IDENTITY THEFT PREVENTION
SDPD Crime Prevention
December 12, 2016

CONTENTS

PROTECTING PERSONAL INFORMATION
- The Basics
- Using Credit, Debit, and ATM Cards
- Using Bank Checks
- Protecting Your Social Security Number
- Using the Mail
- Using an ATM
- Carrying Personal Information in a Purse or Wallet
- Securing Mobile Devices
- Protecting Your U.S. Passport
- Going Away on an Extended Trip
- Making It Harder for Hackers

PROTECTING YOUR CHILD'S IDENTITY
PROTECTING A DECEASED'S IDENTITY
BUYING IDENTITY THEFT PROTECTION
USING A TAX PREPARER
CHECKING FOR POSSIBLE IDENTITY THEFT
IF YOU BELIEVE YOU MAY BECOME VICTIM
IF YOU BECOME A VICTIM
IF YOU ARE NOTIFIED OF A SECURITY BREACH INVOLVING PERSONAL INFORMATION

Every person who willfully obtains personal identifying information, e.g., name, address, date of birth, Social Security Number (SSN), mother's maiden name, etc. as defined in Cal. Penal Code Sec. 530.5(b), and uses that information for any unlawful purpose is guilty of a public offense. Identity theft is the fastest growing crime in the United States. Every year about 15 million people become victims. Everyone is vulnerable. Skilled identity thieves use a variety of methods to steal your personal information. These include the following:

- Dumpster diving. They rummage through trash looking for bills and other paper with your personal information on it.
- Skimming. They steal credit- or debit-card numbers with a special storage device when processing your card.
- Phishing, Spear Phishing, Smishing, Vishing, and Whaling. These are defined and tips for dealing with them are suggested in the section on Internet Fraud and Other Crimes in the paper entitled Cyber Security on the Prevention Tips page of the SDPD website at **www.sandiego.gov/police/services/prevention/tips**.
- Changing your address. They divert your billing statements to another location by completing a change-of-address form.
- Stealing. They steal wallets, purses, mail (credit card and bank statements, pre-approved credit offers, new checks, tax information, etc.), employee personnel records, etc.

Often there are no warning signs that your identity has been stolen. But if the following occur, you may be a victim:

- Your credit card and bank statements suddenly stop arriving in the mail.
- Other mail that contains personal and financial information does not arrive when expected.
- You are denied credit for no apparent reason.
- You start getting bills from companies you don't recognize.
- Collection agencies try to collect debts that don't belong to you.
- Charges you didn't make start appearing on your credit card statements.
- Debit card charges you didn't make or checks you didn't write start appearing on your bank or other account statements.
- Charges you didn't make show up when you check your account activity online.
- You are told that your address is not on your credit card account when you try to use your card to make a purchase by telephone.
- Your credit card or bank calls to ask about an unusual charge that you didn't make.
- An account you didn't open shows up on your credit report.
- You see withdrawals from your bank account that you can't explain.
- Merchants refuse your checks.
- Debt collectors call you about debts that aren't yours.
- Medical providers bill you for services you didn't use.
- Your health plan rejects a legitimate claim because their records show that you have reached your benefits limit.
- A health plan won't cover you because your medical records show a condition you don't have.
- The IRS notifies you that a tax return has already been filed in your name, or that you have income from an employer you don't work for.
- You get notice that your information was compromised by a data breach at a company where you do business or have an account.

An enormous amount of information is available on various identity theft issues. Much of this is summarized in this paper, which contains tips for minimizing risk, things to do if you become a victim or are notified of a security breach involving personal information, links to other websites that deal with preventing identity theft, etc. Another good source is the Identity Theft Resource Center (ITRC). On home page at **www.idtheftcenter.org**, click on Prevention Tips under Consumer Info and then go to Fact Sheets and Solutions for details. Also look at ITRC Blogs/Articles on Identity Theft at **www.idtheftcenter.org/Articles/Financial/**.

PROTECTING PERSONAL INFORMATION

It is not possible to protect all of your personal information. Opting out of the services provided by data vendors can be time consuming and not always possible. There are hundreds websites that can be used to find addresses, phone numbers, civil and criminal court records, birth and death records, genealogy, etc. These include personal information aggregators like Spokeo that collect and sell public information from all these sources and social networks. Even if you hire a reputation manger to do this, public information will remain available online. You need to find the original source of the information and remove it there, which also may not be possible. However, there are a great many things you can do to minimize your risk of identity theft. They deal with using credit and debit cards, protecting your SSN, managing your accounts, using the mail and ATMs, carrying personal information, securing mobile devices, protecting your passport, etc. They are covered in this section.

The Basics

- Give out credit or debit card, bank account, and other personal information only when you have initiated the contact or know and trust the person you are dealing with. Beware of e-mail or telephone calls designed to obtain personal information. An example, it's a scam if someone claiming to be from your local election board calls and asks for your SSN or other personal information to confirm your voter registration. These calls often occur prior to a big election.

