Digital Resource Packet

Identity Theft Intervention
Presentation by Barb Hedstrom, Shakopee PD
Wednesday, April 11, 2018
MITCIRN Advanced Training

Contents:

Shakopee Specific Resources

General Resources

Examples of Reports to View

Identity Theft /Scam/ Financial Exploitation Resources

- **Shakopee Police Department 952-233-9400**
  http://www.shakopeemn.gov/public-safety/police-department
  - **Stop. Confirm. Alert. Monitor. Share.** S.C.A.M.S. resistance training.
  - Identity Theft: How to Protect Yourself and What to Do If It Happens pamphlet
- **Federal Trade Commission: 877-438-4338 ftc.gov**
  - Bookmarkers and pamplets on phone scams, Avoiding Identity Theft and more
  - Identity Theft Affidavit https://www.identitytheft.gov/
  - OnGuardOnline https://www.consumer.ftc.gov/features/feature-0038-onguardonline online security tips
  - Application for **Western Union** settlement: www.WesternUnionRemission.com or contact Remission Administrator, Gilardi & Co. at 844-319-2124 to request a Petition for Remission Submission form which must be returned by **May 30, 2018.**
- **Minnesota Attorney General's Office: 651-539-1600 ag.state.mn.us**
  - Guarding Your Privacy: Tips to Prevent Identity Theft
  - Seniors Guide to Fighting Fraud
  - Reducing Unwanted Calls and Mail
- **Consumer Financial Protection Bureau: 855-411-2372 https://www.consumerfinance.gov/**
  - MONEY SMART for Older Adults Resource Guide
  - Know Your Financial Adviser
  - Help for agents under a power of attorney
  - Help for trustees under a revocable living trust
  - How to spot frauds and scams
- **Identity Theft Resource Center: 1-888-400-5530** https://www.idtheftcenter.org/ non-profit providing free help to victims and providing information on ID Theft, data breaches, cyber security, scams/frauds & privacy issues and several identity theft and data breach emails.
- **Privacy Rights Clearing House:** https://www.privacyrights.org/ non-profit education/advocacy organization offering information about data breaches, ID theft, online privacy & safety, credit and more.
- **Better Business Bureau of MN & ND 651-699-1111** https://www.bbb.org/en/us/local-bbb/bbb-of-minnesota-and-north-dakota non-profit who takes complaints about local businesses and thru their Marketplace Ethics scam protection education including scam tracker map, scams targeting businesses, military advocacy and more.
- **AARP Fraud Watch Network: Helpline: 877-908-3360** www.aarp.org https://www.aarp.org/money/scams-fraud/fraud-watch-network/ non-profit assisting seniors and free scam victim assistance to avoid & respond to scams, fraud and identity theft and provide resources, education, scam alert emails and fraud tracker map.
- **Treasury Inspector General for Tax Administration** https://www.treasury.gov/tigta/ federal agency that provides IRS oversight and related information including how to report IRS imposter scam, employment related identity theft, email updates, downloadable posters and flyers and webinars
- **Financial Industry Regulatory Authority** http://www.finra.org/investors/protect-your-identity organization to monitor, license security brokers to safeguard the investing public against fraud & bad practices. They offer securities helpline for seniors, complaint center, ombudsman's office and protect your money tips that include protecting your identity and avoiding fraud plus more. Good suggestions for protecting personal financial info.
- **US Postal Service Informed Delivery** https://informeddelivery.usps.com/ Delivery application that allows you to digitally preview you letter sized mail being delivered to an address, which may help deter mail thefts or respond to determine what mail was stolen. Research if this service provides benefits to you. See https://krebsonsecurity.com/2017/10/usps-informed-delivery-is-stalkers-dream/ and comments.
- **US Social Security Administration** "My Social Security account" https://www.ssa.gov/myaccount/
  Online service that lets you request a replacement Social Security card (in some states but NOT Minnesota); get your SS statement, change your address and phone number and more. Creating your account may help deter future theft of your SS retirement benefits. See the site's "How We Verify & Protect Your Identity." Research if this service provides benefits to you. See article and comments at: http://www.investmentnews.com/article/20171106/BLOG05/171109958/someone-tried-to-hack-my-social-security-account

What to do if you think you are being scammed? From the Shakopee Police Department

S STOP. Take your time before responding or acting. Do NOT act right away no matter how much you are pressured to do so. HANG UP. Do Not CLICK on or open message or computer ad or storyline.

C CONFIRM. Check out the story or identity of person. Call a trusted family, friend, neighbor, pastor, banker or the police to get their opinion on what to do. Research the phone number, person or company.

A ACT immediately If you are out any money. Try to cancel the money transfer. Report it to police. If you act soon enough *sometimes* the money you sent can get intercepted and returned to you.

M MONITOR. Watch your bank and credit card statements for incorrect charges. Request & review credit reports and dispute any incorrect information. Be wary of additional scam attempts.

S SHARE. Tell others about scams or frauds attempted on you. Share what you learned!

Barb Hedstrom, Crime Victim & Community Outreach Coordinator
Liz Guggisberg, Crime Prevention Specialist
Shakopee Police Department
952-233-9400 or 911 or after hours 952-445-1411

I've Been SCAMMED! Can I get my money back ?

If you realize you have been scammed and act promptly, you may be able to cancel the payment you sent to the scammer. Below are suggestions on how to attempt to cancel and get a refund:

Western Union, MoneyGram or USPS Money Orders:

- Keep your original documents or receipts. IF you still have the original money order, return the document to the issuer so that it does not get cashed and to speed up the refund process.
- Go back to the location where you purchased the MoneyGram, USPS money order or Western Union money order when possible.
- Pay the cancellation fee vs. having it deducted from your refund which will slow things down if the money order was cashed.
- Expect a refund, if approved, to take 30-60 days.
- If the money order was cashed or deposited, you usually will get a photocopy of the document so you can see who endorsed the money order, a copy of which should be provided to law enforcement for their investigation. If the bank paid out funds without properly verifying the identity of whoever cashed the money order, a demand can be made to the bank.
- You can review in advance the forms and information you will have to provide by reviewing the following links:

- For Western Union, a Money Order Customer Request form
- For MoneyGram, a Money Order Claim Card
- For USPS money orders, form PS 6401 (Money Order Inquiry)

If a pre-paid **VISA or MasterCard (Green Dot)** card was purchased at places like CVS Pharmacy or Walgreens, you might be able to be *canceled* the transaction by contacting the customer service number on the back of the card or by calling 866-795-7597. You can report the fraud here: https://secure.greendot.com/customersupport/report-fraud . You will have to provide proof of purchase if any funds are recovered. You should be contacted by phone or email within 5 business days if Greendot is unable to recover funds.

You could also try to see if the card is "register" to you or if you should try to register the card in your name to try to prevent the scammer from accessing the money on the card without the name and passwords you create. You could also try to complete a Transaction Dispute Form regarding the unauthorized activity. Visit www.greendot.com

iTunes Gift Card can only be used to buy from the iTunes Store, App Store, iBooks Store or an Aple Music membership. You can NOT make a payment with iTunes Gift Cards. By giving the iTunes Gift Card number to a caller, you are just allowing them to spend your money at one of these "app stores" which are hard to cancel and hard to trace so your money is likely gone. If you have been a victim of a scam involving iTunes Gift Cards you can call Apple at 800-275-2273 or contact Apple Support online.

PayPal should be contacted if you suspect any instance or fraud or if you think your account has been compromised. Change your password and update your security questions right away! Go to PayPals's website to see what actions you should take if you have had any of these types of fraudulent activity:

- Unauthorized activity on your PayPal account
- Unauthorized transactions on your PayPal Debit MasterCard®
- Fake PayPal emails or spoof websites
- Items not received or a potential fraudulent seller

In addition to reporting to your local police department, you can report what happened to the Federal Trade Commission at www.identitytheft.gov or by calling 1-877-438-4338 to get a personalized recovery plan.

The Harm in Password Reuse

Shakopee Police Department
475 Gorman Street
Shakopee, MN 55379
952-233-9400

From the Desk of Thomas F. Duffy, Chair, MS-ISAC

Every day malicious cyber actors compromise websites and post lists of usernames, email addresses, and passwords online. While this can be embarrassing, such as when thousands of SLTT employees email addresses and passwords were exposed during the recent Ashley Madison breach, it also leaves users open to follow-on attacks due to password reuse.

Password reuse is when someone reuses the same password on multiple websites or accounts. This is a vulnerability when the password is exposed in coordination with other information that identifies who is using the password, such as first and last names, login names, or email addresses.

How Password Reuse is a Threat

Password reuse is a threat because it gives other malicious actors information they can use to identify you, and potentially access all your accounts. This typically occurs through one of two potential scenarios:

In the first, and most common scenario, the malicious actors can search for other accounts you use and try to login with the same password. In some cases the actors might try to find personal accounts such as Facebook, Twitter, or banking websites. If they can identify those accounts, and you reuse your password, they can login as you. In other instances the malicious actors may try to determine where you are employed and attempt to use for remote access, such as through a remote email or timecard access.

A second scenario involving a malicious website is much less common, but still poses a threat. In this scenario the malicious cyber actor sets up a website that makes you enter an email address, password, and potentially other information to gain access. Once you have done that, they know who you are and can search for your other accounts where you used the same password.

Avoiding Password Reuse

Avoiding password reuse can be challenging because of the number of websites and accounts that require passwords, some of which require updating your password every 30 days. There are two ways to both avoid password reuse and to ensure any password meets the recommended password complexity requirements.

The first technique is to use a password manager. Password managers are applications that can be stored on a computer, smartphone, or in the cloud, and will securely track passwords and where they are used. As long as the password to access the password manager is sufficiently complex, this technique can be affective. However, if the company

running the password manager is compromised (which does happen!) it is possible that all your passwords will also be compromised. If you choose a password manager that is local to your computer or smartphone, that information may be compromised if malware gets on your computer or you lose your smartphone. When choosing a password manager, ensure it is from a known, trustworthy company.

