# The Very Real Risk of Identity Theft

By James LaPiedra and Jeffrey A. Kerman

## Get Educated, Not Overwhelmed

When it comes to identity theft, ignorance does not equal bliss. What you don't know can damage your reputation, jeopardize your financial future, and even threaten your health. We can no longer afford to deny this very real threat and its potentially disastrous consequences. This is the first of a three-part series that provides the latest information on the current state of identity theft, the types of fraud to look out for, and next steps you can take to prevent, detect, and recover from identity fraud.

## Preparation Is Key

In this fast-paced, technology-driven world, identity thieves are devising increasingly innovative and complex strategies to obtain and misuse your personal information. This explosive epidemic demands new protective measures beyond the limited reach of credit monitoring services. New vulnerabilities mean we must be more proactive, vigilant, and self-reliant than ever. *Prepare or Repair—the choice is yours.*

## Identity Theft by the Numbers

According to the U.S. Department of Justice, *identity theft has officially surpassed drug trafficking as the number one crime in America*, with a new victim every two seconds. Identity theft costs victims billions of dollars, and hundreds of hours to correct. Given the number of large data breaches occurring regularly, and the massive scope of the recent Equifax breach—which compromised approximately 145 million personal records—it's not a matter of *if* you'll become a victim of identity theft, but *when*.

## *Theft* vs. *Fraud*: An Important Distinction

Identity **theft** is the act of illegally obtaining personal information. Identity **fraud** is the act or acts of using that information to commit crimes.

## What Constitutes Identity Theft?

The Identity Theft and Assumption Deterrence Act of 1998 states that identity theft takes place when: "a person knowingly transfers, possesses, or uses, without lawful authority, *a means of identification* of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law."

*Simply put, identity theft is:* A federal crime that occurs when a criminal steals your personal information with the intent of using it to assume your identity, commit fraud, and/or access your benefits.

The "means of identification" mentioned above can include: name, date of birth, social security number, driver's license number, official state or government issued identification number, alien registration number, passport number, employer identification number, or federal tax ID number; your unique biometric data—fingerprint, voiceprint, retina or iris image—or other unique physical representation; your unique electronic identification number, address, or routing code; telecommunication identifying information or access device (this includes any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used to obtain money, goods, or services or to initiate a transfer of funds, other than a transfer originated solely by paper instrument).

In this digital age, we're known by our *personally identifiable information* or *PII* —name, address, phone number, driver's license number, social security number, ATM PIN, and credit or debit card numbers. These key identifiers are vital access points to our accounts and privileges. They can all be used to distinguish and trace an individual's identity—and they're prime targets for thieves to commit fraud.

---

**James LaPiedra** is the president and CEO of ID360°, an identity theft risk management and recovery provider. He holds the Certified Identity Theft Risk Management Specialist (CITRMS®) designation, and frequently speaks at identity theft seminars and workshops. Jim is the author of IDENTITY LOCKDOWN: Your Step-By-Step Guide to Identity Theft Protection. He is also a CERTIFIED FINANCIAL PLANNER™ focusing on retirement and distribution strategies. Jim earned a BBA in accounting from St. John's University and holds general securities and investment adviser representative licenses, as well as life, accident, and health insurance licenses. He is a highly decorated veteran of the New York City Police Department, where he served as the commander of several investigative and patrol units before retiring as a deputy inspector. **Jeffrey A. Kerman,** JD, CWS is an independent financial advisor who enjoys working with his clients and listening to their unique stories. As the Senior Managing Director of Wealth Partners Advisors LLC, Jeff focuses on combining the estate planning, financial, investments, insurance, tax and business planning processes for people who want more confidence and satisfaction in their financial matters. Jeff has spoken and published articles on various financial, investment, and retirement planning topics for the New York State Bar Association. He recently presented on "The Financial Elements of Retirement Income Planning" to the Senior Lawyers Section at the 2017 NYSBA Annual Conference, and he holds the Certified Identity Theft Risk Management Specialist (CITRMS®) designation.

## How Thieves Can Steal Your Identity

Fraudulent activity ranges from low-tech to highly advanced schemes that require special skills. Here's a brief overview of the most common methods used today:

**On the street:** Thieves know that most people carry valuable items beyond cash. Your driver's license, credit and debit cards, and even your employment ID card are useful. Carrying anything beyond what's absolutely necessary that day puts you at risk.

**Pickpockets** target victims who have their guard down, or have "telegraphed" the location of their wallets, purses, and other valuables. Many work in teams, usually in highly trafficked areas. In a typical play, one distracts or directly engages the target by bumping him or initiating conversation, while the second removes the property.

