The Very Real Threat of Identity Theft: Measures for Risk Reduction and Detection—Part II

By James LaPiedra and Jeffrey A. Kerman

In the first article of our three-part series, we identified the many forms of identity theft and the methods used by thieves to commit fraud. In this second article, we discuss several measures to reduce the risk of identity theft, and how to be proactive in detecting this fraud. With this deeper understanding of the threat, people should be compelled to act. Unfortunately many don't. The reality is you cannot eliminate the risk of becoming a victim. However, you can greatly reduce your risk by taking the following simple preventive measures.

Risk Reduction Measures

Secure Your Sensitive Information

Inventory all your important legal, medical and financial documents and secure them in a fireproof safe. Secure certain original documents such as wills, trusts, life insurance policies, deeds, and titles in a safe deposit box at your bank and maintain back-up copies in your home safe. Far too often these documents are left unsecured, and anyone with access to your home would have access to them and the valuable information they contain.

Shred

Develop the habit of shredding all documents that contain personal information, as well as unsolicited credit offers and convenience checks you won't be using. Place your shredder where you normally open your mail, since the tendency is to just throw out the item if the shredder is located elsewhere in the house or office. Thieves definitely target paper in recyclable bags because of this known tendency.

Reduce What You Carry

Most people carry more than what they normally need in their wallet or purse thereby increasing their risk. Carry only the items you will need for the day. Limit your credit cards to one or two, and never carry your Social Security or Medicare card unless there is a specific need that day. Make photocopies of the items you carry in the event they are lost or stolen.

Opt-Out

Opting out of receiving unwanted solicitations is an empowering and proactive measure. It will greatly reduce the number of times your information is shared, which decreases your odds of becoming a victim. Since you're not expecting these unsolicited offerings, you won't notice them missing if they were stolen from your mailbox.

To opt-out visit: www.optoutprescreen.com.

Financial Statements

Contrary to common belief, electronic delivery of financial statements is safer then mail delivery. Going paperless will reduce your risk of mail theft. Also, companies that maintain your personal information (P.I.) are required to annually provide you with their privacy policy and how they share your information. You can opt-out of some forms of sharing similar to the opting out of prescreened offers. Refer to the privacy policy, or contact the company for their specific opt-out directions.

Social Security Number and Card

Always use an abundance of caution when providing your Social Security number or card. When asked to provide your Social Security number ask the following questions:

- Why do you need my Social Security number?
- How will my Social Security number be used?
- How do you protect my Social Security number from being stolen?
- What will happen if I don't give you my Social Security number?

Continued on page 22

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™ concentrating 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. **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 Meeting, and he holds the Certified Identity Theft Risk Management Specialist (CITRMS®) designation.

Identity Theft

Continued from page 18

Answers to these questions will help you decide if you want to share your Social Security number. Also, be aware that no government agency or legitimate business will contact you and request you to provide your Social Security number.

Protect your Mailbox

Identity thieves love mailboxes. This cannot be overstated. They know the mail you receive contains enormous opportunities to commit fraud: pre-approved credit offers, convenience checks, account statements, annuity and insurance documents, and other forms of personal identity. This is why we strongly recommend receiving your correspondence via email, or online business sites. Discontinuing hard mail greatly reduces your risk.

These additional measures will help protect your mailbox:

- If you continue to receive sensitive items by mail, purchase a locking mailbox with limited space for mail deposit.
- Discontinue use of roadside mailboxes, if possible. Have a secured mailbox at your front door instead.
- Retrieve your mail as close to delivery as possible each day.
- Have personal checks delivered to your bank and pick them up there.
- Have sensitive documents sent via FedEx or UPS, and requiring a signature.
- Mail sensitive documents at the post office during business hours. Do not use street mailboxes—not even the one in front of the post office. These mailboxes have been, and will continue to be, looted by identity thieves.
- Consider opening a Post Office Box to receive sensitive mailings.
- Monitor your mail. If expected statements and bills don't arrive, contact the sender to ascertain if fraud may be involved. If fraud is suspected, you will be able to take more timely remedial steps.

