Identity Theft: Awareness Strategies to Protect Yourself

by Dianne Christensen and Bryce Jorgensen[1]

pubs.nmsu.edu • Cooperative Extension Service • Guide G-200

The College of Agricultural, Consumer and Environmental Sciences is an engine for economic and community development in New Mexico, improving the lives of New Mexicans through academic, research, and Extension programs.

New Mexico State University
aces.nmsu.edu

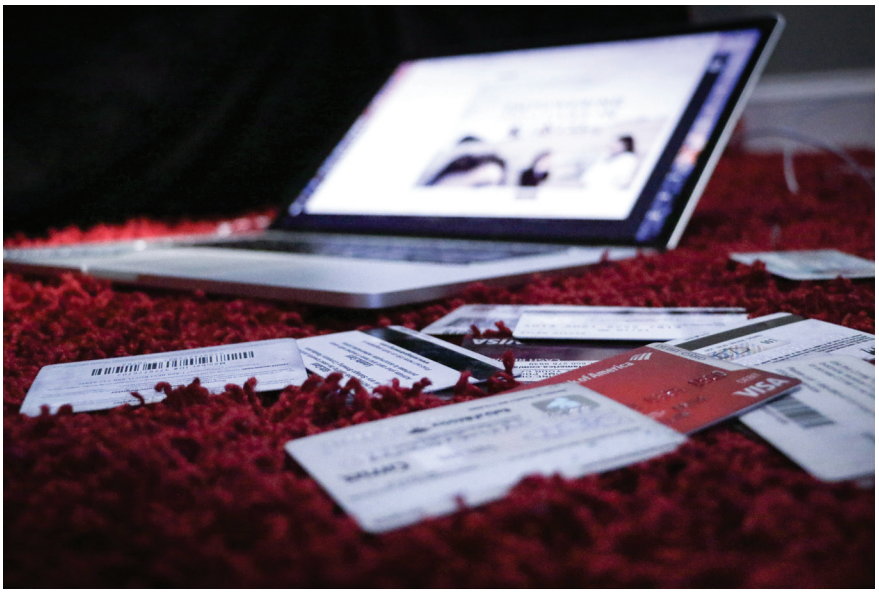

Photo by Dylan Gillis, 2020.

IDENTITY THEFT: AWARENESS STRATEGIES TO PROTECT YOURSELF

Identity theft is the deliberate act of obtaining and using another person's personal and financial information, without their consent, for fraudulent purposes. This can result in significant financial loss and have other long-term consequences. This publication will discuss the prevalence of identity theft, common ways it is done, and most importantly, how to protect yourself. Understanding identity theft is the first step in minimizing risk. The reality is no one can 100% prevent having their identity stolen but taking precautions and building secure information sharing habits can help protect you.

In 2024, there were more than 1.1 million reports of identity theft received through the Federal Trade Commission (FTC) website.[5] In a report sponsored by the Association of American Retired Persons (AARP), in 2023 identity theft cost Americans $43 billion. Approximately 15 million were victims of identity theft, much higher than the FTC figure because victims are reluctant to report these crimes.[6] Consumers aged 30-39 had the highest fraud reports in 2024 while seniors ages 80 and over had the highest median dollar amount lost.[2] The FTC provides data by state in its annual reports.[3,4] The top five states in 2020 for complaints were Georgia, Louisiana, Illinois, Kansas, and Rhode Island.[7] In 2024, New Mexico had 150 identity theft reports per 100K in population ranking relatively low nationally.[3]

[1]Respectively, Associate Professor and Bernalillo County Extension Family and Consumer Sciences Agent; and Associate Professor and Extension Family Resource Management Specialist. New Mexico State University.

Awareness is the Key to Protection

Everyone is at risk when sharing any personal information in public places, but knowledge is power and being aware of ways to protect yourself will lessen your exposure to identity theft. Develop good habits on how much information you share, where, and with whom to develop strong personal protection strategies.