The second technique is to choose a repeatable pattern for your password, such as choosing a sentence that incorporates something unique about the website or account, and then using the first letter of each word as your password. For example the sentence: "This is my August password for the Center for Internet Security website." would become "TimAp4tCfISw." Since a strong password is complex, and includes upper and lower case letters, numbers, and a symbol, this password keeps the capitalization within the sentence, translates the word "for" to the number "4," and adds the period to include to add a symbol. The vulnerability in this technique is that if multiple passwords from the same user are exposed it may reveal the pattern.

Regardless of how a unique password is chosen, it is critically important that every password is unique. Some companies, such as Facebook, have begun programs to identify password reuse. Facebook's program to identify password reuse involves monitoring for lists of compromised usernames, emails, and passwords, and attempting to match those to the usernames or email addresses of existing Facebook users. If a match is found Facebook asks the user to reset their Facebook password.

Further advice on choosing a strong, complex password is available in the MS-ISAC Security Primer available at:
http://iic.cisecurity.org/resources/documents/SecuringLoginCredentials_001.pdf

---

Provided By:

MS-ISAC MULTI-STATE Information Sharing & Analysis Center™

STOP THINK CONNECT

Understand your credit score

Banks, credit card companies and other businesses use credit scores to estimate how likely you are to pay back money you borrow.

A higher score makes it easier to qualify for a loan or lower interest rates. Many scores range from 300-850, but different companies use different ranges.

You have many credit scores

You can have more than one score, because:

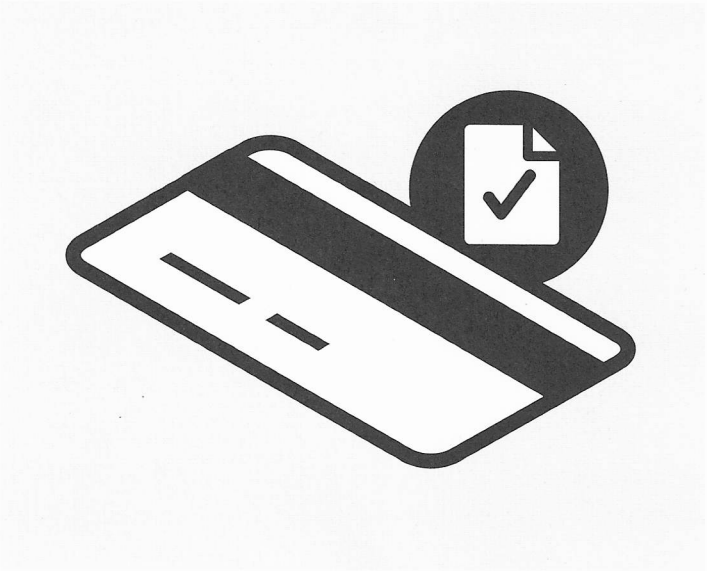
- Lenders use different scores for different products.
- There are many different credit scoring formulas.
- Information can come from different credit reporting sources.

For example, your credit card score could be different from your home loan score, and the scores you purchase online could be different from both of those.

For some people, these differences aren't that big. But because lenders use different scores, you might qualify for lower rates with one lender and not another. It can pay to shop around.

Where do credit scores come from?

Your credit scores are generally based on information in your credit reports. This information is reported by your creditors to credit reporting companies. The three biggest are Equifax, Experian and TransUnion.



Several variables affect your credit score:

- How many credit accounts you have
- How long you've had those accounts
- How close you are to your credit limit
- How much credit you have left
- How often your payments have been late
- Other factors

How to raise your score

- **Pay your bills on time, every time.** One way to make sure your payments are on time is to set up automatic payments, or set up electronic reminders. If you have missed payments, get current and stay current.
- **Don't get close to your credit limit.** Credit scoring models look at how close you are to being "maxed out," so try to keep your balances low in proportion to your overall credit limit. Experts advise keeping your use of credit at no more than 30 percent of your total credit limit.

- **A long credit history will help your score.** Credit scores are based on experience over time. Your score will improve the longer you have credit, open different types of accounts, and pay back what you owe on time.
- **Be careful closing accounts.** If you close some credit card accounts and put most or all of your credit card balances onto one card, it may hurt your credit score if you are using a high percentage of your total credit limit. Frequently opening accounts and transferring balances can hurt your score too.
- **Only apply for credit you need.** Credit scores look at your recent credit activity as an indicator of your need for credit. If you apply for a lot of credit over a short period of time, it may appear that your economic circumstances have changed for the worse.

Your credit report matters as much as your score

Mistakes in your credit reports could hurt your credit history and credit score, so check them regularly. You can get one free credit report from each of the big three credit reporting companies every 12 months. Go to annualcreditreport.com or call **877-322-8228**.

When you get your report, look for:

- Mistakes in your name, phone number, or address.
- Loans, credit cards, or other accounts that are not yours.
- Reports saying you paid late when you paid on time.
- Accounts you closed that are listed as open.
- The same item showing up more than once (like an unpaid debt).

How to fix mistakes

If you find something wrong in your credit report, you may contact both the credit reporting company and the creditor that provided the information. Explain what you think is wrong and why. Include copies of documents that support your dispute.

Your credit reports will come with instructions on how to dispute mistakes.

Submit a complaint

If you have a credit reporting problem, you can submit a complaint:

Online
consumerfinance.gov/complaint

By mail
Consumer Financial Protection Bureau
P.O. Box 4503
Iowa City, Iowa 52244

We'll forward your complaint to the company and work to get a response from them. You will receive email updates along the way and can track the status of your complaint online.

Watch accounts closely when card data is hacked

Keep a close eye on your account activity and report suspicious transactions quickly if you believe someone stole your credit or debit card information.

It doesn't matter if your account number was among millions of others swept up in a massive data breach, or if a hacker snared your information from an unsecure WiFi network, if you take the right steps, you will not be responsible for unauthorized debits to your checking account, or charges to your credit card.

Check your statements for unauthorized charges or debits

If you have online or mobile access to your accounts, check your transactions as frequently as possible. If you receive paper statements, be sure to open them and review them closely. You should do this even if you're not sure your information was compromised.

Look for any suspicious activity like unfamiliar merchant names, especially from merchants outside your area, even if the transaction amounts are small. Sometimes thieves will process a small debit or charge against your account and return to take more if the small debit or charge goes through.

Make a habit of monitoring your accounts. Fraudulent charges or debits to your accounts might occur months after the theft of your information.

Immediately alert your provider if you spot suspicious activity

Contact your bank or card provider immediately if you suspect an unauthorized debit or charge. If a thief takes money from your bank account by debit, or charges items to your credit card, you should cancel the card and have it replaced before more transactions come through. You should also consider changing your PIN just to be on the safe side.

For credit cards

You are not responsible for unauthorized charges if someone stole only your credit card account number. If the card is lost or stolen too, you could be responsible for up to $50.

For debit cards

If an unauthorized transaction appears on your statement (but your card or PIN has not been lost or stolen) you will not be liable for the debit if you report it within 60 days after your account statement is sent to you. But, if the charge goes unreported for more than 60 days, your money could be lost. When you report the theft, the bank will investigate and may credit the money back to your account.

The time for you to report is much shorter if your card or PIN has been lost or stolen (2 business days, in order to limit your liability to no more than $50 of unauthorized charges), so make the report as soon as you learn that your card is missing or your PIN has been stolen.

For payroll, benefits, and prepaid cards

For these types of cards, your rights vary depending on the card. If you think someone stole information from a payroll, government benefit, or prepaid card, check with the provider to find out its policy and deadlines for disputing charges. Your rights vary depending on the type of card.

How to report a suspicious charge or debit

If you spot a fraudulent transaction, call the card provider's toll-free customer service number immediately. Ask how you can follow up with a written communication. Your monthly statement or error resolution notice also likely includes instructions on how and where to report fraudulent charges or billing disputes.

Be sure to keep copies of your letters for your records. Write down the dates you make follow-up calls and keep this information together in a file.

Tip: If you get a replacement card with a new number, remember to update any automatic payments linked to the card.

Contact us if you're unhappy with card providers' response

Card providers should investigate the charges and respond quickly – generally within 10 business days of receiving an error notice for debit card disputes or within two billing cycles for credit card disputes. You have a right to know the results of the investigation.

Submit a complaint

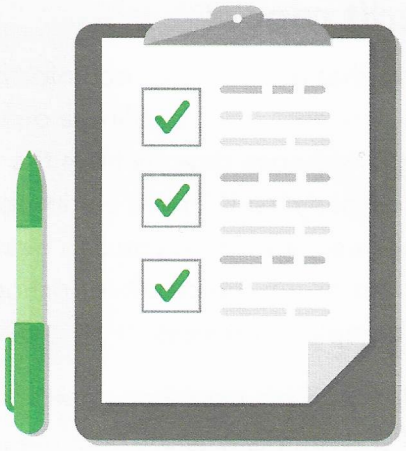
If you have an issue with the card provider's response, you can submit a complaint to us. Go to consumerfinance.gov/complaint or call (855) 411-CFPB (2372).

You can also learn more about billing disputes and your card protections at consumerfinance.gov/askcfpb.

You have a right to see specialty credit reports

You have the right to know what nationwide specialty credit reporting companies are saying about you.

And you're entitled to one free report each year, just like with the traditional nationwide credit reporting companies – Experian, Equifax, and TransUnion. What's more, nationwide specialty credit reporting companies have to make it easy for you to get a copy of any file they keep on you. At a minimum, they have to provide a toll-free number for you to call and order your report.



Check for errors

This is an important right, because if you don't know what's in those files, you can't dispute any inaccuracies. Errors in your credit reports, or fraud caused by identity theft, can make borrowing more expensive. In certain instances, they can also prevent you from getting credit, insurance, a lease, or a new job. You may want to check your files:

- If you were a victim of identity theft.
- If you think someone may have fraudulently used one of your accounts.
- Before applying for insurance.
- Before applying for a lease.
- If you've applied for a new job and you've been asked to authorize a report.

What is a nationwide specialty credit reporting company?

These are companies that collect information about consumers' medical records or payments, residential or tenant history, check-writing history, employment history, or insurance claims. Like the three largest nationwide credit reporting companies (Experian, Equifax, and TransUnion), they gather and report information about you to creditors, landlords, insurance companies, employers, and others.