Protect Your Computer

- Keep your firewall turned on. A firewall is the first line of defense between your computer (and all the information stored on it), and the bad guys.
- Install and update antivirus software.
- Install and update your antispyware.
- Keep your operating system current. Computer operating systems routinely update their technology, and often include solutions to newly discovered security vulnerabilities. Updating to the latest version of your operating system is in your best interest.
- Be aware of what you download. Even the best antivirus protection software can be circumvented by malware embedded in email attachments, pop-ups, and music or video links. Before opening this kind of content, make sure that it's coming from a trusted site. Never open email attachments from someone you don't know.
- Turn off your computer when not in use.
- Back up the contents of your computer to an external hard drive regularly.
- Use a secure browser. You can determine whether or not you're using a secure browser by looking for the small lock icon next to the URL, or at the bottom of the webpage. Another way to determine if your communication is being securely transmitted is to check the URL scheme located in front of the web address—https:// is secure; http:// is not.
- Encrypt financial and personal information.
- Securely dispose of computers, printers, copiers, and fax machines. To securely dispose of these devices, be sure to wipe their hard drives of all information. You can purchase software, or bring the device to a trusted professional to perform this service. If you're not planning to donate the device, remove the hard drive and destroy it with a hammer before disposing. Destroy CDs, disks, and flash drives before disposing as well.
- Use strong passwords. Here are some dos and don'ts regarding passwords:
    - Don't underestimate the power of your passwords. Since most thieves can easily access and authenticate the more traditional forms of identification—Social Security numbers, account numbers, dates of birth, addresses, and most commonly used security questions—a strong password really raises the bar of effort required on their part. We liken using weak passwords to using a knotted rope to secure the front door of your home— it's neither wise, nor effective!
    - Do make passwords strong and unique for each account. They should be at least eight to 10 characters long and contain multiple character types (lowercase, uppercase, numbers, and special characters).
    - Don't store your passwords on a list under your keyboard or blotter, inside your top desk drawer, or on a sticky note stuck to your monitor.

- Don't create passwords using familiar or personal information like your date of birth, the last four digits of your Social Security number, nicknames, addresses, phone numbers, or the names of your children.
- Do change your passwords every 60 to 90 days.
- Don't use the auto-memory features of a Web browser to remember your username and password.

- Secure your wireless network. Enable Wi-Fi Protected Access 2 (WPA2) instead of Wired Encryption Privacy (WEP).
- Exercise caution when using public wireless hotspots or kiosks. Always use a private VPN to ensure your protection.
- Use security questions and dual authentication if available for additional access control.
- Be alert for phishing and pharming scams.

Protecting What You Know: Social Engineering

Some thieves are bold enough to steal your information right out in the open, employing tactics like charm, impersonation, flattery, and intimidation to manipulate you into revealing information you'd normally keep under lock and key. The most common types of social engineering are in-person, phone, email, and website. Here are some precautions to note:

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking for or trying to verify your personal information. If an unknown individual claims to be from a legitimate organization—such as the IRS, the Social Security Administration, or a company you do business with—try to verify his or her identity directly with the company.
- Don't enter information or use links embedded within an unsolicited email. Be aware of whom you are communicating with, and always verify.
- Never be pressured into releasing your personal information.
- With companies you do business with, have the representative confirm information that only legitimate employees of that company would know, such as the date of your last purchase, the type of account you have, or when it was opened. You can even lie about certain activity such as purchase and payment activity to see if the unsolicited caller falls for it.

In summary:

- If you didn't initiate the call, get their information and call or email them back.
- Stay in control of the phone call.
- Know whom you're talking to, and ask questions if you're unsure.
- Don't be paranoid; be aware!

Protecting the Deceased

If you're a relative of a recently deceased person, or the executor of an estate, the following steps will reduce the risk of your loved one's identity being used to commit fraud:

- Protect the Certificate of Death as if it were a Social Security card.
- Request at least 12 original copies of the Certificates of Death to show proof of death when closing down accounts.
- Request a credit report from each of the three credit reporting agencies. This will give you a list of accounts that may need to be closed.
- Request a flag to be placed on the deceased's file. It should read, "Deceased: do not issue credit."
- Indicate the person to be notified in the event someone attempts to open an account. This could be a surviving spouse, a family member, or the Executor of the estate.
- Notify the following institutions:
    - Social Security Administration
    - Insurance companies—auto, health, life, etc.
    - Veterans Administration—if the person was formerly a member of the military
    - Immigration Services—if the deceased was not a U.S. citizen
    - Department of Motor Vehicles—if the person had a driver's license or state ID card
    - Professional licensing agencies—bar association, trade certifications, medical associations, union affiliations, etc.
    - Membership programs—video rental, public library, fitness club, etc.