An identity thief is looking for information that will help give access to personal accounts that will benefit them in committing fraud such as:

- Full Legal Name
- Social Security Number
- Maiden Name (often used as a security question)
- Medical insurance card
- Date of birth

This information is then used illegally in many ways. A few examples are below.

- Obtain credit or credit cards from banks or retailers
- Steal money from victim's existing account
- Rent an apartment
- File bankruptcy
- Apply for loans
- Obtain a job
- Establish account with utilities
- Commit insurance fraud

Ways Your Identity is Stolen and Steps to Secure Personal Information

It is important to be aware of where and how identity theft occurs so you can create security habits to protect your private information.

The most common forms of identity theft:[1]

- SPAM/Unsolicited phone calls or email: Emails are sent by thieves to deceive you with false information and request your bank and personal information.

  Action Step: Do not provide sensitive information via email. If possible, look up independent of the information on the email and call the sender to verify the accuracy of any request and/or check the legitimacy of the sender. Legitimate companies generally do not request information via email. Resources to get rid of unwanted contacts are below:

  » For unwanted emails go to: https://www.optoutprescreen.com
  » For unwanted phone calls go to: https://www.donotcall.gov

- Mail Interception: A thief waits for sensitive mail to arrive in your mailbox and then steals it.

  Action Step: Be aware of when you are expecting bank records, tax refunds, and credit card statements. If they do not arrive, call the company. Consider paying bills online.

- ATM Skimming/ PIN Capturing: These are devices used on your bank's ATM. ATM skimming occurs when a thief places their own card reader device on top of the ATM's original card reader, which looks identical to one another (Figure 1). When you insert your bank's debit/credit card into the card reader, it will record all your bank card information. PIN capturing occurs when a thief uses an identical PIN number keyboard of an ATM and places it on top of the original keyboard and records your PIN number as you type it in (Figure 2).

  Action Step: Limit your ATM usage. Consider other ways to obtain cash or use apps to make cash transactions. If you need to use ATMs, discuss the ATM security measures in place with your bank.

- Phishing: Phishing occurs when someone claims a false identity to gain something from someone else, like money, affection and attention, medical records. An example might look like the following:

  "Hello, I am your great uncle from London. I understand we have never met before or you have never heard of me, but I helped raise your parents when they were little. I am struggling financially right now, but since we are family, would you send me $2,000 to the following bank account so that I can visit you and your family? I would love to visit your parents and surprise them."

  If you receive an email or letter like the above, delete it and don't send money.

Figure 1. ATM skimming. Photo courtesy of Giovanni Gagliardi, 2021.

Figure 2. PIN capturing. Photo courtesy of Eduardo Soares, 2020.

Action Step: Delete questionable emails. Also, never click on links or attachments in this type of email as doing so can provide sensitive data to thieves.

- Dumpster diving: Thieves access garbage cans to find sensitive information that was not shredded.

  Action Step: Shred sensitive documents and junk mail such as credit card applications sent to you.

- Shoulder surfing: This can occur as you look at sensitive and private accounts on your phone, computer, or you pull out your social security card in a public setting. A thief can walk by and look over your shoulder, taking a picture of your information.

  Action Step: Do not access sensitive information in public places. If not at home, access it from your vehicle, a restroom, or other location where you are alone.

- Employees Theft: Employees can take your debit/credit card when you purchase something in their store. When you are not looking, they can write down your card number and security code of the card.

  Action Step: If possible, watch who has your credit card at all times. Dine at reputable restaurants, where your card isn't removed for processing.

- Unsecure websites: There are websites set up with a virus that tracks your activity on your computer when you access unsecure sites. Then, as you access other websites and log in to other accounts, it will record your activity. Your activity is then sent to the person that encrypted the virus on your computer.

  Action Step: Be very careful about what websites you access and leave open on your computer. Secure websites have an 's' at the end of the https web address.

- Public Wi-Fi: Be careful where you connect to public Wi-Fi. A thief can install a Wi-Fi hotspot with a name leading you to believe it's trustworthy, but the thief uses a special software that captures the information you're sending out.

  Action Step: Use public Wi-Fi cautiously.