- Passwords are the first line of defense to stop hackers and identity thieves from accessing your computer, tablet, mobile phone, wireless network, and other Internet-accessible devices.
  - Put unique, strong passwords on all your online accounts and computing devices. Avoid using easily remembered numbers or available information like mother's maiden name or date of birth. Passwords should have more than eight characters, with at least one capital letter, one lowercase letter, one number, and one symbol. Use of non-dictionary words or easily-remembered phrases is recommended, e.g. Johnhave3dawgs! Hackers can run a program that goes through the entire dictionary very quickly and crack any password that can be found in it. They can also use grammar rules to crack long passwords, especially those with pronouns. So use bad grammar and nouns. Another way to generate passwords is with anagrams based on song lyrics or common sayings. And to make them more secure, include symbols or umbers and alternate upper and lower case letters. For maximum security you should use passwords that are at least 12 characters long, completely random, and have at least one capital letter, one lowercase letter, one number, and one symbol. You can test your passwords online at **www.passwordmeter.com**.
  - Select password reset questions whose answers cannot be found online or from other research tools. Don't compromise a strong password with an easily answered reset question like: What is your mother's maiden name?
  - Memorize your passwords. Don't carry them in your purse or wallet.
  - Change passwords regularly. Replace all factory passwords.
  - Use a different passwords on each account.
  - Use two-factor authentication wherever available.
  - Keep your password list in a secure place.
  - Don't share passwords with anyone. It's a scam when anyone asks for your password in a call, e-mail, or text message.
- Keep your computer up to date with the latest firewalls and anti-virus/malware software. Set the software to update automatically.
- Encrypt all sensitive files.
- When shopping or banking online, make sure the website page you are on is secure, i.e., uses encryption to protect your information. You can tell it's secure when the address on the top of your screen where the URL is displayed begins with **https** rather than **http**. You can also look for a closed padlock or an unbroken key on the bottom of your screen to indicate the page is secure. If the lock is open the site or the key is broken, the page is not secure. Make sure the **https** is on all pages of the website, not just the sign-on page.
- Secure your home and business wireless network with a strong password and encrypt all sensitive information in it. Otherwise another computer within range could access your network and steal information from your computer. Criminals also can use your network to send spam or commit crimes that would be traced back to you. And be cautious when using public wireless networks. Public Wi-Fi hotspots are convenient but often not secure. Tax or financial Information you send though websites or mobile apps may be accessed by someone else. If a public Wi-Fi hotspot does not require a password, it's probably not secure. Remember, if you are transmitting sensitive information, look for **https** in the website address to ensure that the information will be secure.
- Keep personal and financial information in a secure place at home, especially if you have roommates, employ outside help, or are having work done in your home. Include all your credit and debit card, bank, charge, brokerage, and other account numbers, passwords, expiration dates, and phone numbers and addresses for quick reference if identity theft or any other problems occur.
- Make sure that the copying machines used by you and others who have your personal data, e.g., tax preparers, have data security measures installed to prevent unauthorized access to data on the copier's disk.
- Protect your health insurance cards like you would your credit or debit cards. If asked for your policy numbers or any other personal information in a doctor's office, make sure no one else is near enough to hear or see them.
- Protect your Medicare card number as you would your SSN. Don't give it to anyone who offers free medical equipment or services, or says they are from the government and then requests your number. And don't let anyone borrow or pay to use your Medicare card. That's foolish and illegal.
- Shred or tear up any documents with personal or financial information before throwing them in the trash. Use a cross-cut shredder. Or go paperless by signing up for electronic delivery.
- Avoid all online games and quizzes that request personal information, including your e-mail address. Providing this information can put your identity at risk.
- Omit any information that is not explicitly requested or required on forms, applications, surveys, etc. Information on them may be sold and become publicly available.

- Assume that anything placed on social networking websites will be publicly available. Do not post personal or sensitive information, or photos. And use appropriate security settings for anything you do post.
- Obtain free copies of your credit reports from Equifax, Experian, and TransUnion, the three Consumer Credit Reporting Bureaus (CCRBs), by visiting **www.AnnualCreditReport.com** or calling **(877) 322-8228**. This is the ONLY source of free reports authorized under Federal law. You can get one free report annually from each bureau. Check these reports for errors, fraudulent activities, e.g., accounts opened without your knowledge or consent, and persons or businesses checking on your credit. Contact the bureau immediately if you see any inaccuracies.
- Take the time to examine, identify, and protect yourself from e-mails that:
  - Contain a link. Scammers often pose as the IRS, financial institutions, credit card companies, tax preparers, or software providers. They may claim they need you to update your account information or change your password. The e-mail usually has a link to a spoofing site that may look similar to the legitimate website. Follow a simple rule. Don't click on the link. If in doubt, go directly to the legitimate website to access your account.
  - Contain an attachment. Another option for scammers is to include an attachment to the e-mail. This attachment may be infected with malware that can download malicious software onto your computer without their knowledge. If it's spyware, it can track your keystrokes to obtain your passwords, SSN, credit card numbers, and other sensitive information. Remember, you shouldn't open attachments from unknown sources.
  - Are from a "government agency" or "financial institution." **S**cammers attempt to frighten people into opening e-mail links by posing as government agencies or financial institutions. They often do this during the tax filing season.
  - Are from a "friend." Scammers often hack into e-mail accounts to steal e-mail addresses. If you receive an e-mail from a person who might have your e-mail address in their address book and the message doesn't look right or make sense, it's probably from a scammer who's trying to get you to click on a link or open an attachment. Contact that person and tell him or her that their e-mail account has been hacked.
  - Contain a false "lookalike" URL. The scammer will be trying to trick you into clicking on a link to another URL or open an attachment that infected with malware. To verify the authenticity of the URL, place your cursor over it to view a pop-up of the real URL.

Using Credit, Debit, and ATM Cards

- Guard your account information. Never disclose any numbers over the phone unless you initiate the call. Never put a card number on a post card or on the outside of a mailing envelope.
- Report all lost or stolen cards immediately and request cards with new numbers. Contact the card issuer if replacement cards are not received in a reasonable time.
- Your liability for unauthorized charges is one factor to consider in deciding whether to use a credit or debit card. As explained in the Federal Trade Commission (FTC) paper entitled *Lost or Stolen Credit, ATM, and Debit Cards* at **www.consumer.ftc.gov/articles/pdf-0075-lost-or-stolen-credit-atm-and-debit-cards.pdf**, liability under federal law depends on the type of card used and when the loss is reported.
  - If you use a credit card the federal Fair Credit Billing Act limits your liability to $50 for any unauthorized or fraudulent charges made before you report the billing error. To protect yourself you should write a follow-up letter to your credit card company to confirm that you reported the problem. Do this within 60 days after the date of the statement with any unauthorized or fraudulent ch it arge. And send it by certified mail and ask for a return receipt. If your credit card is lost or stolen, you are not responsible for any charges you didn't authorize if you report the loss before the card is used. And if the card number is stolen but not the card, you are not liable for any unauthorized use.
  - If you use a debit or ATM card and something goes wrong, your bank account can be emptied quickly without your knowledge. This can result in overdrafts, fees, and an inability to pay your bills. The federal Electronic Funds Transfer Act (EFTA) provides some liability protection in the event of any fraudulent charges resulting from the loss or theft of your card, or your card data. If you report a debit or ATM card missing before someone uses it, the EFTA says you are not responsible for any unauthorized transactions. If someone uses your card before you report it lost or stolen, your liability depends on how quickly your report it. Your maximum liability would be $50 if you report the loss or theft within 2 business days after you learn about the loss or theft. It would be $500 if your report the loss or theft more than 2 business days but less that 60 calendar days after your statement is sent to you. And it would be all the money taken from