To help you access specialty and other credit reports, we created a list with the websites and toll-free telephone numbers for many credit reporting companies. Visit http://files.consumerfinance.gov/f/201207_cfpb_list_consumer-reporting-agencies.pdf.

The list includes more than nationwide specialty credit reporting companies. It also includes other companies that have identified themselves as credit reporting companies or that provide consumers access to their credit reports. Not all of them are required to provide a free copy of your report.

If you find incorrect information on your credit report

If you believe that there's incorrect information on your credit report, start by filing a dispute and getting a response directly from the credit reporting company itself. There are important federal consumer rights that you can best preserve by first going through the credit reporting company's complaint process.

After you file a complaint with the credit reporting company, if you are dissatisfied with the resolution, you can submit a complaint to us.

Submit a complaint

Have an issue with a financial product or service? We'll forward your complaint to the company and work to get a response from them.

Online
consumerfinance.gov/complaint

By phone
(855) 411-CFPB (2372)
(855) 729-CFPB (2372) TTY/TDD

By fax
(855) 237-2392

By mail
Consumer Financial Protection Bureau
P.O. Box 4503
Iowa City, Iowa 52244

CYBERSECURITY ALLIANCE

BBB

DO A DIGITAL DECLUTTER THIS SPRING

A few easy, actionable tips will help you stay cyber safe and protect your personal data and identity. The National Cyber Security Alliance (NCSA) and Better Business Bureau (BBB) are encouraging all consumers freshen up their online lives by conducting a thorough cleaning of their cyber clutter. With preventing identity theft a top safety concern for Americans, NCSA and BBB encourage everyone to make "digital spring cleaning" an annual ritual to help protect valuable personal data.

Refreshing your online life is a relatively simple process. NCSA and BBB have identified the top trouble-free tips everyone should follow this spring and all year round.

KEEP A CLEAN MACHINE

Ensure all software on internet-connected devices – including PCs, smartphones and tablets – is up to date to reduce risk of infection from malware.

LOCK DOWN YOUR LOGIN

Your usernames and passphrase are not enough to protect key accounts like email, banking and social media. Begin your spring cleaning by fortifying your online accounts and enabling the strongest authentication tools available, such as biometrics, security keys or a unique one-time code through an app on your mobile device.

DECLUTTER YOUR MOBILE LIFE

Most of us have apps we no longer use and some that need updating. Delete unused apps and keep others current, including the operating system on your mobile devices.

DO A DIGITAL FILE PURGE

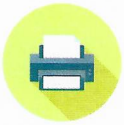
Perform a good, thorough review of your online files. Tend to digital records, PCs, phones and any device with storage just as you do for paper files. Get started by doing the following:

- Clean up your email: Save only those emails you really need and unsubscribe to email you no longer need/want to receive.
- Back it up: Copy important data to a secure cloud site or another computer/drive where it can be safely stored. Passphrase protect backup drives. Always back up your files before getting rid of a device, too.

OWN YOUR ONLINE PRESENCE

Review the privacy and security settings on websites you use to ensure they're at your comfort level for sharing. It's OK to limit how and with whom you share information.

Here are some user-friendly tips to help with the safe disposal of electronically stored data. Prep your devices in advance of participating in BBB's Secure Your ID Day.



KNOW WHAT DEVICES TO DIGITALLY "SHRED"

Computers and mobile phones aren't the only devices that capture and store sensitive, personal data. External hard drives and USBs, tape drives, embedded flash memory, wearables, networking equipment and office tools like copiers, printers and fax machines all contain valuable personal information.

CLEAR OUT STOCKPILES

If you have a stash of old hard drives or other devices – even if they're in a locked storage area – information still exists and could be stolen. Don't wait: wipe and/or destroy unneeded hard drives as soon as possible.

EMPTY YOUR TRASH OR RECYCLE BIN ON ALL DEVICES AND BE CERTAIN TO WIPE AND OVERWRITE

Simply deleting and emptying the trash isn't enough to completely get rid of a file. Permanently delete old files using a program that deletes the data, "wipes" it from your device and overwrites it by putting random data in place of your information – that then cannot be retrieved.

- For devices like tape drives, remove any identifying information that may be written on labels before disposal, and use embedded flash memory or networking or office equipment to perform a full factory reset and verify that no potentially sensitive information still exists on the device.

DECIDE WHAT TO DO WITH THE DEVICE

Simply deleting and emptying the trash isn't enough to completely get rid of a file. Permanently delete old files using a program that deletes the data, "wipes" it from your device and overwrites it by putting random data in place of your information – that then cannot be retrieved.

CYBERSECURITY ALLIANCE

STAYSAFEONLINE.ORG

STAYSAFEONLINE

NCSA_US

STAYSAFEONLINE

BBB

BBB.ORG

BBB_US

BETTERBUSINESSBUREAU

Top Scams Targeting Seniors

Do not share information or send money.

Fake IRS Calls: Scammers claim to be with the IRS and demand immediate payment. The IRS doesn't call people.

Lottery and Sweepstakes: You receive a check and letter announcing you have won a large sum of money. You are asked to pay a fee/tax to collect the prize. Never pay money to claim a prize.

Grandparent Scam: You receive a call from someone pretending to be your grandchild. The caller claims to be in trouble in a foreign country and asks you to wire money, to post bail, or pay for damages. The money goes to a scam artist and you are out thousands of dollars.

Romance Scam: You meet someone on a dating website. The person quickly professes love for you and then asks you to move off the secure dating site so you can be in touch via phone, email or text. Shortly afterward, you are asked for money. Never send money to someone you've met online.

Home Repair or Inspection Fraud: A person comes to your door and claims to be an expert who can do repairs at a very low price. Trust your instincts. If the "expert" uses high-pressure sales tactics or you feel intimidated, turn them away. Never pay the full cost of a job up-front.

Imposter Schemes: You receive calls or emails from individuals claiming to be with Medicare, a credit card company or a bank; these communications ask you to verify your personal information. Do not engage with these solicitors.

Resources

Scam Tracker - bbb.org/scamtracker

Federal Trade Commission - ID Theft
877-438-4338 • ftc.gov

MN Attorney General - Consumer Protection
651-296-3353 or 800-657-3787
ag.state.mn.us

MN Department of Commerce
651-539-1600 or 800-657-3602
mn.gov/commerce

ND Attorney General - Consumer Protection
800-472-2600 • ag.nd.gov

ND Department of Commerce
701-328-5300 • commerce.nd.gov

Minnesota Elder Justice Center
651-440-9300 • elderjusticemn.org

Senior Linkage Line
800-333-2433
minnesotahelp.info/specialtopics/seniors

AARP
888-687-2277 • aarp.org

United States Postal Inspection Service
877-876-2455
postalinspectors.uspis.gov

To stop telemarketing:
Do Not Call Registry
888-382-1222 • donotcall.gov

To stop junk mail:
Direct Marketing Association
212-768-7277 • dmachoice.org

To opt out of credit card offers:
888-567-8688

To get your free credit report:
annualcreditreport.com • 877-322-8228

BBB
BBB Institute for
Marketplace Ethics

Mission:
To provide education, resources and training on ethics, as well as to prevent marketplace fraud and scams targeting at-risk consumers.

Vision:
An ethical marketplace where buyers and sellers trust each other.

We are a 501(c)3 non-profit:
Charitable business and public support allows us to offer free fraud prevention resources that protect at-risk consumers and provide trainings, tools, scholarships and recognition programs that further promote ethical enterprise and leadership. To support fraud prevention services in our community, visit **thefirstbbb.org**

To request materials or to schedule a BBB speaker for your group about marketplace trust issues affecting seniors, their families, friends and caregivers, please contact:

Twin Cities Metro
safeguarding.seniors@thefirstbbb.org

Greater Minnesota & North Dakota
senior.outreach@thefirstbbb.org.

Start With Trust®

BE WISE
BE INFORMED
BE EMPOWERED

Thank you to our sponsor:

Allianz

Purchase With Confidence

BBB.org - Your Free and Trusted Resource

BBB Business Profiles – Research a company's track record, complaint details, and ratings before you do business with them.

BBB Online Directory – Search our online directory by category to find local BBB Accredited Businesses.

Customer Reviews - Read about consumers' experiences with area companies and/or submit your own customer review.

Dispute Resolution - Resolve business complaints and disputes using conciliation, mediation or arbitration services. Last year, BBB of Minnesota and North Dakota handled more than 23,000 complaints with a 90% satisfaction rate.

Estimates – Receive multiple free quotes from area Accredited Businesses in one easy step with BBB Request a Quote.

Scam Tracker - Use our interactive map to report and read about fraud, scams and schemes across North America by visiting. **bbb.org/scamtracker**

BBB
bbb.org

Better Business Bureau of Minnesota and North Dakota
bbb.org • 800-646-6222

Red Flags and Do's & Don'ts

Have you received a phone call asking for bank account, credit card or other personal information?

Hang up and call your provider.

Did you receive a check in the mail with a letter stating you've won a sweepstakes or prize?

Don't cash the check and never pay fees or taxes to collect a prize.

Has someone knocked on your door selling products, services or repairs?

Don't let them in. Ask for IDs and check the company out with BBB.

Does the offer or product sound too good to be true?

Be wary. It probably is.

Were you invited to an estate planning seminar?

Make sure the product is registered with the Securities and Exchange Commission, that the broker is licensed in your state, and avoid making quick financial decisions. Check with more than one trusted advisor.

Are there unexpected charges to your bank account or credit card?

Check your statements often and correct discrepancies as soon as possible.

Red Flags and Do's & Don'ts

Did you receive suspicious e-mails or calls from someone claiming to be from a computer company saying they need to update or fix your system?

Do not give them information. They may install malware which allows them access to everything on your computer.

Did you receive a high-pressure, emotional call from a charity with a name that sounds similar to a well-known charity?

Check out the charity name with BBB at give.org

Have you been asked to wire money to someone you don't know?

Don't do it!

Has a family member or caregiver asked to have access to your funds or to change your Power of Attorney, your will or beneficiary designation?