- Pickpocketing: This form of theft is still a very effective way to steal sensitive information you carry with you physically such as credit cards. This type of highly skilled theft often occurs in crowded places or with someone bumping into you.

  Action Step: In crowded places or while traveling keep your passports, credit cards, and cash in more secure places like around your waist or your neck where it is not accessible to thieves.

Identity Theft with Taxes

Tax identity theft happens in many ways. Tax returns can be filed with a stolen social security number. Fraud can also occur when a thief claims another person's children as dependents, uses a deceased taxpayer's information, or earns wages under someone else's social security number.

Warning signs that you might be a victim of tax fraud include:

- Delay in receiving your refund.
- IRS notification stating you have duplicated tax filing.
- W2 or 1099 tax form from a company you're not aware of or expecting.
- IRS notification your dependents have been duplicated.

If you believe you are a victim of tax fraud, contact the IRS ID Theft Protection Specialized Unit at 800-908-4490. The specialists will help you with having your tax return filed legitimately and keep your account safe from future identity thieves. To reduce risk of tax fraud:

- File your taxes early in the season.
- Mail your tax return at the post office.
- Respond to mail from the IRS as soon as possible (Note: The IRS will ONLY contact you through mail. They will not contact you through email, social media, or text.) For further information visit: ftc.gov/taxidtheft

Minimize Identity Theft Exposure in Public Places

Look at current ways you share private information in public ways and consider changes that could increase your protection from identity theft.

Social Media: Review your social media accounts and look for things shared that might help a thief steal your identity. Thieves can get hints or answers to your security questions by looking at your profile. For an example, a security question could ask, "What was the name of your first pet?" Look at parent/sibling links which often provide personal information.

Mobile Phones: Phones do so much more today than make calls, such as banking and mobile wallets with many account options. Verify your phone is password protected so if a thief steals your phone they cannot access the information on it. You can also set up a "find my phone" account that allows you to see the location of your phone as well as reset it, thus protecting your private information.

Money Access Habits: Households that make more purchases, have more money in bank accounts, and often withdraw money from an ATM are at higher risk. Shop only on reliable internet sites and stores. Consider using alternative ways of accessing cash other than ATMs. Consider replacing the ways you used cash previously with more secure money transfer options that allow easy transfer of money to friends and family such as Venmo, Cash App, etc.

Easy Tips to Protect Yourself from Identity Theft

Implement these steps to build protection around your personal information.

- Install anti-virus software on your computer and your smart phone. It's important to treat your devices with care, especially if you store sensitive information on your computer and remain logged into websites such as banking or investment websites giving access to thieves.
- Create strong passwords and not things thieves could easily guess. Phrases are often helpful to remember but more difficult for thieves to guess than shorter passwords. Don't make your PIN numbers easy to guess such as "1234" or your birthdate. Change your passwords and PINs on a regular basis.
- Make note on your calendar when you are expecting important mail to come in. Follow up with companies if your bills don't arrive.
- Be cautious and do not click "save password" on public computers or any computer that does not belong to you. Always make sure to log out of your accounts when you are done using a computer or device that does not belong to you. Also, be careful where you open sensitive websites and type in security information. A thief could be looking at the computer screen and taking notes or a picture of your activity.
- Cross-shred sensitive documents making it almost impossible for a thief to put it back together after shredding.
- Review your credit report three times a year at AnnualCreditReport.com. You can use this site to get your credit report from the three major credit bureaus (one every 4 months): Equifax, Experian, and TransUnion. Children are 50 times more likely to be victims than adults because a child's identity is less likely to be monitored. Thieves often use the social security numbers of children to open new lines of credit. The fraud often goes undetected until the child reaches 18 years of age and tries to open their own credit lines. Monitor the credit reports of your children periodically.
- Do not give your social security number when you're applying for a job. You don't owe prospective employers that information until you receive the job.
- Do not carry your social security, passport, or birth certificate around with you unless you are using it. If you will not be using those documents, place them in a safe at home.
- Limit the cards you carry and don't give the thief a bigger opportunity to steal from you.

