .bas, .bat, .chm, .cmd, .com, .cpl, .crt, .exe, .hlp, .hta, .inf, .ins, .isp, .js, .jse, .lnk, .mdb, .mde, .msc, .msi, .msp, .mst, .pcd, .pif, .reg, .scr, .sct, .shb, .shs, .url, .vb, .vbe, .vbs, .wsc, .wsf, .wsh, .app, .fxp, .prg, .mdw, .mdt, .ops, .ksh, .csh, .ceo, .cnf, .htm, .html, .mad, .maf, .mag, .mam, .maq, .mar, .mas, .mat, .mav, .maw, .mht, .mhtml, .scf, .uls, .xnk
  - COULD BE DEADLY - .doc, .pdf, .zip
  - USUALLY SAFE - .bmp, .jpg, .tif
  - **One of the latest cyber crime techniques is the use of videos to install malware (malicious software) and/or Trojans just by watching the video**

On-line vs. Off-line IDT



FOUR TYPES OF LAWS

- 1) **Retributive** - Detailing of crime, punishments, etc.
- 2) **Reconstructive** - Helping victims reconstruct files, setting things right
- 3) **Integrative** - Rallying government institutions to aid
- 4) **Functional** - Adopting measures to help detect and prevent identity theft

Consequence of Identity Theft

- **Identity thief seldom pays bills for debts incurred under victim name.**
- **Due to bad credit report, victim may be denied new credit, loans, mortgages, utility service, or employment.**
- **Where identity thief established criminal record in victim name, victim may fail background checks for employment, firearms, etc., or may even end up in jail.**

FAST DETECTION = LOWER $

47% of cases are detected by the victims first.

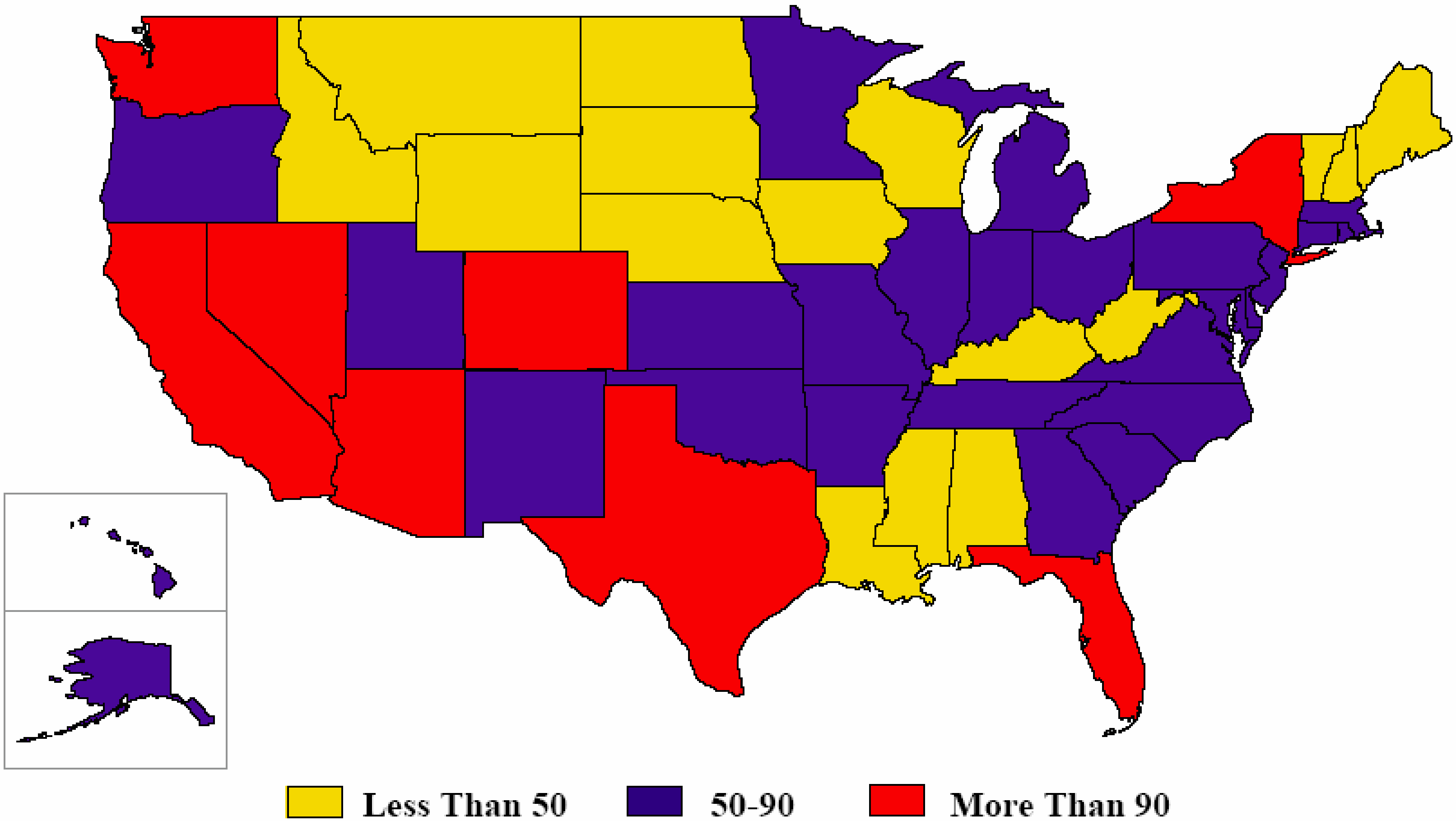
- 35% shorter detection times and 36% ($347) lower consumer costs
- reviewing credit reports or using a credit monitoring service ($264)