your debit/ATM account and possibly more, e.g., money in accounts linked to your debit account, if you report the loss or theft more than 60 calendar days after your statement is sent to you. If someone makes unauthorized transaction with your debit or ATM account number, but your card is not lost or stolen, you are not liable for those transactions if you report them within 60 days of your statement being sent to you. If have to use a debit card, use one that is reloadable. Then you only risk the amount you put on the card if something goes wrong.
    - After October 1, 2017, a new rule issued by the Consumer Financial Protection Bureau (CFPB) will give users of prepaid debit cards the same liability protection against fraud that currently exits for users of debit and ATM cards.
- Keep a record of all your card numbers and their customer-service phone numbers. Put it in a safe place at home.
- Never loan your card to anyone.
- Never sign a blank charge or debit slip.
- Draw a line through blank spaces of a charge or debit slip so the total amount can't be changed.
- Pay attention to billing cycles. Check with the credit card company if you miss a bill to make sure that your address has not been changed without your knowledge.
- Only put the last four digits of your account number on checks you write to your credit card company. It knows the whole number and anyone who handles your check as it is processed won't have access to the number.
- Memorize the PINs for your debit and ATM cards. Don't carry them in your wallet or purse, or write them on anything that could be lost or seen.
- Bring home all transaction receipts. Never leave them at bank machines or counters, gasoline pumps, etc. or throw them in public trashcans. Tear them up and dispose of them at home after matching them against your monthly statements.
- Open your monthly statement promptly. Look for charges you didn't make. Notify your card companies or financial institutions immediately if you find any mistakes or discrepancies.
- Check your balance and transactions periodically during the month if you bank online.
- Call the credit card company or bank involved if a new credit card you applied for hasn't arrived in a timely manner.
- Monitor the expiration dates of your cards and contact the card issuer if new cards are not received before your card expires.
- Sign and activate new cards promptly on receipt. Or write "See ID" on the signature line on the back of the card. Then a thief won't have your signature. A merchant will ask you for a picture ID to make sure you are the cardholder.
- Cut up old cards, cutting through the account number, before you dispose of them.
- Make sure only the last four digits of your card number show up on your receipts. Use of full card numbers on electronically printed receipts is prohibited by California law. (Note that the merchant copy can show the full credit card number.) Report non-complying businesses to the Methamphetamine Strike Force hotline at **(877) 662-6384**.
- Cancel accounts you don't use or need. Carry only the cards and identification you need when you go out. Store others in a safe place.
- Tear into small pieces or shred any pre-approved credit card offers. They can be used by thieves to order cards in your name.
- Ask your credit card company to stop sending blank checks.
- Have your name removed from lists supplied by the three CCRBs to be used for pre-approved/pre-screened offers of credit or insurance. Call **(888) 567-8688** or go to **www.optoutprescreen.com** to do this.
- Don't let your card out of sight. A person taking it to a Point of Sale (POS) device might copy your name and account number and the card's expiration date and 3-digit verification code or security number. The person might also have a skimmer to steal the above information from the magnetic stripe on the back of your card, or keep your card and give you one that looks like yours. If you do give your card to a waiter or other sales person, make sure you get your card back.
- Make sure your bank and credit-card companies have your latest home and cell phone numbers, and e-mail address so they can contact you quickly if they suspect fraud in your accounts. Notify them in advance of any address or phone number changes.