Reporting is Key to Limiting Your Loss

Reporting your identity theft loss needs to be done in a timely manner, generally within 60 days but the sooner the better. Credit cards and debit cards have different liability limits. Credit cards are generally more protected from identity theft loss than debit cards. If your credit card is lost or stolen, your liability is generally limited to $50, and in many cases, it could be zero with prompt reporting. Debit cards, on the other hand, carry more risk because the stolen funds are immediately deducted from your bank account. The liability for debit card fraud can escalate significantly, especially if you don't report the theft promptly. If you report your loss or theft of your debit card before there are unauthorized transactions, then you are not liable for any loss. Although, if you report the loss after there were unauthorized transactions, then your liability depends on how quickly you report it and bank policy. The table below shows generally how much you are liable for depending on how quickly you report. Check with your bank to learn more about their policies.

Debit Card Liability Time Limits

Table 1. Liability time limits for debit cards.

How Quickly You Report	Your Maximum Loss
Before any unauthorized charges are made.	$0
Within 2 business days after you learn about the loss or theft	$50
More than 2 business days after you learn about the loss or theft, but within 60 calendar days after your statement is sent to you.	$500
More than 60 calendar days after your statement is sent to you.	All the money taken from your ATM/debit card account, and possibly more; for example, money in accounts linked to your debit card account.

Check Your Credit Report Regularly

A key tool in being aware of theft is to request your credit report regularly. Under the Fair Credit Reporting Act, credit reporting agencies must provide you with any information in your credit file, upon your request, once a year. There are three credit bureaus where you can pull your credit report: Equifax, Experian, and TransUnion. You can check these credit reports at https://annualcreditreport.com free of charge. It is recommended you request an annual report from each company and do so alternating every four months so you can take advantage of the annual free report each one offers.

Identity Theft Monitoring Systems

Identity theft monitoring systems, like LifeLock, IdentityGuard, IdentityForce, or Experian Identity Theft Protection aim to protect individuals from identity theft by providing various monitoring and alert services. These services track activity across various databases, including credit reports, public records, and dark web sites, to detect suspicious activity that may indicate fraud or theft. These companies require a paid monthly service fee. Free credit monitoring services are also available with companies like Credit Karma, Credit Sesame, and Aura. These services will alert you when your score changes or someone is applying for new credit. They also show what is on your credit report and provide access to your Vantage credit score.

Services of Identity Theft Monitoring Systems

A variety of services are offered by these companies and there are advantages and disadvantages to consider.

- Credit Monitoring and Alerts: These services alert users when there are significant changes to their credit report, such as new accounts being opened, address changes, or credit inquiries. Early alerts can be helpful in spotting signs of identity theft.
- Fraud Detection and Resolution: LifeLock and other services offer fraud resolution services, including assistance in restoring stolen identities. This may involve working with creditors, the credit bureaus, and even law enforcement. However, this process can be time-consuming, and results are not always guaranteed.
- Dark Web Monitoring: Many services scan the dark web for stolen personal information like Social Security numbers, bank account details, and credit card numbers. This can give early warning signs of potential fraud.
- Protection Scope: LifeLock and similar services often offer protection for financial accounts, personal information, and social media accounts. However, they generally do not cover all forms of identity theft (such as medical or criminal identity theft), and you still need to monitor your own accounts actively.

Pros:

- Early Alerts: Timely notifications of suspicious activity can help you react quickly.
- Credit Score Monitoring: Many services include credit score tracking, so you can stay on top of any major changes.
- Identity Restoration Support: LifeLock offers support services if your identity is stolen, which can help you navigate the recovery process.

Cons:

- Limited Scope: No system can guarantee 100% protection, and these services often don't cover all types of identity theft.
- False Sense of Security: Some users may rely too much on these services and overlook other important precautions (e.g., strong passwords, safe online practices).
- Cost vs. Value: These services run from $9.99 to $29.99/month so evaluating the costs versus value is up to the individual. Being aware and practicing sound privacy habits may provide enough protection for many individuals.

Steps to Recover from Identity Theft

If you discover your identity has been stolen, there are steps to recover and repair the damage.