Have more than one trusted individual involved before you make any changes.

Have you received a call, offer or solicitation?

Don't send money or share personal information without checking the company's track record with BBB first.
Visit bbb.org or call 1-800-646-6222 to access BBB's free tools and resources.

Guidelines for Giving Wisely To Charities

Warning Signs

Sound-Alike Names: Don't be fooled by names that sound impressive or that closely resemble the name of a well-known organization.

High-Pressure Tactics: If an on-the-spot donation is requested, be skeptical. A legitimate charity will welcome your donation as much tomorrow as they will today.

Emotional Appeals: Be wary of vague appeals which use a heartbreaking story, but are short on facts describing the charity's services.

Cash Payment Requested: Always pay by check or credit card - never by cash. Make the check payable to the organization and not to an individual.

Unable to Provide Information: If the organization cannot provide information regarding their services, walk away. A legitimate organization will offer you a brochure detailing their services or will direct you to their website.

Tips for Giving Wisely

- If contacted by phone, ask for the organization's address, phone number and a contact person so you can research the organization before you send any donation.
- Verify that the charity asking for donations is registered with the Attorney General in Minnesota or the Secretary of State in North Dakota. Organizations are required to register before asking for donations.
- Keep records of your donations so you can document your charitable giving at tax time.
- Research the organization with BBB's Wise Giving Alliance at **give.org**.

FTC FACTS for Consumers

ftc.gov
For The Consumer
Federal Trade Commission
1-877-FTC-HELP

To Buy or Not To Buy:

Identity Theft Spawns New Products and Services To Help Minimize Risk

Recent headlines about data breaches and losses of personal information have prompted many companies to advertise products or services to help consumers prevent or minimize their risk of identity theft.

The Federal Trade Commission (FTC), the nation's consumer protection agency, says before you pay for an identity theft prevention product or service, make sure you understand exactly what you're paying for. Many people find value and convenience in paying an outside party to help them exercise their rights and protect their information. At the same time, some rights and protections you have under federal or state laws can help you protect your identity and recover from identity theft at no cost. Knowing and understanding your rights can help you determine whether — or which — commercial products or services may be appropriate for you.

Fraud Alerts

A **fraud alert** is a signal placed in your credit report or credit file to warn potential creditors that they must use what the law calls "reasonable policies and procedures" to verify your identity before they issue credit in your name. Fraud alerts may be effective at stopping someone from

opening new credit accounts in your name, but they may not prevent the misuse of your existing accounts.

Under the federal Fair Credit Reporting Act (FCRA), you may be entitled to two kinds of free fraud alerts: *initial* and *extended*.

You may ask a consumer reporting company to place an *initial* fraud alert on your credit report if you suspect you have been, or are about to be, a victim of identity theft. This may be appropriate after your wallet or another source of personal information is lost or stolen. An *initial* fraud alert is good for 90 days, and can be renewed when appropriate. To place an *initial* fraud alert, call the toll-free fraud number of any one of the three national consumer reporting companies. The company you call is required to contact the other two; they, in turn, will place an alert on their versions of your report. Expect to receive a confirmation from each of the companies.

Equifax: 1-800-525-6285

Experian: 1-888-EXPERIAN (397-3742)

TransUnion: 1-800-680-7289

When you place an *initial* fraud alert on your credit report, you're entitled to order one free credit report from each of the consumer reporting companies; if you ask, only the last four digits of your Social Security number will appear on your reports.

If you have been a victim of identity theft, you may ask for an *extended* alert, which stays on your credit report for seven years. To get an *extended* fraud alert placed on your report, you will need to contact one of the credit bureaus, and provide an Identity Theft Report, such as a police report or other report to a law enforcement agency, including a report to the FTC. If your credit report has an *extended* alert, potential creditors must contact you in person, or by phone or some other method you have provided before they can issue credit in your name. When you place an *extended* alert on your credit report, you're entitled to two free credit reports from each of the consumer reporting companies within 12 months. In addition, the consumer reporting companies must remove your name from marketing lists for pre-screened offers of credit for five years — unless you ask them to put your name back on the list.

Credit Freezes

A **credit freeze** allows you to restrict access to your credit report. If you place a freeze on your report, potential creditors and certain other people or businesses can't get access to it unless you lift the freeze temporarily or permanently. For more information about credit freezes, check with your state attorney general's office or visit www.naag.org.

Limiting access to your credit report makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors will need to view a credit file before opening a new account; if they can't see the file, they may not extend the credit. Still, a

credit freeze may not prevent the misuse of your existing accounts or certain other types of identity theft.

A credit freeze is different from a fraud alert in a number of ways. A freeze generally stops all access to your credit report, while a fraud alert permits creditors to get your report as long as they take steps to verify your identity. The availability of a credit freeze depends on state law or a consumer reporting company's policies; fraud alerts are federal rights intended for consumers who believe they may have been, or actually have been, victims of identity theft. And some states charge a fee for placing or removing a freeze, although it is free to place or remove a fraud alert.

Most states have laws that allow consumers to place a credit freeze with consumer reporting companies. In many of these states, any consumer can freeze their credit file; in others, only identity theft victims can freeze their files. The cost of placing a credit freeze and the lead times vary. In many states, credit freezes are free for identity theft victims; other consumers typically are charged about $10 per credit reporting company. Contact your state attorney general for the particulars of your state's freeze laws. To place a freeze, contact each of the nationwide consumer reporting companies because a credit freeze placed at one company is not referred to the other companies. And be aware that the three major credit reporting companies have begun offering credit freezes directly to consumers — for a fee — regardless of whether their state has a freeze law.

Placing a credit freeze does not affect your credit score, keep you from getting your free annual credit report, or keep you from buying your credit report or score. It doesn't prevent you from opening a new account yourself, applying for a job, renting an apartment, or buying insurance, either. In these situations, the business usually needs to review your credit report. You can ask the consumer reporting company to lift your credit freeze temporarily, or remove it altogether. But the cost and lead times to lift or remove a freeze vary, so it's wise to check with your state authorities or with a consumer reporting company in advance if possible.

Free Credit Reports

Federal law gives every consumer the right to one free credit report from each nationwide consumer reporting company every 12 months. Staggering these reports — that is, getting a report from a different company every few months — can help you monitor activity on your credit reports. For more information, or to request your free credit reports, visit www.annualcreditreport.com.

Identity Theft Protection Products and Services for Sale

Identity theft protection companies offer a range of products and services for sale. Some allow you to "**lock**," "**flag**," or "**freeze**" your credit reports. Often, the companies advertising these services simply are offering to place a fraud alert or credit freeze on your report. These services also may renew or update your alerts or freezes

automatically, as long as you continue to pay. Under the law, initial fraud alerts and renewals are available for free if you have reason to believe you have been — or are about to be — a victim of identity theft.

Some companies, including consumer reporting companies, offer subscriptions to credit monitoring services. These services track your credit report, and generally send you an email alert reflecting recent activity, such as an inquiry or new account. Typically, the more frequent or more detailed the report, the more expensive the service.

Some companies offer services to help you rebuild your identity in the event of identity theft. Typically, these services operate by obtaining a limited power of attorney from you, which enables the company to act on your behalf when dealing with consumer reporting companies, creditors, or other information sources.

Many companies may offer additional services, including removing your name from mailing lists or pre-screened offers of credit or insurance, representing your legal interests, "guaranteeing" reimbursement in the event you experience a loss due to identity theft, or helping you track down whether your personal information has been exposed online. Before you agree to pay for any of these services, read the fine print. You can get some of them yourself at no cost: for example, if you decide you don't want to receive pre-screened offers of credit and insurance, you can opt out for five years or permanently by calling toll-free 1-888-5-OPTOUT (1-888-567-8688) or visiting www.optoutprescreen.com.

The FTC has a library of resources to help victims of identity theft report the crime and take steps to recover their identity. Visit www.ftc.gov/idtheft.

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or to get free information on consumer issues, visit www.ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

FEDERAL TRADE COMMISSION	ftc.gov
1-877-FTC-HELP	FOR THE CONSUMER

Federal Trade Commission
Bureau of Consumer Protection
Division of Consumer and Business Education

November 2007

Average time to complete: 10 minutes

Identity Theft Victim's Complaint and Affidavit

A voluntary form for filing a report with law enforcement, and disputes with credit reporting agencies and creditors about identity theft-related problems. Visit ftc.gov/idtheft to use a secure online version that you can print for your records.

Before completing this form:

1. Place a fraud alert on your credit reports, and review the reports for signs of fraud.
2. Close the accounts that you know, or believe, have been tampered with or opened fraudulently.

About You *(the victim)*

Now

(1) My full legal name: _____
First Middle Last Suffix

(2) My date of birth: _____
mm/dd/yyyy

(3) My Social Security number: _____-_____-_____

(4) My driver's license: _____ _____
State Number

(5) My current street address:

_____
Number & Street Name Apartment, Suite, etc.

_____
City State Zip Code Country

(6) I have lived at this address since _____
mm/yyyy

(7) My daytime phone: (____)_____
My evening phone: (____)_____
My email: _____

Leave (3) blank until you provide this form to someone with a legitimate business need, like when you are filing your report at the police station or sending the form to a credit reporting agency to correct your credit report.

At the Time of the Fraud

(8) My full legal name was: _____
First Middle Last Suffix

(9) My address was: _____
Number & Street Name Apartment, Suite, etc.

_____
City State Zip Code Country

(10) My daytime phone: (____)_____ My evening phone: (____)_____
My email: _____

Skip (8) - (10) if your information has not changed since the fraud.

The Paperwork Reduction Act requires the FTC to display a valid control number (in this case, OMB control #3084-0047) before we can collect – or sponsor the collection of – your information, or require you to provide it.

About You *(the victim) (Continued)*

Declarations

(11) I ☐ did OR ☐ did not authorize anyone to use my name or personal information to obtain money, credit, loans, goods, or services — or for any other purpose — as described in this report.

(12) I ☐ did OR ☐ did not receive any money, goods, services, or other benefit as a result of the events described in this report.

(13) I ☐ am OR ☐ am not willing to work with law enforcement if charges are brought against the person(s) who committed the fraud.