- Use caution in talking to someone on the phone who claims to be a representative of your bank or credit-card company. Hang up and call your card issuer to determine if they are trying to reach you.
- Put a dollar limit on credit and debit card transactions and withdrawals. And put a number limit on transactions and withdrawals on any day.
- Some credit cards now have embedded Radio Frequency Identification (RFID) chips that are designed to be read by secure card readers at distances of less than 4 inches when properly oriented for "contactless payments." Thus, RFID readers that are available to the general public and can operate at ranges up to 25 feet and are essentially useless in stealing the information on your card. And even if that information is "hi-jacked," the cards are said to have security features that make it difficult or impossible to make a fraudulent transaction. Furthermore, the information on the chip is not the same as that on the magnetic stripe, and it cannot be used to create a functioning counterfeit version of the card. If you are concerned about unauthorized reading or tracking of the card when it is not in use, you can buy a protective RFID-blocking sleeve for the card. Make sure you carry the card in the sleeve. And if you have a card with a RFID chip and don't want to risk having the information on it stolen and used in any fraudulent activity, ask your card company for a new card without a chip. Or better, request a new card with new Europay, MasterCard and Visa (EMV) technology. These cards have a secure microchip that is designed to make them very difficult and expensive to counterfeit. Also, the chip stores encrypted data about the cardholder account, as well as a "cryptogram" that allows banks to tell whether a card or transaction has been modified in any way.
- Beware of skimmers on self-checkout terminals at grocery stores, gasoline pumps, and other places where you might swipe your credit or debit card. To avoid being liable for unauthorized charges on their credit or debit cards, consumers should keep a close eye on their statements and report the phony transactions ASAP. Also, it is better to use credit cards instead of debit cards to prevent having your checking account emptied of cash while your bank sorts out the situations discussed below.
  - In a KrebsonSecurity report on skimmers in fuel station pumps in Arizona in 2015 and 2016 posted online on Sept. 27, 2016 at **https://krebsonsecurity.com/2016/09/ inside-arizonas-pump-skimmer-scourge**, it was found that skimming devices tend to be installed in pumps that lack non-standard locks and tamper-evident seals in off-brand stations that lacked security cameras. Few stations had changed the factory-default locks on their pumps, meaning thieves armed with a handful of master keys were free to unlock the pumps and install skimming devices at will. The pumps targeted were usually the one furthest from the station and closest to the street. A review of the locations of the stations with skimmers in their pumps suggested that the scammers prefer poorly secured stations that are close to a major highway. Other than avoiding these stations and pumps, there's not much a consumer can do to prevent this scam.
  - Another KrebsonSecurity report posted on Oct. 14, 2016 deals with Bluetooth-enabled, self-checkout overlay skimmers. Scammers connect their mobile phones to the Bluetooth elements embedded in the skimmers so they can intercept PIN pad presses and card swipe data. With a range of approximately 100 meters, a scammer could sit in a vehicle parked outside the store and record card data wirelessly in real-time. Or if the skimmer is configured to store the stolen PIN and card data, the scammer could instruct it to transmit the stored data when he or she comes within range of the device. It turns out that Ingenico payment terminals retrofitted with overlay skimmers have quite a few giveaways. You can learn how to identify one by checking out Krebs' online tutorial entitled *How to Spot Ingenico Self-Checkout Skimmers*.
- Use a Virtual Account Number (VAN) when shopping online from unfamiliar or unsecure sites. (You should not be shopping from an unsecure site in any case. They are ones that do not have lock icons on the browser's status bar or a URL that begins with **https**.) Some credit card companies offer this service. Here's how it works. Log onto your credit card account and generate a random account number. Enter it into the online merchant's purchase order form instead of your real account number. This VAN will only be valid for the time it takes the merchant to process your transaction. Your credit card company will recognize it and charge the amount to your account. If a hacker breaks into the merchant computer and steals your VAN, it will be useless. Note that VANs cannot be used for purchases that require you to show your credit card at time of pick-up (e.g., movie tickets, etc.), because the account numbers won't match. VANs make it virtually impossible for anyone to steal your real account number from an online merchant. A variant on the VAN is a temporary card number that has a spending limit, expiration date, and security code that you can use for multiple online transactions.
- When shopping online, log out of payment accounts before closing your browser.
- Don't store your card information on any online payment account. This helps to protect it in the event the account's security is breached.

Using Bank Checks

- Don't carry blank checks or a checkbook in your purse or wallet. If it is lost or stolen, the finder or thief can spend them until you notify the bank and get a new account number.
- Put as little personal information as possible on your checks.
- If someone gets your account number and the bank's routing number, he or she can order a whole book of checks and spend them until your account is emptied.
- Review your bank statements carefully. Match your checkbook entries against paid checks. Look for checks you didn't write. Notify your bank immediately if you find any. Then request a new account number and new checks.
- Keep only enough money to pay upcoming bills in your checking account. You will eventually recover the payments on forged checks. But in the meantime, you will not have use of it.

Protecting Your SSN

- Examine your Social Security Personal Earnings and Benefits Estimate Statement for possible fraud. You will receive it about three months before your birthday each year. Make sure the reported income on the statement is not higher than that on your records. Contact the Social Security Administration (SSA) on its Fraud Hotline at **(800) 269-0271** or by e-mail to the Office of the Inspector General at **www.ssa.gov/org** about any differences.
- Provide your SSN only when it is required by a government agency, employer, insurance company, healthcare provider, or financial institution. Never provide it on a request by e-mail or phone call. In a recent case a man received a call from a person who claimed to be a jury coordinator and said that a warrant has been issued for his arrest because he failed to report for jury duty. When he protested that he never received a summons he was asked for his SSN and date of birth to verify the records. Caught off guard he provided this information. Instead he should have hung up realizing that court workers would never ask for a SSN or other personal information.
- In a variation of the above scam, the caller says that you've been selected for jury duty and asks you to verify your name and SSN. Remember, notification of jury duty is always done by mail.
- Never use your SSN for identification.
- Don't routinely carry your Social Security card or any document that includes your SSN, e.g., your Medicare card, in your purse or wallet.
- Do not have your SSN or driver license number printed on your checks. And never write your SSN on a check.
- Provide your driver license or some other identification number when reporting a crime in which you are the victim. Do not provide your SSN. The crime report will be available to the defense if a suspect is prosecuted.
- If you use a tax preparer, have them read the IRS Fact Sheet 2016-23 entitled *Tax Professionals: Protect Your Clients; Protect Yourself from Identity Theft* at **www.irs.gov/pub/irs-news/fs-16-23.pdf**. It urges preparers to follow the security recommendations found in IRS Publication 4557 entitled *Safeguarding Taxpayer Data* at **www.irs.gov/pub/irs-pdf/p4557.pdf**. It contains a fact sheet that outlines the critical steps necessary to protect taxpayer information and to build client confidence and trust. And for the latest tax information, preparers should subscribe to *e-News for Tax Professionals* at **www.irs.gov/uac/join-e-news-for-tax-professionals**, the IRS *Tax Pro Twitter* at **https://twitter.com/irstaxpros**, and the Return Preparer Office's *Facebook* page at **www.facebook.com/IRStaxpros**.