- Place an initial fraud alert on one of your credit reports. Then, the credit bureau you contacted must notify the other companies of your alert.
- Freeze or lock your credit. Both options limit who can access your credit, not allowing thieves to open any new accounts while you are trying to resolve the issues. Credit locks are typically done by credit monitoring companies and almost always have a fee. You can initiate a credit freeze with one or all the major credit reporting bureaus without paying a fee as it is governed by U.S. Law. Once your credit is frozen, companies are unable to view your credit file blocking any new loans. However, if you want to borrow money, you must remove the freeze to do so.
- Request your credit reports to be able to notify the police, the debt collectors, and businesses which accounts were not opened by you.
- Create an identity theft report that will help you deal with the credit reporting companies, debt collectors, and businesses of the opened accounts in your name.
  - » Submit a complaint to the Federal Trade Commission.
  - » File a police report.
  - » Attach both these documents and this will be your identity theft report.

Don't Live in Fear, Be Aware

Identity theft is a serious issue for consumers. By using the strategies and tips presented in this publication, you have taken the first important steps to being aware and protecting yourself from this threat.

RESOURCES:

Federal Trade Commission (FTC): The FTC offers helpful advice on identity theft prevention, warning consumers about monitoring services and pointing out the limitations of monitoring services. FTC Identity Theft Resources https://www.identitytheft.gov.

Other resources recommended for further reading:

- Anderson, G.O. (2014). *Identity Theft: Who's At Risk?* American Association of Retired Persons (AARP). https://www.aarp.org/pri/topics/work-finances-retirement/fraud-consumer-protection/identity-theft-incidence-risk-behaviors/
- Budd, K. (2019). *Identity Theft and Fraud Can Be Devastating*. Here's How to Avoid It. American Association of Retired Persons (AARP). https://www.aarp.org/money/scams-fraud/identity-theft/
- Federal Trade Commission (FTC). (2025). *New FTC Data Shows a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024*. https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024
- Federal Trade Commission (FTC). (n.d.). *Identity Theft*. https://www.ftc.gov/news-events/topics/identity-theft

REFERENCES

1. Consumer Affairs. (2024). U.S. *Identity Theft Statistics 2025*. https://www.consumeraffairs.com/finance/identity-theft-statistics.html
2. Federal Trade Commission (FTC). (2024). *Age and Fraud. Tableau Public*. https://public.tableau.com/app/profile/federal.trade.commission/viz/AgeandFraud/Infographic
3. Federal Trade Commission (FTC). (2024). *Fraud and ID Theft Maps*. Tableau Public. https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudandIDTheftMaps/IDTheftbyState
4. Federal Trade Commission (FTC). (2024). *Fraud Reports*. Tableau Public. https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts
5. Federal Trade Commission. (n.d.). *Identity Theft*. https://www.identitytheft.gov/
6. Ianzito, C. (2024). *Identity Fraud Cost Americans $43 Billion in 2023*. American Association of Retired Persons (AARP). https://www.aarp.org/money/scams-fraud/identity-fraud-report-2024/
7. McAfee. (2025). *A Guide to Identity Theft Statistics for 2025*. https://www.mcafee.com/learn/a-guide-to-identity-theft-statistics/

Dianne Christensen is an Associate Professor at New Mexico State University and serves with Bernalillo County Cooperative Extension Service as the Family and Consumer Sciences Agent. She is passionate about wellness and assisting others to discover ways to craft healthy lifestyles that work in their unique lives. She serves on the national board for the National Extension Association of Family and Consumer Sciences. Locally, she serves on the board for the New Mexico Diabetes Advisory Council and sits on the Health Advisory Council for Roadrunner Food Bank.

Bryce Jorgensen is an Associate Professor and Extension Family Resource Management Specialist at NMSU. He earned his Ph.D. at Virginia Tech. As a consultant, trainer, author, and speaker, he focuses on achieving individual, relational, and financial wellness for New Mexicans. An expert in the psychology of change, mindset, and behavioral economics, he provides customized programs leading to life and financial success.

March 2025 **Las Cruces, NM**