**In your home**: Victims often leave themselves most vulnerable to theft where they feel the safest—in their own home. Leaving sensitive PII like financial statements, tax records, birth certificates, social security information, Medicare cards, and insurance policies unsecured makes you a prime target, not only for the burglar who enters illegally, but for those looking to capitalize on your trust (e.g., friends; relatives; nannies; health care, home improvement, and cleaning service employees).

*"Victims often leave themselves most vulnerable to theft where they feel the safest—in their own home."*

**From your mailbox**: Unsecured mailboxes are a hot target, typically stuffed with valuable PII (financial statements, insurance policies, credit card account information, personal records, and new checks). Pre-approved credit offers and convenience checks pose the greatest risk, since the victim isn't expecting them and might not even know if they're stolen.

**From public records**: Our biggest life events—birth, marriage, property ownership, criminal records, professional licenses, and death—are all part of public record and contain all an identity thief needs to commit fraud or assume someone's identity. Some public records have signatures that can be copied and transposed onto other documents. With the help of online tutorials, public records are relatively easy for thieves to search.

**Exploiting insider access:** Companies, government agencies, and organizations have a responsibility to protect the PII they collect, and while many have developed robust security policies and procedures to detect the misuse of sensitive information, insider access is still a big threat. Knowing these insiders have valuable information, thieves target and exploit them using bribery and/or extortion tactics. As we witnessed in the infamous NSA data leak, insiders can also steal records as an act of revenge or part of a misguided political agenda. Government agencies, businesses, hospitals, and schools have experienced insider thefts that exposed hundreds of millions of personal records.

**Social engineering** preys on our fears and our natural tendencies to trust and avoid confrontation. In these cases, thieves pretend or "pretext" to be a legitimate source before tricking you into sharing valuable information. "Scareware" schemes can include e-mails or pop-ups claiming that your computer or smartphone is infected with a virus. They then direct you to call a number for tech support or download a repair link, and once you do, a virus is installed with malware designed to capture files, usernames, and passwords to otherwise secure accounts. Thieves continue targeting the elderly in phone schemes by impersonating an official from the IRS, Social Security Administration, or a law enforcement agency, and using scare tactics to get them to provide personal information. Some even demand payment in the form of prepaid cards or wire transfers.

**Hacking** is an attempt to exploit vulnerabilities in an individual computer or network. Thieves then obtain personal information directly, or by paying other hackers for the information they've stolen. Hacking has evolved into a billion dollar global business. Perpetrators are often highly skilled experts who work alone, in teams, or even within government entities. The highly publicized hacking of Equifax, Target, NSA, Anthem Health, Facebook, JPMorgan and Citibank reflect just how vulnerable our personal information is these days.

**Dumpster diving** occurs when identity thieves rummage through residential and business trash, and even public garbage sites in search of information they can use to commit fraud or to assume another's identity. Dumpster divers also target discarded electronic devices that haven't been properly destroyed, knowing that most have internal hard drives that store valuable files and/or records of processed documents.

**Shoulder surfing** is the peering over one's shoulder as they enter passwords, PINS, or access codes on a computer, ATM machine, or point-of-sale terminal. Advanced techniques capture your information using hidden cameras mounted above the keypad.

**Skimming** is when thieves use a small electronic device to scan and store the information on your credit or debit card's magnetic strip. These devices have been used by restaurant and sales staff at point-of-sale terminals. Skimming devices are also placed over card receptacles at ATMs and gas station pumps. The information is then used to commit fraud or is sold to other thieves. It's important to note that while the new EMV smart chip cards are a positive step, the magnetic strip with your personal information can still be skimmed.

## Types of Identity Fraud

Many believe that identity theft is mostly limited to bank accounts and credit card fraud, but non-financial identity theft is increasing at an alarming rate.

**Financial identity theft** occurs when a thief unlawfully obtains your unique PII and uses that information to commit financially-driven fraud. Thieves use your information to open new credit or checking accounts, take out loans, access existing bank and brokerage accounts, and even take out mortgages. They may max out or even deplete existing accounts. Even if you're not held liable for the activity, you are left with the daunting task of correcting it and trying to reclaim your financial reputation. From the perspective of creditors, you're required to prove your innocence. This task—known as *recovery*—is both time-consuming and stressful. While it's the most commonly known, financial fraud comprises only one-fourth to one-third of all ID theft cases. With *non-financial ID theft*, there are other driving factors, like disguising one's identity.