17% of cases are not detected at all until a creditor contacts the victim or until the victim applies for credit and is denied.

- 241 days to be discovered – cost consumer $1,391.

Figure 4b
Identity Theft Victims by State (Per 100,000 Population)[1]

January 1 – December 31, 2004

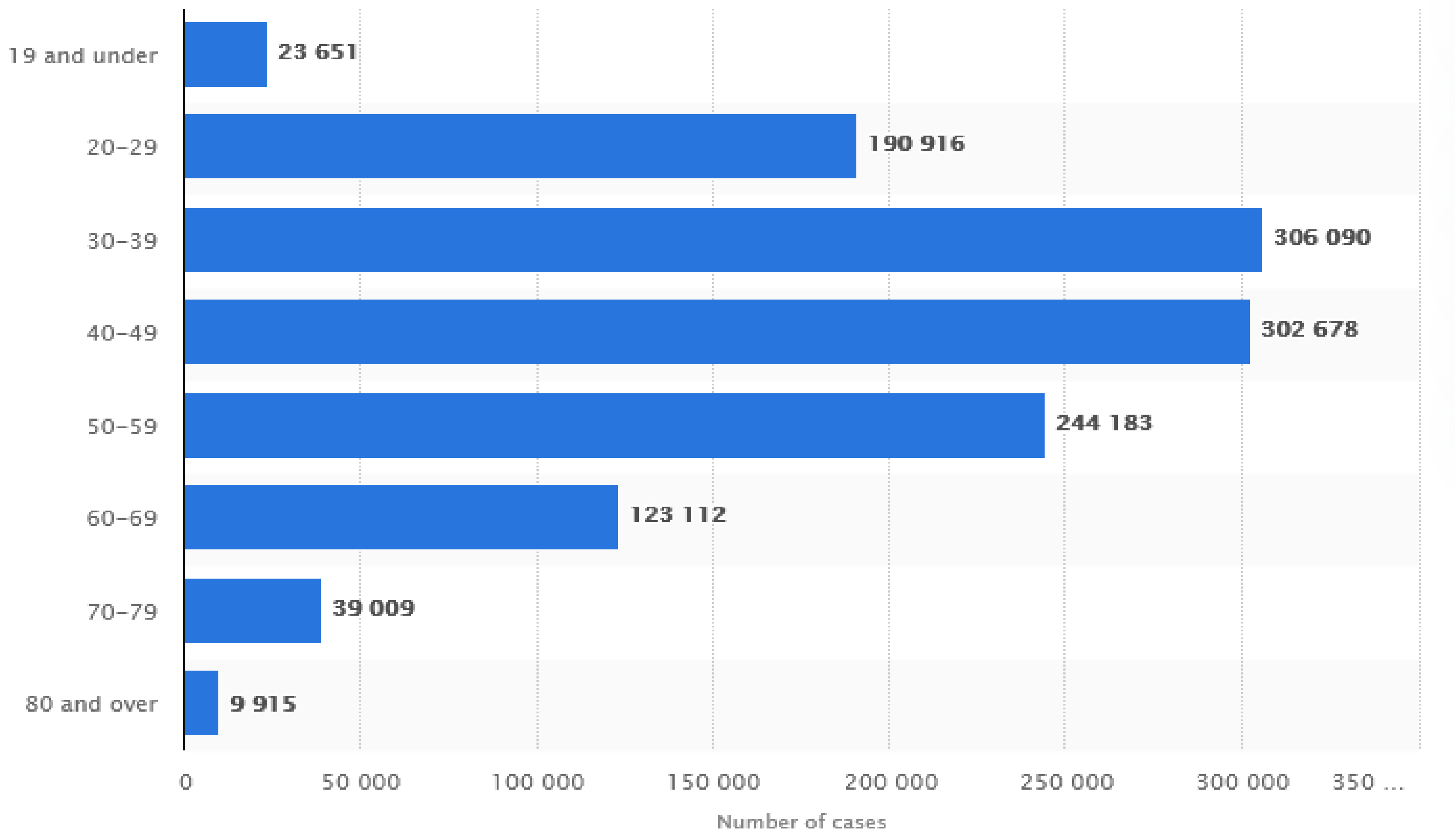


[1]Per 100,000 unit of population estimates are based on the 2004 U.S. Census population estimates (Table NST-EST2004-01 - Annual Estimates of the Population for the United States and States, and for Puerto Rico: April 1, 2000 to July 1, 2004). Numbers for the District of Columbia are 922 victims and 166.6 victims per 100,000 population.

Federal Trade Commission
Created February 1, 2005

IDT Complaints by Victim's Age

2020



TEENAGER IDT

- Teens with unused SSNs have no credit ratings or history
- A teen’s good credit sits unused until he or she is old enough to obtain a credit card
- The theft can go undetected for years

SENIOR “ROMANCE”

- Elder fraud is increasing due to isolation
- Distant relatives or online meetups develop into money requests
- Scammers impersonate a real person whose profile they steal from the web
- Children take control of their parents’ bank accounts and use it for their own needs
- Gift card request are common

PROTECT YOURSELF

- Always read your bank and credit card statements. Report anything suspicious to your bank or credit card issuer – even a charge as little as a penny.
- Check your credit report frequently throughout the year. If you’re not monitoring your credit report, new account fraud could go undetected for months, even years.

PROTECT YOURSELF

- Follow up on calls and letters about accounts you didn’t open. These are often warning signs of identity theft.
- Shred documents that have your sensitive personal and financial information on it.
- Avoid carrying your Social Security card with you.
- Be leery of online and offline sweepstakes, contests and giveaways

