The Very Real Threat of Identity Theft: A Guide to Identity Recovery and Resolution—Part III

By James LaPiedra and Jeffrey A. Kerman

In this third and final article of our three-part identity theft protection series, we discuss the final phase of the identity security cycle, the recovery/resolution phase. As a friendly reminder, the first two articles identified the many forms of identity theft and the methods used by thieves to commit fraud, several measures to reduce the risk of identity theft, and how to be proactive in detecting this fraud. This recovery/resolution phase article will provide helpful guidance for disputing fraudulent claims, so that you can act quickly to greatly reduce the risk of becoming a victim.

Confronting a case of identity theft can be very challenging. Successful resolution requires the accurate and timely gathering, organization, tracking, and follow-up of information (often to multiple sources). Some cases may even require the specialized skills of an attorney, law enforcement professional, or company with services within the credit and/or identity fields. In all cases, your liability depends upon how quickly you act.

Outlined below are steps you can take if you suspect or discover fraudulent activity:

Taking Action

If you suspect fraud immediately contact the creditor and credit reporting agencies reporting the fraudulent activity.

In addition:

- Create a case folder containing all correspondence and supporting documentation.
- On the inside cover, attach a data sheet to conveniently and chronologically record all details.
- Include dates, times, types of communication (e.g., notification, follow-up), the names of company representatives with whom you've communicated, and in-depth descriptions and notes of all your discussions.

Disputing ATM, Debit Card, and Credit Card Transactions

The **Electronic Fund Transfer Act (EFTA)** highlights your rights and responsibilities regarding ATM and debit card fraud transactions. The **Fair Credit Billing Act (FBCA)** highlights your rights and responsibilities regarding credit card fraud transactions.

The following are several examples of billing errors under the **FCBA**:

- charges not actually made by the consumer
- charges in the wrong amount
- charges for goods or services not received by the consumer
- charges for goods not delivered as agreed
- charges for goods that were damaged on delivery
- failures to properly reflect payments or credits to an account
- calculation errors
- charges that the consumer wants clarified or requests proof of
- statements mailed to the wrong address.

If you detect unauthorized or fraudulent transactions involving your ATM, debit, or credit card, immediately report it to the issuer's fraud department. You must follow up your phone notification with a written letter detailing the disputed transactions. Keep the originals of all correspondence, and send copies to the address provided for ***billing*** inquiries, ***not*** the ***address for payments***. This

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™ specializing in 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. Please feel free to check out the co-author's identity services at www.id360.com. **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 the business planning processes for people who want more confidence and satisfaction in their financial matters. He helps clients align their values and goals into a rational financial and life Plan. 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. Please feel free to check out the co-author's financial services at www.wealthpartnersadvisors.com.

notice must be mailed within 60 days of the date you received the first statement concerning the fraudulent charge.

Many major credit card issuers promote "*zero liability*" for fraudulent transactions involving their ATM or debit cards. There are exceptions, however—most are noted in the fine print of your cardholder agreement. This is why it's imperative to monitor your account regularly, and report suspicious activity and lost or stolen cards. If lost or stolen cards are reported before any fraudulent transactions take place, you will not be held responsible for those that occur after your notification to the issuer.

You may be liable for unauthorized withdrawals generally with the following liability limits:

For debit/ATM cards:

- Loss is limited to $50 if institution is notified within two business days.
- Loss is limited to $500 if institution is notified between three and 60 days.
- Loss liability is unlimited if loss is *not r*eported within 60 business days.

For credit cards:

- Loss is limited to $50 if your credit card is used at the point of purchase.
- There is no liability if the purchase was made by phone or online.
- Loss liability is unlimited if loss is *not r*eported within 60 business days.

Once the issuing agency receives your notification, it has 10 days to investigate and must notify you within three days of completing its investigation. If the investigation reveals an error or fraud, the issuer must correct the records and replace the funds within one day. If the issuer needs additional time to complete its investigation, the ***EFTA*** allows another 45 days—provided the issuer replaces the disputed funds, and notifies the consumer that the funds have been credited to his or her account.

If, at the conclusion of the investigation, the issuer determines that no error or fraud has occurred, the issuer can withdraw the credited funds and notify the consumer with a written explanation of its findings. Visit the Federal Trade Commission (FTC) site at **ftc.gov** for more information on your credit account consumer rights.

Disputing Information on Your Credit Report

Under the **Fair Credit Reporting Act (FCRA)**, both the credit bureau (e.g., Equifax) and the business that sent the information (e.g., your bank or credit card company) are responsible for correcting fraudulent or inaccurate information in your report.