About the Fraud

(14) I believe the following person used my information or identification documents to open new accounts, use my existing accounts, or commit other fraud.

(14): Enter what you know about anyone you believe was involved (even if you don't have complete information).

Name: _____
First Middle Last Suffix

Address: _____
Number & Street Name Apartment, Suite, etc.

_____
City State Zip Code Country

Phone Numbers: (____)_____ (____)_____

Additional information about this person: _____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

(15) Additional information about the crime (for example, how the identity thief gained access to your information or which documents or information were used):

(14) and (15): Attach additional sheets as needed.

_____

_____

_____

_____

_____

_____

_____

Documentation

(16) I can verify my identity with these documents:

(16): Reminder: Attach copies of your identity documents when sending this form to creditors and credit reporting agencies.

☐ A valid government-issued photo identification card (for example, my driver's license, state-issued ID card, or my passport).
If you are under 16 and don't have a photo-ID, a copy of your birth certificate or a copy of your official school record showing your enrollment and legal address is acceptable.

☐ Proof of residency during the time the disputed charges occurred, the loan was made, or the other event took place (for example, a copy of a rental/lease agreement in my name, a utility bill, or an insurance bill).

About the Information or Accounts

(17) The following personal information (like my name, address, Social Security number, or date of birth) in my credit report is inaccurate as a result of this identity theft:

(A) _____

(B) _____

(C) _____

(18) Credit inquiries from these companies appear on my credit report as a result of this identity theft:

Company Name: _____

Company Name: _____

Company Name: _____

(19) Below are details about the different frauds committed using my personal information.

Name of Institution | Contact Person | Phone | Extension

Account Number | Routing Number | Affected Check Number(s)

Account Type: ☐ Credit ☐ Bank ☐ Phone/Utilities ☐ Loan
☐ Government Benefits ☐ Internet or Email ☐ Other

Select ONE:
- ☐ This account was opened fraudulently.
- ☐ This was an existing account that someone tampered with.

Date Opened or Misused (mm/yyyy) | Date Discovered (mm/yyyy) | Total Amount Obtained ($)

Name of Institution | Contact Person | Phone | Extension

Account Number | Routing Number | Affected Check Number(s)

Account Type: ☐ Credit ☐ Bank ☐ Phone/Utilities ☐ Loan
☐ Government Benefits ☐ Internet or Email ☐ Other

Select ONE:
- ☐ This account was opened fraudulently.
- ☐ This was an existing account that someone tampered with.

Date Opened or Misused (mm/yyyy) | Date Discovered (mm/yyyy) | Total Amount Obtained ($)

Name of Institution | Contact Person | Phone | Extension

Account Number | Routing Number | Affected Check Number(s)

Account Type: ☐ Credit ☐ Bank ☐ Phone/Utilities ☐ Loan
☐ Government Benefits ☐ Internet or Email ☐ Other

Select ONE:
- ☐ This account was opened fraudulently.
- ☐ This was an existing account that someone tampered with.

Date Opened or Misused (mm/yyyy) | Date Discovered (mm/yyyy) | Total Amount Obtained ($)

(19): If there were more than three frauds, copy this page blank, and attach as many additional copies as necessary.

Enter any applicable information that you have, even if it is incomplete or an estimate.

If the thief committed two types of fraud at one company, list the company twice, giving the information about the two frauds separately.

Contact Person: Someone you dealt with, whom an investigator can call about this fraud.

Account Number: The number of the credit or debit card, bank account, loan, or other account that was misused.

Dates: Indicate when the thief began to misuse your information and when you discovered the problem.

Amount Obtained: For instance, the total amount purchased with the card or withdrawn from the account.

Your Law Enforcement Report

(20) One way to get a credit reporting agency to quickly block identity theft-related information from appearing on your credit report is to submit a detailed law enforcement report ("Identity Theft Report"). You can obtain an Identity Theft Report by taking this form to your local law enforcement office, along with your supporting documentation. Ask an officer to witness your signature and complete the rest of the information in this section. It's important to get your report number, whether or not you are able to file in person or get a copy of the official law enforcement report. Attach a copy of any confirmation letter or official law enforcement report you receive when sending this form to credit reporting agencies.

Select ONE:

- ☐ I have not filed a law enforcement report.
- ☐ I was unable to file any law enforcement report.
- ☐ I filed an automated report with the law enforcement agency listed below.
- ☐ I filed my report in person with the law enforcement officer and agency listed below.

(20):
Check "I have not..." if you have not yet filed a report with law enforcement or you have chosen not to. Check "I was unable..." if you tried to file a report but law enforcement refused to take it.

Automated report:
A law enforcement report filed through an automated system, for example, by telephone, mail, or the Internet, instead of a face-to-face interview with a law enforcement officer.

_____
Law Enforcement Department State

_____ _____
Report Number Filing Date (mm/dd/yyyy)

_____
Officer's Name (please print) Officer's Signature

_____ (____)_____
Badge Number Phone Number

Did the victim receive a copy of the report from the law enforcement officer? ☐ Yes OR ☐ No

Victim's FTC complaint number (if available): _____

Signature

As applicable, sign and date *IN THE PRESENCE OF* a law enforcement officer, a notary, or a witness.

(21) I certify that, to the best of my knowledge and belief, all of the information on and attached to this complaint is true, correct, and complete and made in good faith. I understand that this complaint or the information it contains may be made available to federal, state, and/or local law enforcement agencies for such action within their jurisdiction as they deem appropriate. I understand that knowingly making any false or fraudulent statement or representation to the government may violate federal, state, or local criminal statutes, and may result in a fine, imprisonment, or both.

_____ _____

Signature Date Signed (mm/dd/yyyy)

Your Affidavit

(22) If you do not choose to file a report with law enforcement, you may use this form as an Identity Theft Affidavit to prove to each of the companies where the thief misused your information that you are not responsible for the fraud. While many companies accept this affidavit, others require that you submit different forms. Check with each company to see if it accepts this form. You should also check to see if it requires notarization. If so, sign in the presence of a notary. If it does not, please have one witness (non-relative) sign that you completed and signed this Affidavit.

_____

Notary

Witness:

_____ _____

Signature Printed Name

_____ _____

Date Telephone Number

Other Federal Rights

Under the Justice for All Act, you have additional rights when the identity thief is being prosecuted in federal court. **You have the right to:**

- Reasonable protection from the accused.
- Reasonable, accurate, and timely notice about any public court proceeding; parole proceeding involving the crime; or release or escape of the accused.
- Not be excluded from any public court proceeding unless the judge decides that your testimony would change significantly if you heard other testimony.
- Be reasonably heard at any public proceeding in the district court involving release, plea, sentencing, or parole proceeding.
- Confer with the attorney for the government in the case.
- Full and timely restitution as provided in the law.
- Proceedings free from unreasonable delay.
- Be treated with fairness and respect for your dignity and privacy.

Other Rights:

In many states, businesses or organizations that lose or misplace certain types of personal information must tell you if that has happened. Ask your state attorney general's office for more information.

Resources

- To file a complaint and get an affidavit: **ftc.gov/complaint** or call (877) FTC-HELP
- For more information about identity theft: **ftc.gov/idtheft**
- To learn about rights in your state and credit freeze laws: **www.naag.org**
- For OVC materials related to identity theft: **http://ovc.ncjrs.gov/topic.aspx?topicid=29**

Federal Trade Commission
www.ftc.gov

Department of Justice
www.ojp.usdoj.gov/ovc

JUSTICE FOR VICTIMS
JUSTICE FOR ALL

Office for Victims of Crime
OVC

Statement of Rights for Identity Theft Victims

FTC.GOV/IDTHEFT

Several federal laws protect victims of identity theft. These laws relate to:

- documenting the theft
- working with credit reporting companies
- communicating with creditors and debt collectors
- limiting financial losses that may result from identity theft

Documenting the Theft

You have the right to create an identity theft report. An identity theft report will help you take advantage of many of your rights. The report consists of your complaint, an affidavit, and a report to law enforcement. To prepare for filing a report with local law enforcement, complete the FTC's complaint form and affidavit (**ftc.gov/complaint**) and print a copy. Give it to your local law enforcement agency when you file a report there. Your complaint and affidavit provide the details that allow credit reporting companies and the businesses involved to verify that you are a victim and to know which of your accounts or information have been affected so far.

You have the right to:

- Create an identity theft report.
- Place a 90-day initial fraud alert on your credit report.
- Place a seven-year extended fraud alert on your credit report.
- Get free copies of your credit report.
- Have fraudulent information blocked from your credit report.
- Dispute fraudulent or inaccurate information on your credit report.
- Stop creditors and debt collectors from reporting fraudulent accounts.
- Get copies of documents related to the theft of your identity.
- Stop a debt collector from contacting you.

Working with Credit Reporting Companies

You have the right to:

- Place a 90-day initial fraud alert on your credit report. The alert tells anyone who uses your credit report that they must take reasonable steps to verify who is applying for credit in your name. To place this alert, contact one of the three nationwide credit reporting companies. The one you contact must notify the others.
- Place a seven-year extended fraud alert on your credit report. To do this, provide an identity theft report to each credit reporting company and explain how potential creditors can contact you. The credit reporting companies will put your contact information on the extended fraud alert to tell potential creditors they must contact you before issuing credit in your name.
- Get one free copy of your credit report and a summary of your rights from each credit reporting company when you place a 90-day initial fraud alert. If you place an extended fraud alert with a credit reporting company, you have the right to two copies of that company's credit report about you in a 12-month period. These are in addition to the free credit report everyone is entitled to each year from each credit reporting company.
- Have credit reporting companies block fraudulent information from appearing on your credit report. You must send them a copy of a valid identity theft report, proof of your identity, and a letter stating which information is fraudulent. Then the credit reporting companies must tell any creditors who gave them fraudulent information that it resulted from identity theft. Creditors may not turn fraudulent debts over to debt collectors.
- Dispute information on your credit report — if you think it's fraudulent or inaccurate — with a credit reporting company. The credit reporting company must investigate your dispute and amend your report if you are right.
- In many states, you have the right to place a freeze on your credit report. A credit freeze makes it less likely that an identity thief could open a new account in your name.