Credit Inquiries, Fraud Alerts, and Credit Freezes

Credit inquiries list all parties who have accessed your credit report within the past two years. There are two types of inquiries: hard inquiries and soft inquiries. Hard inquiries are those made by lenders who evaluate your information when you apply for credit. Soft inquiries are those made by lenders for promotional purposes. There are two types of fraud alerts: an initial alert and an extended alert.

Initial Fraud Alerts

- An initial fraud alert can be placed on your credit report if you're a victim of identity theft, or if you suspect you may become one (e.g., you've received collection notices for accounts you didn't open, or you've provided your Social Security number or other personal information to someone you now believe to be fraudulent).
- An initial fraud alert remains on your credit report for ninety (90) days, unless you request to remove it before that period.
- When an initial fraud alert is placed on your credit file, you're automatically "opted out" of pre-approved credit and insurance offers for a period of two years.
- You're also entitled to one free credit report from each of the three (3) major bureaus *in addition to* the standard one available every twelve months.
- Once the initial fraud alert is in place, creditors must use "reasonable policies and procedures" to verify your identity before issuing credit in your name (though these vary from creditor to creditor).

Extended Fraud Alerts

- You're allowed to place an extended fraud alert on your credit report if you are a victim of identity theft, and can provide an Identity Theft Report—the Identity Theft Complaint Report filed with the Federal Trade Commission, along with a police report.
- An extended fraud alert remains on your credit report for seven years unless you request removal during that period.
- Creditors are required to contact you when you have an extended fraud alert. Be sure to include your cell number in your contact information.
- With an extended fraud alert, you're entitled to two additional free credit reports within twelve months from all three major credit bureaus.
- The credit reporting agencies will remove your name from pre-screened credit offers for five years, unless you request to remain on their marketing lists.

What Is a Credit Freeze?

Most states have laws allowing you to restrict access to your credit report, also known as a credit freeze. This measure greatly reduces the chances of a thief opening a new account in your name.

- A credit freeze is something you can do *before* an identity thief strikes.
- When you freeze your credit reports, you are telling the three major consumer reporting companies to block access to your credit report and credit score.
- A freeze works because most businesses won't open new credit accounts without first checking the prospective consumer's credit history. So, once you place a freeze on your credit, new creditors will not be allowed access to your credit report. If your credit files are frozen, even someone who has stolen your Social Security number (or other personal identifying information) will have a hard time getting credit in your name.
- Companies you already do business with, and the collection agencies working with them, are still allowed access to your credit report so they can check your credit until your loan or business with them is resolved. Non-lenders like potential employers, insurance carriers, and landlords are also allowed access to your credit report in some states.
- Placing a freeze on your credit report does not prevent you from getting your free annual report, or obtaining your credit score.
- Most states allow identity theft victims to place credit freezes on their credit reports for free, and only charge a fee for unfreezing the report.
- Most states require a filing fee for non-victims to freeze and unfreeze their credit reports.
- You are allowed to temporarily or permanently unfreeze your credit report at any time. For example: Before applying for a credit card or a loan, unfreeze your credit report by providing each credit bureau with the PIN given to you at the time of the initial freeze. A fee is normally required for each agency to lift the credit freeze. There's also a fee to reactivate the freeze once you've completed the credit application process.

What Are the Limitations of Fraud Alerts and Credit Freezes?

Fraud alerts and credit freezes are valuable measures of protection, but they do have limitations:

- They can help keep an identity thief from opening new accounts in your name, but they won't stop a thief opening new accounts that don't require a credit check—a telephone, wireless, or bank account.
- They will not protect you against nonfinancial fraud—driver's license, criminal, and medical identity fraud.
- They will not protect you from someone compromising an existing account.

Detection of Identity Theft

As with most things, being your own advocate is the most powerful form of protection. Proactive self-detection is the most effective method of detecting fraud. Self-detection is the process by which consumers actively monitor their own financial and personal accounts. Those who engaged in this process are usually able to detect fraud faster than any external source. Early detection reduces the chance of further fraud and economic loss, in addition to reducing the time and expense needed to recover.

Individuals are afforded certain rights under the Fair Credit Reporting Act (FCRA) and the Fair and Accurate Transaction Act (FACTA). These laws provide you with the ability to receive a free copy of your credit file from credit bureaus and specialty consumer agencies that collect, store and sell your personal information.