To dispute inaccurate or fraudulent information, notify, **in writing**, all three credit bureaus and any companies or creditors whose information is in question. **Be sure to send all correspondence via certified mail, return receipt requested.** This provides a record that the correspondence was actually delivered.

This notification should include the following items:

- a detailed description of the account information and why you believe it to be inaccurate, along with copies of any additional supporting documentation;
- the unique **reference number** appearing on your credit report;
- copies of identification for verification; and
- an identity theft report (if you believe the information disputed is fraudulent).

An **identity theft report** is an extensive police report with enough detail for credit reporting agencies and businesses to verify that you are in fact a victim of identity theft, and to determine which inaccurate account information is a result of that theft. It facilitates your rights in the Recovery process.

Creating Your Identity Theft Report

1. File a complaint report with the *FTC* detailing the events of the theft. Once you write and print those details, an **identity theft affidavit** is created. It is a document critical to reporting and resolving fraudulent accounts. The identity theft affidavit includes general information about yourself, the theft, and the account(s) opened or affected in your name.
2. Bring your FTC identity theft affidavit with you when you file a police report.
3. Together, your FTC identity theft affidavit, and your police report make up an **identity theft report**. Be sure to get a copy of the police report or the report number.

For various reasons, it's not uncommon for victims requesting a police report to get pushback from local law enforcement. Don't get discouraged. Some people forget that identity theft is a federal crime that should be treated as such. Be persistent and know that there are additional outlets you can pursue.

Any local, state, or federal law enforcement agency is obligated to take your police report. If you still encounter resistance, your state attorney general's office will take it. To locate your state attorney general's office visit **usa.gov/state-attorney-general.**

Information Blocking Process

The **information block** process is another way for identity theft victims to manage fraudulent information. Upon accepting your identity theft report, the credit

bureau has four business days to **block** the fraudulent information in question until it's resolved. Your report is still accessible, just not the information in dispute. Note that the credit bureau must notify you and the creditor in writing if it places the block in effect. It must also notify you if it refuses to place the block in effect.

Reinvestigation is a process designed to help consumers dispute credit report errors or inaccuracies. Contrary to how it sounds, it is actually the *initial* investigation that follows a dispute. Upon accepting a dispute notification from the consumer, the credit bureau is required to investigate. Each has its own procedure. The credit bureau must forward your notification, along with all supporting documents and information, to the company reporting the disputed information. The creditor must then investigate the matter and report its findings back to the credit bureau. This process usually takes about 30 days.

If the creditor finds the disputed information to be inaccurate or unverifiable, it must correct or remove that information and notify each of the national credit bureaus. Contact the agency that has reported the inaccurate information to determine its current procedure.

Criminal Violations

It's frightening to think someone could commit crimes in your name. Even more disturbing is the fact that you could get arrested for those offenses. Unfortunately, it's a very real threat. In most cases, thieves use fraudulent addresses, and it's only after the victim has a police contact—like a minor traffic infraction—that he or she becomes aware of the impersonation.

If you become aware of violations falsely committed in your name, contact your state Attorney General's office. Procedures for disputing and correcting criminal records vary from state to state. Contact the local law enforcement agency that filed the charges on the thief, and file a criminal complaint of impersonation. Request that the agency take your fingerprints, photograph, and copies of other identifying documents (your driver's license and passport).

Once your identity has been verified, the law enforcement agency and the local district attorney's office *should* issue some form of a clearance letter or, in the case of an arrest, a certificate of release. Monitor the investigation and confirm that any follow-up findings supporting your innocence are filed with the appropriate District Attorney's office and court. A criminal defense attorney may be required to help fully reconcile your status, and correct criminal records filed with prosecutors and law enforcement.

Driver's License ID Theft

- If you suspect that someone has illegally obtained a driver's license in your name, contact your state department or the Department of Motor Vehicles (DMV).
- Some states add fraud alerts to your file if you are a victim of identity theft.
- Request your driving record once a year from your state DMV office to proactively detect any fraudulent activity. Visit **dmv.org** to locate your local DMV office.

Medical Identity Theft

Medical identity theft occurs when someone uses your personal information without your knowledge or consent to obtain, or receive payment for, medical treatment, services, or goods. Victims of medical identity theft may find that their medical records are inaccurate, which can have a seriously negative impact on their ability to obtain proper medical care and insurance benefits.