**Criminal identity theft** occurs when a victim's PII is misused during a contact with law enforcement. This can have devastating consequences for the victim, like having incorrect criminal records and even being improperly arrested. Others are fired or denied employment. This type of ID misuse is very hard to resolve and likely requires legal representation. According to the US Federal Trade Commission, approximately 12 percent of ID theft victims spend time correcting false criminal records.

**Social security number ID theft and misuse** happens in most ID theft cases, since that number is linked to credit cards, bank and brokerage accounts, government service programs, health insurance, and in some states, even your driver's license number. The *financial misuse* of a victim's SSN to compromise bank and credit accounts, brokerage accounts, insurance policies, etc., constitutes financial fraud. *Non-financial misuse* occurs when a thief applies for and receives social security, unemployment, Medicare, housing subsidies, or other government benefits. The thief can also obtain employment and avoid paying taxes with a victim's SSN.

**Tax return fraud** is becoming one of the fastest-growing crimes involving social security number misuse. Given the ease of electronic filing, approximately 140 million returns are filed electronically each year, allowing an easy method of filing fraudulent returns. Identity tax fraud has resulted in more than $5.8 billion in fraudulent payments since 2013, according to the General Accounting Office (GAO). In addition, the IRS estimates that over 750,000 false tax returns were filed in 2016.

**Driver's license and identification theft** is increasingly common since your driver's license or ID card number is the second most widely used identifier (after your SSN). Years ago, the most common cases of misuse were by teens trying to purchase alcohol or get into bars and clubs. Using the latest technology, thieves capitalize on system weaknesses to obtain these documents directly from the state's DMV office and make seemingly authentic licenses and identification cards. Armed with a driver's license bearing the victim's name and number, a thief can operate under the radar and ruin that person's driving record. Any driving offenses, suspended or revoked privileges, charges of DWI/DUI, and outstanding warrants are now all linked to the victim. Those linked offenses can turn a routine traffic stop into a false arrest or even jail time for the victim. Resolution isn't possible until the victim's true identity can be verified, and most cases require the representation of an attorney at the victim's expense.

*"FACT: In 2012, the Minnesota Department of Vehicle Services found that upwards of 23,705 licenses were most likely fraudulently obtained."*

**FACT:** In 2012, the Minnesota Department of Vehicle Services found that upwards of 23,705 licenses were most likely fraudulently obtained. In some cases, drivers are first discovering fraudulent activity after renewing their license through the mail and getting a card with someone else's picture on it.

**Medical identity theft** is a dangerous and potentially deadly form of identity fraud where thieves utilize a victim's information to obtain medical treatment, prescription drugs, and even surgery. The costs can range from several hundred to more than a million dollars per incident. Beyond the financial threat is that of erroneous medical files or the misinformation added to existing ones. False blood type, history of drug or alcohol abuse, test results, or diagnoses can lead to improper treatment, injury, illness, and even death. Medical records are extremely difficult to correct, and unfortunately, victims

of medical ID theft aren't extended the same rights and protections as victims of financial ID theft. Files are often shared with other entities—co-providers, insurance carriers, medical billing centers, hospitals, and pharmacies—making it nearly impossible to correct the information on such a wide span of networks.

**Identity cloning** is when the thief literally takes the victim's identity as his/her own, usually in an effort to conceal his/her own identity. All forms of identification are created using the victim's information, creating a duplicate of the victim's identity. Criminals use cloned identities to operate under the radar. The victim is then faced with correcting fraudulent activity and duplicate files maintained by creditors and government agencies.

**Child identity theft** occurs when thieves use a minor's social security number to commit fraud. Most children get their SSN's at birth and don't have credit histories until they're adults, so not only is their identity a clean slate, but the probability of detecting fraud is low. Thieves can establish lines of credit, obtain driver's licenses, or even buy a house with the child's identity, and by the time it's discovered, it may be too late for complete restoration. The impacts on the child's future are profound, threatening his or her chance of securing a student loan, a place to live, and even employment.

### Knowing More Means You're Less Likely to Become a Victim

With a newfound awareness and deeper understanding of identity fraud in its many forms, you can now begin to imagine the scope, scale, and consequences. Victims often feel helpless navigating the daunting and complex maze of protocols and procedures to correct the compromise, but resources are available.

### Take Next Steps Now

In the coming months, we'll be sharing follow-up articles about what you can do to detect and recover from identity fraud. In the meantime, find out how to protect yourself by visiting the Federal Trade Commission at www.ftc.gov, or the Identity Theft Resource Center at www.idtheftcenter.org.