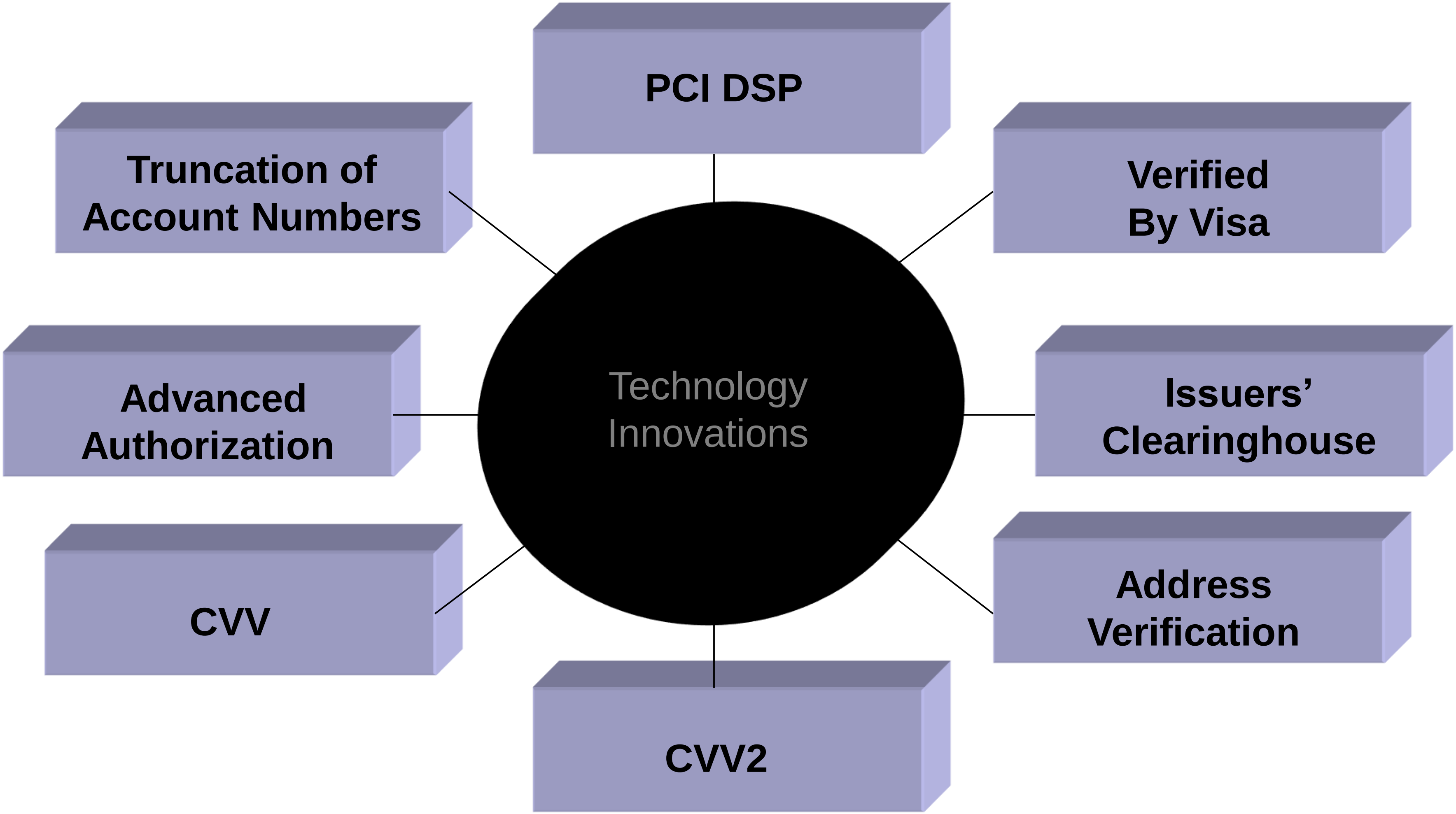
IRC Sec 7216

- Criminal provision enacted in 1971 that prohibits disclosing taxpayer information
- Fines up to $1,000 and/or prison for one year for each criminal violation
- Update effective January 1, 2009
- Specific signed consents from taxpayer are required prior to disclosure of their information (prior to getting tax info)

IRC Sec 7216

- Separate taxpayer consents must be used for authorizing **uses** and **disclosures**
- You cannot engage in tax planning or consultation services without the specific written consent of the taxpayer
- Client lists used for tax preparation services cannot be used to solicit for other consulting and planning services

CREDIT CARD PROTECTIONS

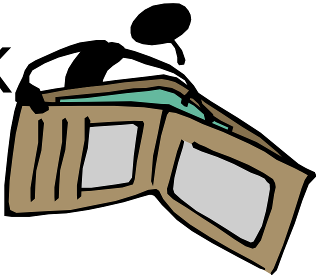


CREDIT CARD PROTECTIONS

- Install firewalls and test security regularly
- Never use vendors default passwords
- Minimize storage of customer card data
- Encrypt data for backup/transmission
- Make stored data unreadable
- Regularly update antivirus software
- Restrict data access to employees who require it and assign unique user ID

DETER

- Shred financial documents
- Protect your social security number
- Don’t give out personal information
- Don’t click on unsolicited emails or links
- Don’t use obvious passwords
- Keep your personal information in a secure place at home and/or work

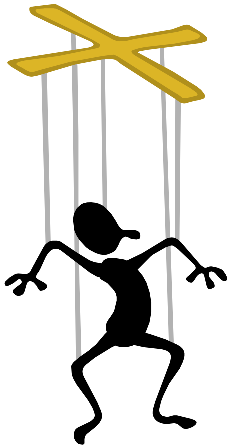


DETECT

- Be alert to unexpected financial activity
- Check your credit reports annually