Using the Mail

- Deposit outgoing mail at a Post Office, in a blue U.S. Postal Service collection box, or give it directly to your mail delivery person. Put it in a collection box only if there is another pickup that day. It is not safe to leave mail in a box overnight. Also, do not leave mail for pickups from personal curbside boxes or cluster box units.
- Pick up your mail as soon as possible after it arrives in your personal curbside box or cluster box unit. If this is not possible, have a trusted friend or neighbor collect your mail, especially if you are expecting a box of checks or a new credit or debit card.
- Consider having new checks mailed to your bank for collection to avoid possible theft from your mailbox.
- Use a locked mailbox and make sure the lock works.

- Investigate immediately if bills do not arrive when expected, you receive unexpected credit cards or account statements, you are denied credit for no apparent reason, and you receive call or letters about purchases you did not make.
- If you don't receive a check or other valuable item you're expecting, contact the issuing agency immediately. If you believe your mail was stolen, call the Postal Inspection Service at **(877) 876-2455**.
- To reduce junk mail you can remove yourself from many national mailing lists by registering for the Direct Marketing Association (DMA) Mail Preference Service at **www.DMAchoice.org/register.php**. There you can stop catalogs, magazine offers, and other mail offers. You can also click on a link to manage prescreened credit offers. It will take you to **www.optoutprescreen.com**.

Using an ATM

- Use ATMs that are inside a store or a bank. These are less likely to have been tampered with for skimming, which is the illegal capture and utilization of a cardholder's financial information from an ATM transaction. If you use an outside ATM, it should be in a well-lighted, well-trafficked area and under video surveillance.
- Get off your cell phone and be alert when using an ATM.
- Check the machine and everything around it before you take out your card. Look for parts that seem crooked or have a different color, or decals that are partially covered. Also for anything that might be attached to the ATM's network cables. If you see anything that doesn't seem right, go to another machine.
- Some ATMs have flashing lights in the card slot. Their obscuration is a sign of tampering.
- Look to see if there is anything in the slot where you insert your ATM card. Some thieves place a small, thin, hard-to-detect skimming device in the card slot to steal the account and card data on the magnetic stripe on the back of your card. If anything looks suspicious, give it a pull or push. Skimmers are usually held in place loosely by glue or tape to make them easy for the thief to remove. If you remove one, turn it over to the local law enforcement agency as soon as possible with a note on where and when you removed it. Don't throw it away or keep it. Be aware that the criminals doing the skimming may be watching the ATM.
- Some thieves are now using wafer-thin skimming devices that fit inside the ATM card acceptance slot and do not alter the outward appearance of a compromised cash machine. It is inserted through the card reader throat and then sits inside the card reader capturing the data on cards that are subsequently inserted. There are also "periscope" skimmers that have been installed inside an ATM and cannot be detected from outside it.
- Although thieves can create counterfeit ATM cards with skimmed data, they cannot use the cards unless they have your PIN. To get that, thieves typically rely on cleverly hidden tiny cameras or fake keypads. Often the camera is tucked inside a false panel above or directly beside the PIN pad. So check the area around the machine for hidden cameras. Even if you don't see one, always shield the PIN entry pad with your hand so it can't be seen by anyone near you or by a hidden camera. And check for a fake keypad that has been installed over the built-in one. Fake keypads record the numbers you type in. They usually stick out too far or look strange.
- Beware of overlay skimmers that record information on card stripes and typed-in PINs. They are slightly larger than authentic terminals to fit over them and are very difficult to detect. They have been found on Ingenico credit-card terminals in self-checkout lands. You can avoid the problems they create by using chip-enable cards and terminals that require them. Even if your PIN is compromised, your card is unlikely to be counterfeited because of the difficulty and expense of counterfeiting chip cards.
- If you use a debit card, memorize your PIN and keep it secret. Don't write it down or keep it in your wallet or purse.
- Keep the customer-service phone numbers of your bank and credit-card company readily available. Call the appropriate number immediately if your card gets stuck in an ATM. Do not leave the ATM.
- Don't leave your transaction receipts at the ATM. Take them home and use them in balancing your account.
- Monitor your bank statements frequently and report any unauthorized activity immediately.

Carrying Personal Information in a Purse or Wallet

- Carry only a driver license, cash, a credit card, and insurance cards. Don't carry blank checks or a checkbook. Don't carry anything with PINs, account numbers, or passwords written on it.

- Don’t carry your Social Security card or anything with your SSN on it. Persons with Medicare cards should carry photocopies of the cards with the last four digits of their SSN removed. Keep the card is a safe place at home and bring it only if needed for a doctor appointment.
- Make a list of all the cards you carry. Include all account numbers and phone numbers to call to report a lost or stolen card. Also make photocopies of both sides of all the cards. Keep the list and copies in a safe place at home. If you carry a library card, make a copy of it too.
- Don’t carry personal information of your family members.

Securing Mobile Devices

Smartphones, smartwatches, tablets, and other mobile devices are now as powerful and functional as many computers. Therefore is necessary to protect them just like you protect your computer or laptop. The following tips will help to safeguard your personal information:

- Use a strong password to protect your device. Use different passwords of each payment app.
- Lock your device when you’re not using it. Even if you only step away for a few minutes, it's enough time for someone else to steal or destroy information in it. Use the security lockout feature so the device automatically locks after it’s not in use for a certain period of time.
- Disconnect your device from the Internet when you aren't using it. The likelihood that attackers or viruses scanning the network for available devices will target you becomes much higher if your device is always connected.
- Keep security software up to date. Update security patches so that attackers cannot take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. Install them.
- Consider creating separate user accounts. If multiple people are using the device, someone else may accidentally access, modify, or delete your information. If you have the option, create different user accounts for each user and set the access and privileges for each account.
- Establish guidelines for usage. If multiple people using your device, especially children, make sure they understand how to use the device safely. Setting boundaries and guidelines will help protect your data.
- Back up your data. Whether or not you take steps to protect yourself, there will always be a possibility that something will happen to destroy your data. Regularly backing it up reduces the stress and consequences that result from losing important information.