Below you'll find information regarding various aspects of self-detection, and the most effective ways to monitor and detect irregularities and fraudulent activity. Consider taking these measures and monitoring your free credit reports as your annual "ID checkup."

Review Your Credit Report

Credit bureaus are companies that collect and compile detailed financial activities, credit ratings, and credit-related payment histories for every consumer in the country.

There are three main credit bureaus in the United States:

- Experian
- Equifax
- TransUnion

You are allowed one free copy of your credit report every 12 months.

To order your free report visit: www.annualcreditreport.com.

- **Innovis** is a fourth credit bureau that functions as more of a data broker, but due to the amount of data they collect, any requests made to the three main credit bureaus should be made to them as well.

To order your free Innovis credit report visit: www.innovis.com/personal/creditReport.

Monitor Your Monthly Account Statements

- At least once per month, review your bank, credit card, utility, brokerage, and annuity statements. As we've mentioned, electronic statements are the safest, most effective, and most efficient way to view activity and detect fraud. They also eliminate the threat of mail theft.
- Review each transaction and verify the legitimacy of all recoded activity. If you're receiving hard copies in the mail, consider scanning paper statements, storing them in encrypted files on your computer, and then shredding the paper statement.
- Account alerts have proven to be very effective in detecting fraudulent activity in real time. Most credit card companies provide alert services—via phone, email, text, or all three—to notify you when certain predetermined conditions are met. Alert conditions may include purchases above a certain amount, change requests, activity within certain time periods, or even general transactions. Utilize this feature on credit cards, checking accounts, and debit accounts. Some even offer the service for free—a sensible alternative to paying for credit monitoring on just one card.

Monitor Your Social Security Statements

- You should review your Social Security account statement every year to verify its accuracy. It provides your record of yearly earnings and your expected retirement and disability benefits. The Social Security Administration mails paper statements to workers age 60 and older three months before their birthday, and if they don't yet receive benefits and don't yet have a *my Social Security* Account.
- You should open an account with the Social Security Administration online so that you can access your information anytime. Visit: www.ssa.gov or call (800-772-1213).

Monitor Your Medical Reports

- For early detection of fraud, actively monitor your medical, insurance, and financial records. Unlike credit information that has a central repository with the credit bureaus, medical information is dispersed and maintained within many file systems and stored on numerous computers. This makes it extremely difficult, if not impossible, to locate and correct errors or fraudulent entries.
- According to the Federal Trade Commission (FTC), the following may be warning signs of medical identity theft:
    - You are contacted or receive bills for medical services you never got.
    - You see medical collection notices you don't recognize on your credit report.
    - You find unexplained office visits and treatments on the explanation of benefits statement from your health insurance company.

- You try to make a legitimate insurance claim and your health plan says you've reached your benefit limit.
- You're denied insurance because your medical records show a condition you don't have.

Monitor Your Explanation of Benefits (EOB) Statement

- Carefully read the Explanation of Benefits (EOB) statement sent by your health insurance company after treatment.
- Verify that the claims paid, names of providers, dates of service, and itemized list of treatments match what you or your family members received.

Monitor Your Medical Records

The Health Insurance Portability and Accountability Act's (HIPAA) Privacy, Security, and Breach Notification Rules help protect the privacy of your health information held by doctors, nurses, pharmacies, hospitals, clinics, nursing homes, health insurance companies, health maintenance organizations (HMOs), employer group health plans, and certain government programs that pay for health care, including Medicare and Medicaid.

- The provisions in the Act give you the right to obtain copies of your medical records maintained by health insurance companies and medical providers. Generally, once you submit your request, these providers are required to comply within 30 days.

Monitor Your Driver's License Record

- Although advanced security measures are taken to detect fraudulent driver's license applications, identity thieves are still able to obtain them with stolen identities. Becoming a victim could result in mounting tickets and even outstanding arrest warrants in your name.
- Monitor your driving record with your state's DMV. Links to each state's DMV can be found by visiting www.dmv.org. Be aware that states do charge a minimal fee for this request.