- Review your financial accounts
- Check on unused credit card accounts or close dormant accounts

DEFEND

- Place a fraud alert on your accounts if you suspect IDT
- Close accounts that may have been tampered with or are dormant
- File a police report
- File a report with the Federal Trade Commission



DISCUSSION POINTS

- Are you a victim of identity theft?
- Do you know someone who was a victim?
- How was it discovered?
- What was the financial effect?
- What are the act’s key features?
- What are the legal implications?
- Why did the act fail?

Credit Bureaus

- EQUIFAX – http://www.equifax.com/,
  - 1-800-685-1111 or 1-800-525-6285
  - P.O. Box 740241, Atlanta, GA 30374-0241
- EXPERIAN – http://www.exerian.com/,
  - 1-888-397-3742
  - P.O. Box 2104, Allen, TX 75013
- TRANSUNION – http://www.transunion.com/
  - 1-800-916-8800 or 1-800-680-7289
  - P.O. Box 1000, Chester, PA 19022

REFERENCES

- Federal Trade Commission — www.ftc.gov
- Privacy Rights Clearinghouse
  - www.privacyrights.org
- National Fraud Information Center
  - www.fraud.org
- Identity Theft Resource Center
  - www.idtheftcenter.org
- Consumer Action
  - www.consumer-action.org

PROTECT YOURSELF

visit
www.annualcreditreport.com

Request your credit from one or all three credit reporting bureaus and follow-up errors

THANK YOU

It is always a pleasure to present to this group.

I am old and we need to recruit young speakers.

Please let me know when you are ready to become one of our new “STAR” speakers.