The 3 nationwide credit reporting companies are:

Equifax	Experian	TransUnion
800-685-1111	888-397-3742	800-916-8800
www.equifax.com	www.experian.com	www.transunion.com

Communicating with Creditors and Debt Collectors

You have the right to:

- Stop creditors and debt collectors from reporting fraudulent accounts. After you give them a copy of a valid identity theft report, they may not report fraudulent accounts to the credit reporting companies.
- Get copies of documents related to the theft of your identity, like transaction records or applications for new accounts. You must include a copy of your police report and an identity theft affidavit with your written request to the company that has the documents. You can tell the company to give the documents to a specific law enforcement agency.
- Stop a debt collector from contacting you. In most cases, debt collectors must stop contacting you after you send them a letter telling them to stop.
- Get written information from a debt collector about a debt, including the name of the creditor and the amount you supposedly owe.

Limits on Financial Losses from Identity Theft

You have limited liability for fraudulent debts caused by identity theft. For example:

- Under most state laws you are not liable for any debt incurred on fraudulent new accounts opened in your name and without your permission.
- Your liability for fraudulent purchases made with your credit card is up to $50, if you tell the credit card company about the fraudulent charges within 60 days of when the company sends you the statement showing the fraudulent charges. Some credit card companies say cardholders who are victims of fraudulent charges have no liability for those charges at all.
- If your ATM or debit card is lost or stolen, your liability for the misuse of your card is up to $50, as long as you notify the bank or credit union within two business days after you realize the card is missing. Your liability may increase if you don't report the loss promptly.
- If fraudulent electronic withdrawals are made from your bank or credit union account but your ATM or debit card is not lost or stolen, you are not liable if you write to let the bank or credit union know about the error within 60 days of when they send you the account statement showing the fraudulent withdrawals.
- Most state laws limit your liability for fraudulent checks issued on your bank or credit union account if you notify the bank or credit union promptly.

Identity Theft Information for Taxpayers

Identity theft places a burden on its victims and presents a challenge to many businesses, organizations and governments, including the IRS. The IRS combats this crime with an aggressive strategy of prevention, detection and victim assistance.

What is tax-related identity theft?

Tax-related identity theft occurs when someone uses your stolen Social Security number (SSN) to file a tax return claiming a fraudulent refund. If you become a victim, we are committed to resolving your case as quickly as possible.

You may be unaware that this has happened until you e-file your return and discover that a return already has been filed using your SSN. Or, the IRS may send you a letter saying it has identified a suspicious return using your SSN.

Know the warning signs

Be alert to possible tax-related identity theft if you are contacted by the IRS about:

- More than one tax return was filed for you,
- You owe additional tax, have a refund offset or have had collection actions taken against you for a year you did not file a tax return, or
- IRS records indicate you received wages or other income from an employer for whom you did not work.

Steps for victims of identity theft

If you are a victim of identity theft, the Federal Trade Commission recommends these steps:

- File a complaint with the FTC at identitytheft.gov.
- Contact one of the three major credit bureaus to place a 'fraud alert' on your credit records:
  - www.Equifax.com 1-888-766-0008
  - www.Experian.com 1-888-397-3742
  - www.TransUnion.com 1-800-680-7289
- Close any financial or credit accounts opened by identity thieves

If your SSN is compromised and you know or suspect you are a victim of tax-related identity theft, the IRS recommends these additional steps:

- Respond immediately to any IRS notice; call the number provided.
- Complete IRS Form 14039, *Identity Theft Affidavit*, if your e-file return rejects because of a duplicate filing under your SSN or you are instructed to do so. Use a fillable form at IRS.gov, print, then attach form to your paper return and mail according to instructions.
- Continue to pay your taxes and file your tax return, even if you must do so by paper.
- If you previously contacted the IRS and did not have a resolution, contact us for specialized assistance at 1-800-908-4490. We have teams available to assist.

More information is available at: IRS.gov/identitytheft or FTC's identitytheft.gov.

About data breaches and your taxes

Not all data breaches or computer hacks result in tax-related identity theft. It's important to know what type of personal information was stolen.

If you've been a victim of a data breach, keep in touch with the company to learn what it is doing to protect you and follow the "Steps for victims of identity theft." Data breach victims should submit a Form 14039, *Identity Theft Affidavit,* only if your Social Security number has been compromised and IRS has informed you that you may be a victim of tax-related identity theft or your e-file return was rejected as a duplicate.

How you can reduce your risk

Join efforts by the IRS, states and tax industry to protect your data. Taxes. Security. Together. We all have a role to play. Here's how you can help:

- Always use security software with firewall and anti-virus protections. Use strong passwords.
- Learn to recognize and avoid phishing emails, threatening calls and texts from thieves posing as legitimate organizations such as your bank, credit card companies and even the IRS.
- Do not click on links or download attachments from unknown or suspicious emails.
- Protect your personal data. Don't routinely carry your Social Security card, and make sure your tax records are secure.

See Publication 4524, *Security Awareness for Taxpayers* to learn more.

NOTE: The IRS does not initiate contact with taxpayers by email to request personal or financial information. This includes any type of electronic communication, such as text messages and social media channels.

Publication 5027 (Rev. 3-2017) Catalog Number 67495R Department of the Treasury **Internal Revenue Service** www.irs.gov

IRS IMPERSONATION SCAM

WARNING:

WHAT?

Individuals impersonating Internal Revenue Service (IRS) employees are making unsolicited threatening telephone calls to taxpayers. They use the threat of arrest to obtain money from victims by falsely representing that the victims owe back taxes or other fees. The perpetrators demand that the victims send them money via iTunes cards, other prepaid debit cards, money orders, or wire transfers from their banks.

WHO?

The perpetrators are individuals who falsely claim to be IRS employees and tell intended victims they owe taxes and must pay using an iTunes card, other pre-paid debit card, money order, or wire transfer. Some of them are in the United States; however, there is a strong international component to this crime as well.

WHEN/WHERE?

Since October 2013, TIGTA has received reports of these fraudulent calls in every State in the country. The perpetrators are calling with multiple caller IDs from around the world. The top five States with the most losses are: (1) California – more than $10 million; (2) New York – more than $4 million; (3) Texas – more than $4 million; (4) Illinois – more than $3 million; and (5) Florida – more than $2 million.[1]

WHAT TO DO?

First, hang up! Do not engage with these callers. If you owe Federal taxes, or think you might owe taxes, hang up and call the IRS at 800-829-1040. IRS workers can help you with your payment questions.

If you do not owe taxes, fill out the "IRS Impersonation scam" form on TIGTA's website, **www.tigta.gov** or call TIGTA at **800-366-4484**. You can also file a complaint with the Federal Trade Commission at www.FTC.gov. Add "IRS Telephone Scam" to the comments in your complaint.

ABOUT US

The Treasury Inspector General for Tax Administration (TIGTA) was established in 1999, as an independent agency that provides oversight of the IRS, and reports directly to the Treasury Secretary. We audit, investigate and inspect the IRS and the Federal tax system in order to ensure that the IRS is accountable for the trillions of dollars in revenue that it collects each year. We protect the integrity of the system and save taxpayers millions of dollars each year. For every dollar invested in TIGTA, taxpayers receive $168[2] in savings.

---

[1] Data are from Oct. 2013 to Nov. 1, 2016.

[2] TIGTA, *Overall Performance Report FY 2015* (September 15, 2015)

Identity Theft Victim Rights

Victim rights under Minnesota and federal law

Victim Rights Minnesota

In Minnesota, victims of identity theft have the right to ask that nationwide consumer reporting agencies place a "security freeze" on their credit file at no cost.

To do so, victims must send their request to each of the three nationwide credit reporting agencies along with a police report or police case number documenting identity theft. A security freeze prohibits the credit reporting agency from releasing a consumer's credit report or any information from it without the consumer's express authorization, with a few exceptions. Under Minnesota law, there is no cost to the victim of identity theft to make this request. Minn. Stat. § 13C.016.

For instructions on making your request, see Minnesota Identity Theft Freeze Law, an information sheet from the Minnesota Attorney General's Office, or Consumers Union Website.

In Minnesota, the victim's local law enforcement agency is required to take a report regardless of where the crime occurred.

Victims should file a police report with the law enforcement agency where they live. Under Minnesota law, your local law enforcement agency *must* take a report of identity theft even if the suspected perpetrator is located and/or the ID theft occurred in another jurisdiction. The law enforcement agency is required to provide the victim a copy of it. This report will be helpful for the victim to provide to creditors who want proof of the crime. That agency can begin an investigation or refer the case to another jurisdiction if the suspected crime was committed in a different jurisdiction. Minn. Stat. § 609.527, subd. 5.

In Minnesota, victims of identity theft are entitled to crime victim rights that accrue under Chapter 611A with an additional right to mandatory restitution.

In cases where the crime of identity theft is charged, victims are entitled to a mandatory restitution award of $1,000. In addition, victims have the ability to get free copies of court documents to aid in clearing up their personal credit and criminal histories without accumulating more costs. See Minn. Stat. § 609.527, subd. 4(b) .

Federal Laws

There are a number of federal laws that protect victims of identity theft. These laws are designed to assist victims in minimizing and repairing the harm done after being victimized. These laws address documenting the theft; obtaining information about fraudulent transactions, correcting inaccurate information, dealing with credit reporting companies, creditors, debt collectors, and merchants; and limiting financial losses caused by the theft.