Monitor Specialty Consumer Reports

- A specialty consumer report is a non-credit report available to anyone inquiring about a consumer's background for decision-making purposes.
- These reports are compiled from thousands of public record databases across the country. These databases apply advanced algorithms to observe, record, and make inferences about your behavior. They contain the detailed personal information you've essentially generated since birth—insurance claims, residential and tenant history, criminal background, employment history, checking account history, email accounts, online purchases, credit applications, and employment and education history.
- Reviewing these reports annually is critical given all that they cover. You're entitled to one free copy every 12 months, just like your credit report. You also have the right to dispute inaccurate information.

LexisNexis is the largest private sector data warehouse in the United States, maintaining approximately 37 billion public and proprietary records. These records are compiled into specialty reports, and sold to businesses making decisions relative to background screening, employment and tenant history, and insurance underwriting. FACTA allows you one free copy of each report every 12 months. LexisNexis provides two specific reports containing personal information gathered from many different sources.

The first is the LexisNexis Accurint Person Report.

- It provides both public and non-public information—real estate title records, liens, death records, and motor vehicle registrations.
- Publicly available information is gathered from general public and non-government sources, such as newspapers, magazine articles, and telephone directories.
- Non-public information includes current and former addresses, Social Security numbers, previous names used—aliases, maiden names, and previous married names—as well as dates of birth and telephone numbers.

For instructions on how to order your report, visit www.lexisnexis.com/en-us/privacy/for-consumers/request-personal-information.page.

The second report is the LexisNexis Full File Disclosure Report.

- It contains your consumer file and a public records search that includes information available via county, state, and federal public records—real estate transactions and ownership information, liens, judgments, bankruptcy records, professional licenses, and previous addresses.
- Additional detailed information contained within your full file disclosure report are auto and personal property insurance claims history, current insurance carriers, pre-employment background checks, and criminal records.

For instructions on how to order your Full File Disclosure report visit https://personalreports.lexisnexis.com/index.jsp.

Check Verification and Checking Account Reports

To review information stored within the checking and deposit account databases, submit requests to the following two companies. Be prepared to provide your name, address, driver's license, and checking account numbers to view a sample checking account history report. This will allow you to check underwriting history and possibly uncover fraud.

- Certegy Check Services, Inc. Visit https://www.askcertegy.com/FACT.jsp.
- Chex Systems, Inc. Visit www.chexsystems.com.

Insurance Claims Reports

- These databases contain information on a consumer's five-year claims and payment history for auto, personal property, burglary, credit card theft, worker's compensation, and medical insurance. Knowing what's in these reports will help protect you against fraud as well as inaccuracies that could negatively impact your financial reputation.
- Insurance Services Offices, Inc. (ISO) is a Verisk-owned company that provides insurance claims information to insurance underwriters. Their report is called the Automobile-Property Loss Underwriting Service, or A-PLUS.
- Request a copy of your A-PLUS loss-history report and review its contents. Even if you haven't made any insurance claims in the past five years, a thief may have made claims with your identity. Your report will be mailed within 15 days. Visit ISO online at www.verisk.com or call 800-627-3487 to find the office serving your geographic area.

Resident History Reports

- Even if you don't rent or haven't rented in years, you should still review your resident history reports. Criminals use stolen identities to rent properties, resulting in fraudulent claims of vandalism, eviction, and unpaid rent. It may be some time before it shows up in your credit report, or before debt collection agencies show up at your door.
- Your LexisNexis residential history report is included in the Full File Disclosure report outlined above in the LexisNexis section of this article.
- CoreLogic SafeRent can also supply you with a copy of your tenant and rental history report.

To get your CoreLogic SafeRent report visit www.corelogic.com.

Medical Information Reports

The Medical Information Bureau (MIB) provides information to insurance underwriters about member companies requesting information on consumers, including the specific information requested and a consumer's insurance application history.

- The report discloses usage codes (related to medical conditions or treatments), not specific medical details. This information is maintained for seven years.
- Again, even if you haven't applied for insurance underwriting in the past seven years, you should not bypass this review. If you haven't applied and a record exists, it may be an indication of fraud.
- Request your report at the MIB website—www.mib.com/request_your_record.html or by calling 866-692-6901.

Take Next Steps Now

In the coming months we will share our third and final article on identity theft covering identity theft recovery and instructions for disputing fraudulent claims. In the meantime, in this article we have identified proven measures that you can use to greatly reduce your risk of becoming a victim, and several measures you can take for timely detection of suspicious activity. We encourage you to review both articles and take proactive action.