Protecting Your U.S. Passport

- Since August 2007 all passports issued by the U.S. State Department have a small contactless RFID computer chip embedded in the back cover. They are called “Electronic or e-passports.” The chip stores the same data that is visually displayed on the photo page of the passport. It also stores a digital photograph of the holder, a unique chip identification number, and a digital signature to protect the stored data from alteration. Unauthorized reading of e-passports is prevented by the addition of a radio-frequency blocking material to their covers. The passports cannot be read until they are physically opened. Then there are protocols for setting up a secure communication channel and a pair of secret cryptographic keys in the chip to ensure that only authorized RFID readers can read the data on the chip.
- In July 2008 the U.S. State Department began issuing U.S. passport cards that can be used to enter the United States from Canada, Mexico, the Caribbean, and Bermuda at land border crossings or seaports of entry that are less expensive that a passport book. It cannot be used for international travel by air. To increase speed, efficiency, and security at U.S. land and sea border crossings the card contains a RFID chip. However, no personal information is on the chip. It only points to a record stored at secure U.S. government databases. And a protective RFID-blocking sleeve is provided with each card to prevent unauthorized reading or tracking of the card when it is not in use. Make sure you carry the card in the sleeve.

Going Away on an Extended Trip

- Consider placing a security freeze, sometime called credit freeze, on your credit files. A security freeze means that your file cannot be shared with potential creditors. A security freeze can help prevent identity theft because most businesses will not open credit accounts without first checking a consumer's credit history. If your credit files are frozen, even someone who has your name and SSN would probably not be able to get

credit in your name. A security freeze is free to identity theft victims who have a police report of the theft. If you are not an identity theft victim and you are under 65 years of age, it will cost you $10 to place a freeze with each of the three CCRBs. That is a total of $30 to freeze your files. If you are not an identity theft victim and you are 65 years of age or older, it will cost you $5 to place a freeze with each of the CCRBs. That is a total of $15 to freeze your files. You should keep the freezes on when you return for identity theft protection. You can always lift the freeze if you want someone to see your credit file, e.g., if you are applying for credit, insurance, or employment. For more information about security freezes see the answers to frequently-asked questions published by the California Attorney General on a page entitled *How to "Freeze" You Credit Files* at **www.oag.ca.gov/idtheft/facts/freeze-your-credit**.

- Call your credit card companies using the customer service number on the back of the card to alert them about when, where, and how long you will be away. This will enable their fraud departments to stop charges if your card is used elsewhere, and reduces the risk that charges made where you are going to be will not be accepted. Or you can do this online if your card issuer has a "travel notification" or similar tab that you can use when you log onto your account.
- Credit cards with embedded microchips are extremely difficult to counterfeit or copy. They are now standard in Canada, Mexico, Europe, and many other countries, and will be mandatory in the United States by October 2015. In the meantime cards without these chips may be rejected in many places. If your card issuer offers micro-chipped cards, you should get one before travelling to these countries.
- Service members who deploy and don't expect to seek new credit while they are away can have an active duty alert placed on their credit files. This alert requires creditors to take extra steps to verify your identity before granting credit in your name. It lasts for one year but can be renewed. Call the fraud department of one CCRB to request this alert; it must contact the other two. Their phone numbers are: **(800) 525-6285** for Equifax, **(888) 397-3742** for Experian, and **(800) 680-7289** for TransUnion. These CCRBs will take your name off their marketing list for prescreened credit card offers for 2 years unless you ask them to add you back onto the list.

Making It Harder for Hackers

You can make it harder for hackers to get your personal information by carefully selecting websites you provide information to. Here are some things you can do.

- Use a website with two-factor authentication that asks for a second one-time code anytime you log in from a new computer.
- Put unique, strong passwords on all your online accounts as suggested under the basics above.
- Use a password to answer a security question such as "What is the name of your first school?" Answers to these kinds of questions are easily found in public record searches on the Internet. If a site offers only multiple-choice answers or requires short passwords, don't use it. Or provide an answer other than the correct one.

PROTECTING YOUR CHILD'S IDENTITY

A child's SSN can be used by identity thieves to apply for government benefits, open bank and credit card accounts, apply for a loan or utility service, or rent a place to live. At a forum on child-centric fraud sponsored by the FTC in July 2011 it was estimated that more than 140,000 American children become victims of identity theft each year. And in 2012 one identity-theft protection company estimated that about 11 percent of children five years of age or under have had their identities stolen. Thieves obtain children's SSNs by various means and sell these genuine numbers to persons with poor credit ratings who obtain credit cards, make extensive purchases, and don't pay their bills. Several signs can tip you off to the fact that someone is misusing your child's personal information and committing fraud. For example, you or your child might:

- Be turned down for government benefits because the benefits are being paid to another account using your child's SSN
- Get a notice from the IRS saying the child didn't pay income taxes, or that the child's SSN was used on another tax return
- Get collection calls or bills for products or services that you or your child didn't order
- Be denied credit for an unpaid debt

The following tips will help you protect your child's identity and prevent fraudulent use of his or her SSN.