To find out more:

Statement of Rights for Identity Theft Victims (brochure)
Identity Theft Victims' Statement of Rights (website)

IDENTITY THEFT RESOURCE CENTER (/index.php)
888.400.5530

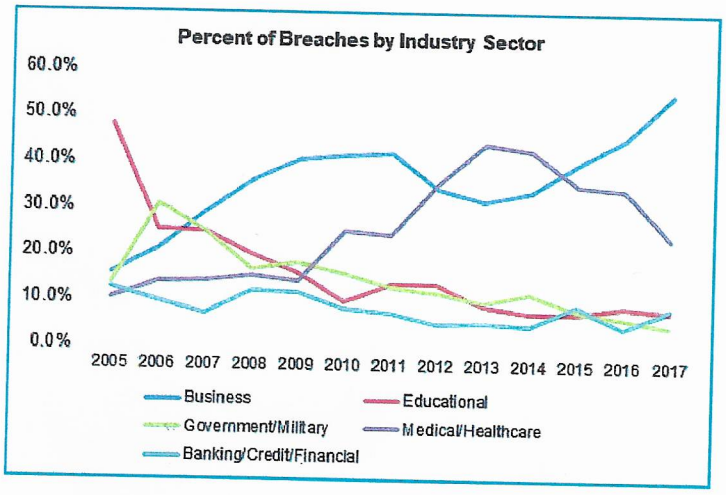
2017 Annual Data Breach Year-End Review (/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf)

Executive Summary

The number of U.S. data breach incidents tracked in 2017 hit a new record high of 1,579 breaches, according to the *2017 Data Breach Year-End Review (/images/breach/MultiYearOverview20052017.pdf)* released by the Identity Theft Resource Center (ITRC) and CyberScout. The Review indicates a drastic upturn of 44.7 percent increase over the record high figures reported for 2016.

"We've seen the number of identified breaches increase as a result of industries moving toward more transparency," said Eva Velasquez, president and CEO of the Identity Theft Resource Center. "We want to encourage businesses and government entities to continue to provide timely reports to their respective Attorney Generals so consumers can be better informed on what are the immediate and long-term impacts to their personal information by any given data breach."

Of the five industry sectors that the ITRC tracks, the business category again topped the ITRC's Data Breach List list for the third year in a row with 55 percent of the overall total number of breaches (870). This marks the eighth time since 2005 that the number of breaches for this sector has surpassed all other industries. The Medical/Healthcare industry followed in second place with 23.7 percent of the overall total number of breaches (374). The Banking/Credit/Financial sector rounds out the top three with 8.5 percent of the overall total (134). This is only the second time since 2005 that the Banking/Credit/Financial sector has ranked in the top three industry categories. (See multi-year summary) The remaining two sectors, Educational and Government/Military, represented 8 percent and 4.7 percent respectively.

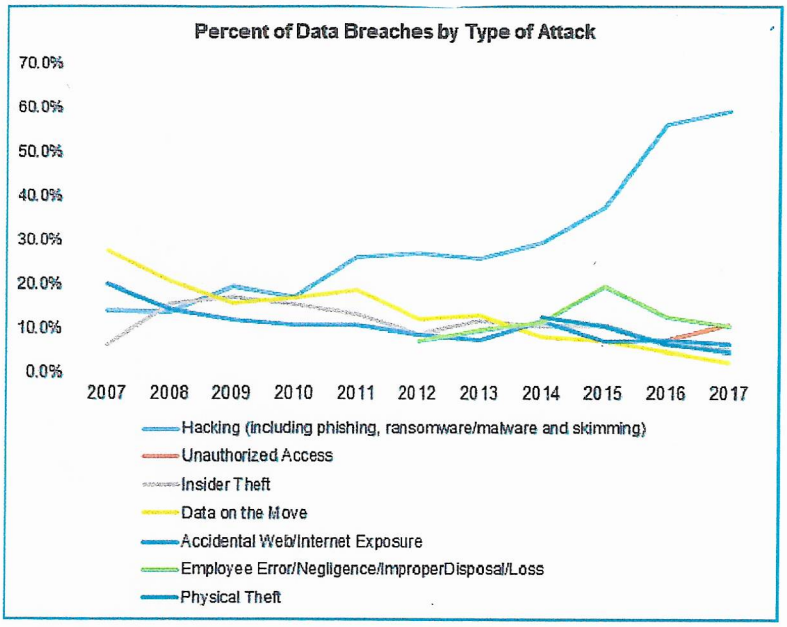


Hacking dwarfs all other methods of data compromise totaling almost 60% of all breaches

The method of exposure is a critical category when determining the level of harm potentially associated with a data breach. Hence, ITRC captures seven different types of attacks: hacking (with subcategories of phishing, ransomeware/malware and skimming), unauthorized access, insider theft, data on the move, accidental exposure, employee error/negligence/improper disposal/loss, and physical theft.

Hacking continues to rank highest in the type of attack, at 59.4 percent of the breaches, an increase of 3.2 percent over 2016 figures: Of the 940 breaches attributed to hacking, 21.4 percent involved phishing and 12.4 percent involved ransomware/malware. Unauthorized Access, which was newly added as a method of attack in 2016, represented nearly 11 percent of the overall total of breaches for a 3.4 percent increase over 2016 figures. Unauthorized Access is defined as breaches which involve some kind of access to the data but the publicly available breach notification letters do not explicitly include the term hacking.

Hacking incidents had signifigant impact on the Business sector this year, with nearly 40 percent of the breached businesses identifying this type of attack as the cause for the breach. On the other end of the spectrum, the Government/Military sector was far less impacted with only 1.3 percent of the total breach occurences being attributed to hacking.

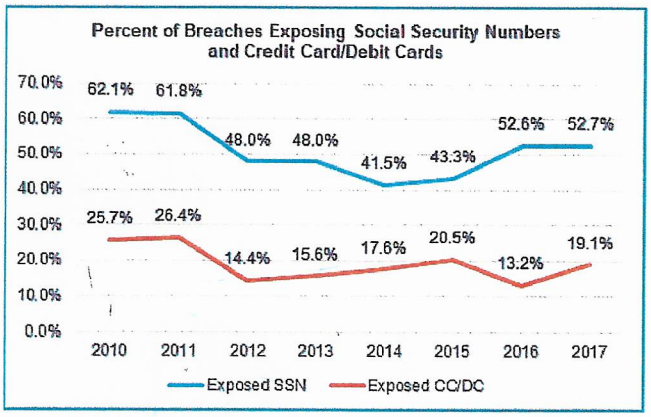


The Appeal of Credit and Debit Card Numbers Continues to Increase Year Over Year

Nearly 20 percent of breaches included credit and debit card information, a nearly 6 percent increase from last year. The actual number of records included in these breaches grew by a dramatic 88 percent over the figures we reported in 2016. Depsite efforts from all stakeholders to lessen the value of compromised credit/debit credentials, this information continues to be attractive and lucrative to thieves and hackers.

Social Security Numbers are even more widely available.

While the debate regarding the use of the Social Security Number as an authenticator continues, it must be called out that with multiple exposures of millions of SSNs they should no longer serve as a primary authenticator. Throughout 2017, there were 830 data breach incidents involving Social Security numbers, representing more than half of the total reported number of breaches. As a result of these breaches, nearly 158 million SSN's were exposed or 88 percent of the total number of records exposed.

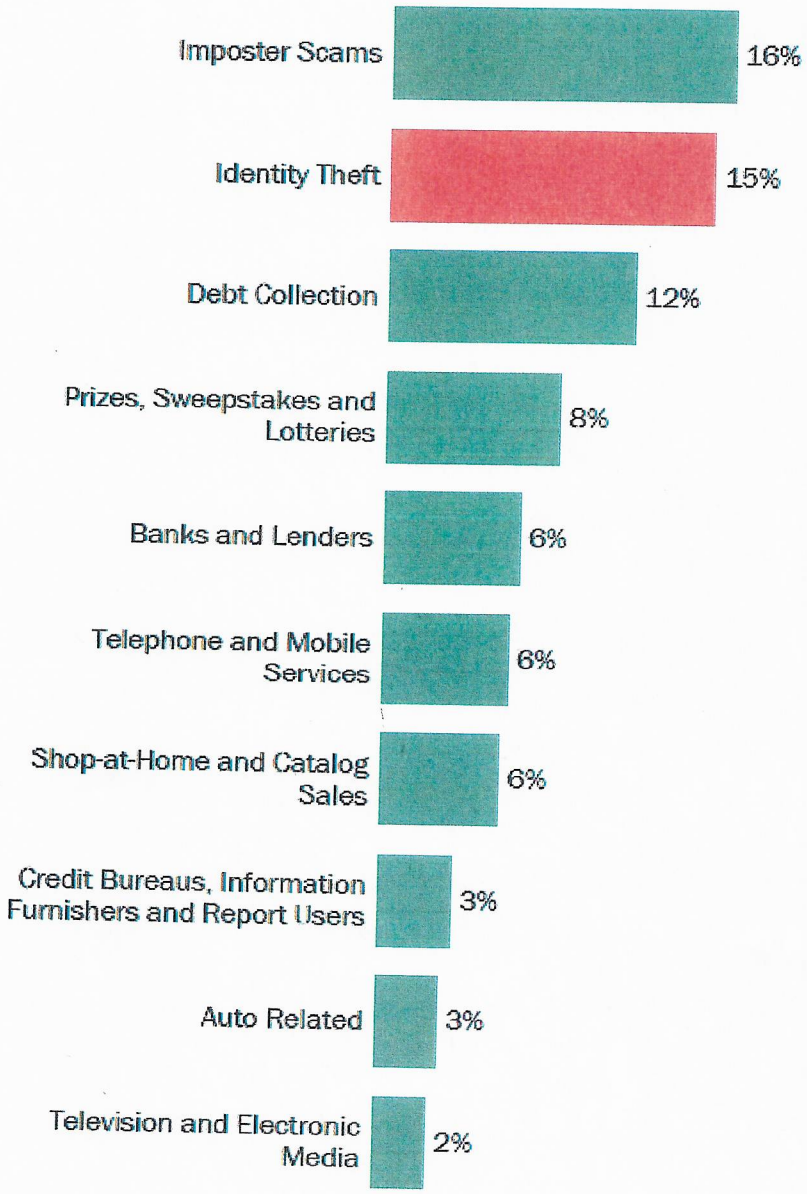


The number of exposed records in this report represents the minimum number and should be viewed as such. A signifigant percentage of the available data breach notification letters (36.7 percent) fail to include the number of exposed records, hence the ITRC's consistent call for more transparency and accuracy in notification letters. Progress is being made however, as this represents an improvement over 2016 when more than half the notifications did not include the number of exposed records.