- If you discover inaccurate information or suspect fraudulent activity in your medical records, immediately request that the health care provider amend the record.
- If the provider created the record in question, it *must* correct the inaccurate information.
- If the provider disagrees with your claim, submit your statement of disagreement in writing. This statement of disagreement *must* be added to your record.
- You can also exercise the following rights under federal law:
  - the right to request copies of your current medical files from each health care provider;
  - the right to have your medical records amended to remove inaccurate or incomplete information;
  - the right to an accounting of disclosures—a record of who has been given access to your medical records—from your health care providers and health insurers, which is very important in tracking down where inaccurate information may have been sent; and
  - the right to file a complaint with the Office of Civil Rights at the U.S. Department of Health and Human Services, if a health care provider does not comply with these rights. In addition, many hospitals have patient advocates who may be able to help you obtain medical records and access information. Review your rights in greater detail at the Department of Health & Human Services site at **HHS.gov**.

Genetic Material (DNA) Identity Theft

With the emergence and growing popularity of Genetic and DNA testing for ancestry purposes, people should be aware of having one's personal DNA compromised. Millions of people have used the direct-to-consumer ge-

netic tests. Many of these genetic test companies allow their customers to download files containing their personal genetic information. This has created several third-party services from other companies that source multiple databases of genetic information in order to conduct long-range family searches. The true effect of having this genetic personal information available for cross-referencing databases is still not known.

Law enforcement agencies are now utilizing these databases as a standard investigative tool to help solve crimes. A serial killer was caught earlier this year after eluding authorities for over 32 years when investigators used his crime scene DNA to conduct a long range family search using the available public genetic databases. It is vital that people understand the privacy rules for each of these genetic testing companies, and take measures to opt out of sharing their genetic information if they so desire. This area of genetic identity theft is likely to continue changing at a rapid pace, and should be watched for future identity protection measures as it evolves.

Phone Fraud

If you suspect that an account for phone service has been fraudulently opened in your name, contact the service provider immediately and cancel the account. Open a new account using a different PIN for access. If you experience any difficulty having the fraudulent charges removed by your service provider, the following agencies can assist you:

- For local service, contact your state's Public Utility Commission.
- For cellular phones and long distance, contact the Federal Communications Commission (FCC), at 1-888-CALL-FCC.

Mail Fraud

If you suspect mail theft or tampering, notify the U.S. Postal Inspection Service (USPIS) immediately and file a complaint. To locate your USPIS district office online visit **uspis.gov** or call your local post office.

Passport Fraud

If you believe your passport is lost, stolen, or used fraudulently, contact the U.S. Department of State (USDS) online visit **travel.state.gov.** When not traveling, secure your passport in a safe or secure file cabinet. When traveling, make a color copy of your passport's first page, and store it separately from the original in case it's ever lost or stolen on your trip. You can also scan and save a copy in an email or a cloud computing folder like Dropbox, which allows you to store virtual files online and access them from virtually anywhere by connecting to the online service if the original is lost or stolen.

Thefts of American tourist passports are on the rise. A U.S. passport is very valuable to a thief, or worse—a terrorist. Take extra precautions to secure your passport abroad and at home.

Identity Theft Insurance, Credit Monitoring and Recovery/Resolution Services

Before you choose **credit monitoring and recovery/resolution** services or **identity theft insurance,** understand that they often have significant limitations and that neither can fully protect you from becoming a victim. Many policies only cover nominal out-of-pocket expenses—photocopying documents, mailing correspondence, and filing fees relative to your case. Further limiting coverage are significant deductibles and maximum caps on reimbursements, which may require pre-approval by the insurance company.

Credit monitoring by itself is a limited form of protection that *cannot* protect against criminal, medical, Social Security, tax return, existing account, or synthetic identity fraud. Credit monitoring won't alert you if someone obtains employment, a driver's license, a birth certificate, a social security card, or other documents in your name. Try to use a reputable company offering a combination of these professional services to best protect your identity from theft.

Words of Caution

While some identity theft protection and credit monitoring services are legitimate, many are marketing companies skilled at selling fear and a false sense of security. Some businesses claiming to monitor all elements of your identity in "real time" and perform a full recovery if you become a victim. In actuality many of these companies have little to no security experience to back up their claims and actually help victims recover or resolve their identity theft issues.

Service agreements can be complicated and misleading. Get the details in writing, read the fine print, and know what you're paying for.

Conclusion

The goal of our three part identity theft article series has been to provide our readers with a real world overview of the many ways that our identities can be compromised. In a world where one's personally identifiable information is often left unprotected, the co-authors sought to create a powerful resource and guide for the protection, detection and recovery of identities. It is our hope that our three identity theft articles can be shared with many people to help educate and protect them from this growing and ever changing problem.