- Protect your child's SSN as you would your own. Encrypt all files on your devices that contain it. Protect your devices with a firewall and anti-virus software. Carry your child's SSN in your purse or wallet only when you know you will need it.
- Provide your child's SSN only when it is required by a government agency or financial institution. Never provide it for identification.
- Teach your child never to give out personal information over the phone or on the Internet.
- Watch your child's mail for credit card applications, bills, or bank statements. They are signs that someone has started a credit history in your child's name.
- Check periodically to see if your child has a credit file. There should not be one unless someone has applied for credit using your child's SSN. No minor should have a credit file. If your child does have one, contact the credit card companies and the CCRBs immediately and ask each one to remove all accounts, account inquiries, and collection notices from any file associated with your child's name and SSN. You should also contact every business where your child's information was misused and ask each one to close the fraudulent account and flag it to show that it resulted from identity theft. Tell the businesses that issued credit that the accounts are in the name of your minor child, who by law isn't permitted to enter into contracts.
- Request that banks in which your child has an account remove his or her name from marketing lists.
- Take advantage of your rights under the Children's Online Privacy Protection Act (COPPA). This Federal law and the FTC mandates under it require websites and mobile apps to get parental consent before collecting and sharing information from children under 13 years old. This includes photos, videos, geolocation, and tracking tools such as cookies that use Internet Protocol addresses and mobile device IDs to follow a child's web activities across multiple apps and sites. COPPA covers sites and apps designed for children under 13 and general-audience sites and apps that know certain users are under 13. It protects information that sites and apps collect upfront and information that children give out or post later. It also requires these sites and apps to post a privacy policy that provides details about the kind of information they will collect and what they might do with the information. You should: (1) know your rights, (2) be careful with your permission, (3) check out the sites your children visit and apps they use, (4) review the sites' and apps' privacy policies, (5) contact the site of app if you have any questions about its privacy policy, and report any site or app that breaks the rules to the FTC at **www.ftc.gov/complaint**. For answers to frequently asked questions about the Children's Online Privacy Protection Rule go to **www.ftc.gov/privacy/coppafaqs.shtm**.
- Also take advantage of your rights under the Family Educational Rights and Privacy Act (FERPA), which is a Federal law that protects the privacy of student education records. It applies to all schools that receive funds under an applicable program of the U.S. Department of Education. It gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students." With certain exceptions, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, schools may disclose without consent "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. But schools must tell parents and eligible students about directory information and allow them a reasonable amount of time to request that the school not disclose directory information about them. Schools must notify parents and eligible students annually of their rights under FERPA. For additional information you can call the U.S. Department of Education's Information Resource Center at **(800) 872-5327**. You should also be concerned about how information about your child is used and shared by organizations that sponsor after-school activities.
- The FTC page on child identity theft at **www.consumer.ftc.gov/articles/0040-child-identity-theft** has more information on checking for a credit report, repairing the damage, prevention and protection, limiting the risks, and what to do when your child turns 16.

You should also be concerned about protecting your children's profiles, which include their name, gender, birth date, parents' names, mailing address, e-mail address, etc. This information may be collected by makers of Internet-connected toys and not be protected very well from hacking. For example, in 2015 VTech announced that one of its databases had been hacked, exposing the names, ages, and genders of six million children who used the company's toys. To be safe, parents should not connect to the Internet any toys or other electronic device their children might use.

PROTECTING A DECEASED'S IDENTITY

Identity thieves obtain information about deceased individuals from obituaries, the SSA Death Master File, and other places. Or the thief may be a family member or someone else who knew about the death. Here are some things the surviving spouse or the executor of the deceased's estate should do to prevent identity theft.

- Limit the amount of personal information in the obituary.
- Obtain at least 12 copies of the official death certificate when it becomes available. These would be sent to various places as needed to prove death. Some places may accept a photocopy.
- Request copies of the deceased's credit files from the CCRBs and have them place the following alert on any files that are requested: "Deceased. Do not issue credit."
- Send a notice of death to all financial companies and institutions in which the deceased had an account. These include credit-card companies, banks, stock brokers, loan/lien holders, collection agencies, CCRBs, etc.
- Close all accounts that were in the deceased's name. Ask that they be listed as "Closed: Account holder is deceased."
- Have all joint accounts put in the survivor's name.
- Also notify the following:
  - SSA
  - Insurance companies
  - Veteran's Administration if the deceased had served in the U.S. military
  - Immigration Services if the deceased was not a U.S. citizen
  - Department of Motor Vehicles if the deceased had a state driver license or identification card.
  - State agencies that licensed the deceased, e.g., State Bar.
  - Places and groups where the deceased was a member, e.g., public library, country and fitness clubs, professional organizations, etc.
- Send all mail certified, return receipt requested. Keep copies of all correspondence.

For more information on contacting CCRBs and other financial institutions, see ITRC Fact Sheet 117 entitled *Identity Theft and the Deceased: Prevention and Victim Tips* at **www.idtheftcenter.org/Fact-Sheets/fs-117.html**.

BUYING IDENTITY THEFT PROTECTION

- You cannot buy absolute protection against identity theft. Beware of any such claims, especially regarding the misuse of existing credit-card accounts, theft of medical records, and theft of personal information from employer's personnel files. Fraud alerts and security freezes just make it more difficult for identity thieves to open new accounts in your name, which make up a small fraction of all identity theft incidents. In contrast to a security freeze defined above, a fraud alert is free but it's only good for 90 days; however, it can be renewed. The alert consists of a special message on a credit file that tells creditors that there may be fraud in the account and to follow certain procedures before they open new accounts in your name or make changes to existing accounts. This may prevent someone from opening a new account in your name but it will not prevent misuse of your existing accounts.
- Identity theft protection companies offer services that range from placing and renewing fraud alerts and security freezes on your credit files to monitoring your credit reports for recent activities, helping you rebuild your identity if is stolen, reimbursing you for losses due to identity theft, removing your name from mailing lists of pre-screened offers of credit or insurance, etc.
- In buying identity theft protection you will be paying for many things you can do for yourself at no cost. These include placing and renewing fraud alerts and security freezes, obtaining annual credit reports, and removing your name from mailing lists. These protective measures are discussed in this paper.
- Before signing up for protection, be sure to understand what services are provided and what protection you are buying. For this you should compare the protection that various companies offer and their costs. Independent reviews can help in this. One company that publishes such reviews is Reviews.com. Its review of identity theft protection companies can be seen online at **www.reviews.com/identity-theft-protection-services**.