"Understanding the type of personal information that has been exposed is absolutely critical for affected consumers. " said Karen Barney, Director of Program Support for the ITRC. "While a Social Security number continues to be the most valuable piece of information in the hands of a thief, even the exposure of emails, passwords or user names can be problematic as this information often plays a role in hacking and phishing attacks.

Consumer Sentinel Network Data Book 2017: Minnesota

Top Ten Report Categories

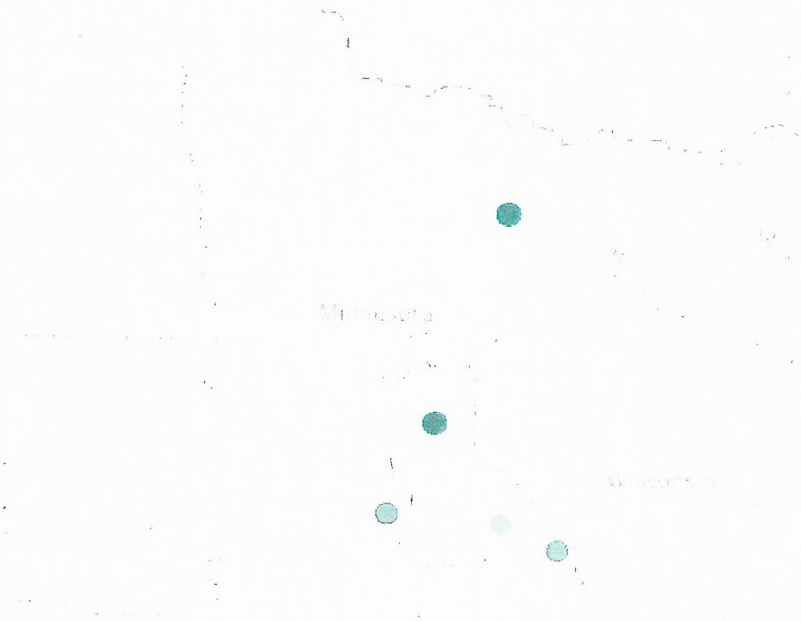


Fraud & Other Reports/Losses

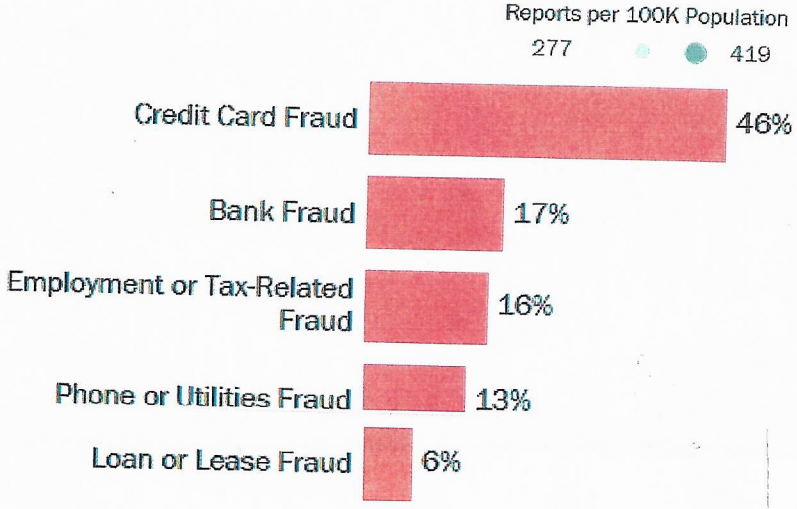
State Rank (Reports per 100K Population)	40th
Total Fraud & Other Reports	24,200
Total Fraud Losses	$10.1M
Median Fraud Loss	$495

Fraud & Other Reports By MSA

Download Metropolitan Statistical Area data [CSV, .93 KB]

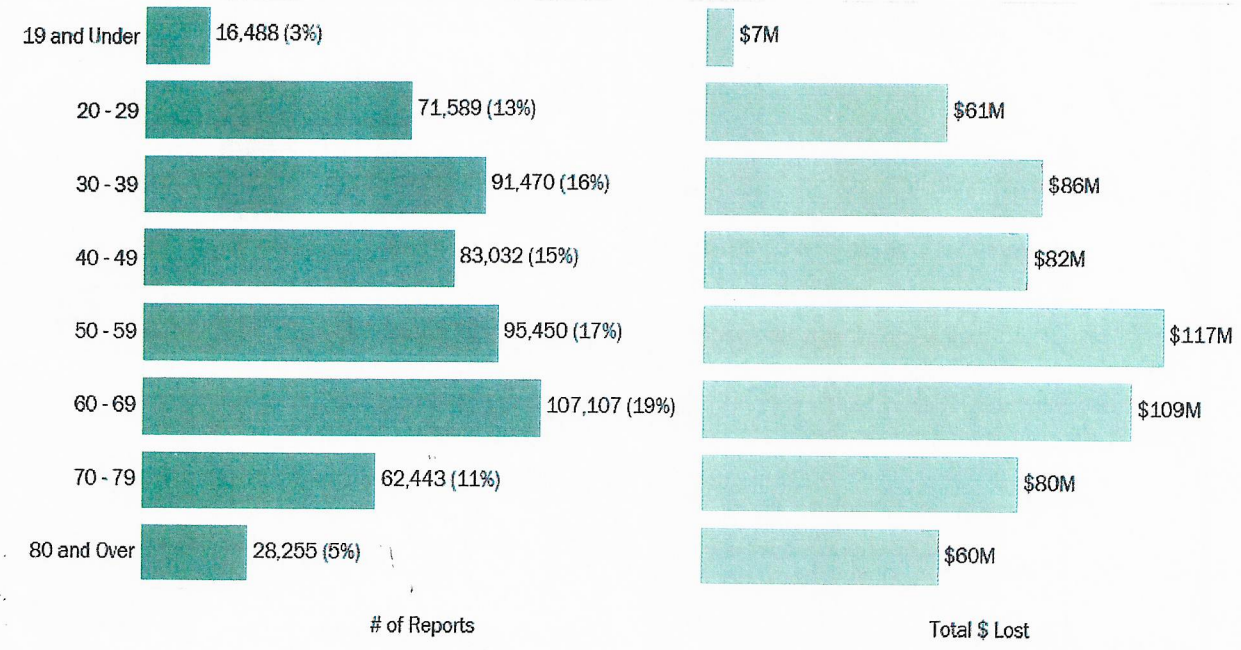


Top Identity Theft Types



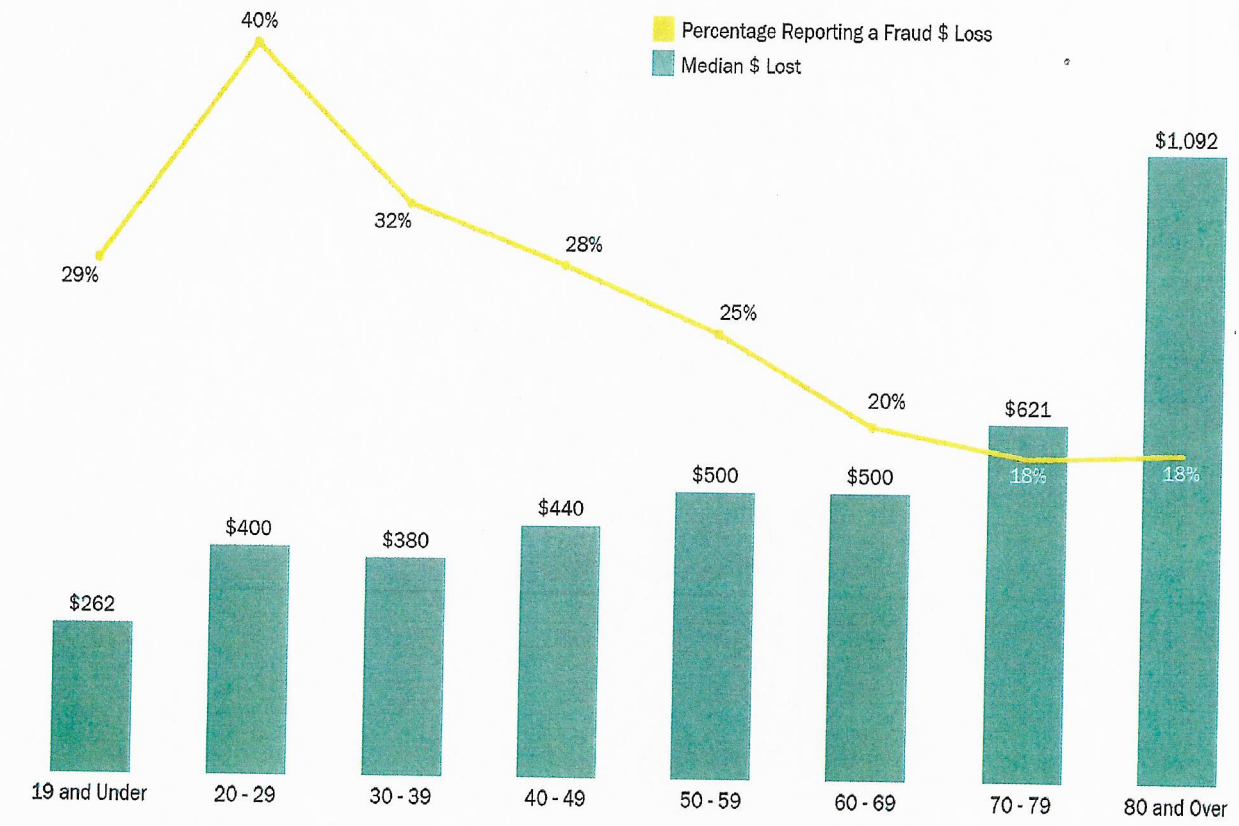
Consumer Sentinel Network Data Book 2017: Reported Frauds and Losses by Age, Percentage Reporting a Fraud Loss and Median Loss by Age

Report Frauds and Losses by Age



Percentages are based on the total number of 2017 fraud reports in which consumers provided their age: 555,834.

Percentage reporting a fraud loss and median loss by age



Of the 1,138,306 total fraud reports in 2017, 49% included consumer age information.