USING A TAX PREPARER

Because tax professionals hold sensitive client data, cybercriminals are increasingly targeting them with a variety of tactics from remote computer takeovers to phishing scams to steal taxpayer identity and other information for use in filing false tax returns. (Taxpayer data is defined as any information obtained or used in the preparation of a tax return.) Thus, tax preparers have a critical role in protecting taxpayer data. Moreover, they have a legal responsibility to have safeguards in place for this. In selecting a tax preparer you should make sure that they have read the IRS Publication 4557 entitled *Safeguarding Taxpayer Data* and follow the safeguards outlined in IRS Fact Sheet FS-2016-23 dated July 2016 entitled *Tax Professionals: Protect Your Clients; Protect Yourself from Identity Theft*. Here are some of the safeguards suggested in these papers.

- Conduct a comprehensive background check on all employees before granting them access to taxpayer data.
- Terminate access to taxpayer data when an employee leaves your office.
- Ensure that all employees have robust security software and that it remains turned on and active at all times and updates automatically so it's always up-to-date and to protect against new and emerging malware and viruses.
- Connect to a software provider from its main webpage and not by clicking on a link or attachment in an unexpected e-mail.
- Use the "deep scan" function to fully scour all computer drives and files for any malware or viruses. Perform a deep scan periodically.
- Never leave taxpayer data unsecured. Use security software on all digital devices.
- Dispose of taxpayer data securely. Shred documents and destroy media.
- Use strong passwords on all computers and software programs.
- Change passwords every 60 to 90 days.
- Store taxpayer data securely and encrypt it when transmitting across networks.
- Encrypt e-mail that contains taxpayer data.
- Keep all paper documents, computer disks, flash drives, and other media in a secure location with access restricted to authorized personnel only.
- Protect your PTIN and monitor it frequently on the online PTIN system for the number of returns filed and processed in the current year.
- Do not permit remote access to internal networks containing taxpayer data.
- Maintain a security plan for your office and its operations. At a minimum, use the checklist in IRS Publication 4557.
- Develop and publish a security manual for your staff regarding access to and use of computer information systems, paper records, and taxpayer data.
- Provide periodic training in security procedures. Educate your employees about the dangers of phishing e-mails and other scams that could lead to malware or virus infections. Clicking on a link or opening an attachment in a phishing e-mail can result in the hacking of all office computers for sensitive data. For example, they should be aware that scammers are sending e-mails pretending to be from a software company that request the recipient click on a link in the e-mail to download and install a software update. If this is done they will have downloaded a program designed to track your strokes, which is a common tactic used by cyber thieves to steal login information, passwords, and other sensitive data.
- Subscribe IRS Tax Tips, an IRS e-mail service for alerts warning of cybercriminal efforts to breach tax preparers' defenses.
- Protect your office from unauthorized access.

CHECKING FOR POSSIBLE IDENTITY THEFT

- Obtain free copies of your credit reports from the CCRBs by visiting **www.AnnualCreditReport.com** or calling **(877) 322-8228**. This is the ONLY source of free reports authorized under Federal law. You can get one free report annually from each bureau. Stagger your requests to obtain one every four months. That way you can monitor your credit during the year. Check these reports for errors, fraudulent activities, e.g., accounts opened without your knowledge or consent, and persons or businesses checking on your credit. Contact the CCRB immediately if you see any inaccuracies. These bureaus may also try to sell you credit monitoring products or services for a fee. The FTC requires that any advertising for such products or services be delayed until after you get your free credit reports.

- Other websites that claim to offer free credit reports, credit scores, or credit monitoring are not part of the legally mandated free annual credit report program. In some cases, the "free" product comes with strings attached. For example, some sites sign you up for a supposedly free service that converts to one you have to pay for after a trial period. And if you don't cancel during that period, you may be unwittingly agreeing to let the company start charging fees to your credit card.
- If you find an error in a report you should submit a dispute directly to the CCRB. Its e-mail address, mailing address, and phone number should be on the credit report. CCRBs are required to respond within 30 days. They will contact the lender that provided the information under dispute. If a fix is made the lender will contact all three credit bureaus. When the investigation is complete must provide written results and a free copy of your report. You should also contact the lender and ask that they update the CCRBs with correct information. If you are not satisfied with the results of these investigations you should file a complaint with the CFPB, the federal agency that enforces the rules for credit reporting and monitors compliance by the CCRBs. You can do this online at **www.consumerfinance.gov/complaint** or by phone at **(855) 411-2372**. In any case don't pay a Credit Repair Organization (CRO) to handle your dispute. It can't do anything more than what you can do. And if you encounter a CRO that promises to remove negative items from your credit reports it is safe to assume it's a scam, as discussed under Credit Repair in the paper on Fraud Prevention on the Prevention Tips page of the SDPD website at **www.sandiego.gov/police/services/prevention/tips**.
- Check your medical bills and health insurance statements to make sure the dates and types of services match your records. Read every letter you get from your insurer, including those that say "this is not a bill." If you see a doctor's name or date of service that isn't familiar, call the doctor and your insurer.
- Once a year request a list of all benefits paid in your name by your health insurer. If the thief has changed your billing address you would not be receiving any bills or statements.
- These checks are critical in detecting synthetic identity theft, which is now the prevalent kind of identity theft. In it the thieves create new identities by combining real and fake identifying information to establish new accounts with fictional identities. In typical case a thief may use your SSN and combine it with another name and address. This combination won't show up on your credit reports. The CCRBs may create a new file for it or a subfile under your file. Although synthetic identity theft mainly hurts creditors, you can be affected and should do the following in addition to the checks listed above:
  - Look out for suspicious mail sent to your home address with someone else's name on it. It may be a change-of-address notice, a credit offer, or a statement for an account you didn't open.
  - Contact your credit-card issuer if any expected mail does not arrive on time.
  - If you are denied credit, make sure the creditor's decision is based on your identity and personal credit information, and not someone else's.
  - Consider buying an identity theft protection service that will monitor your personal credit information, scour the Internet for unauthorized use of your credit and debit cards and SSN, and alert you if any changes are detected.
  - Be prepared to deal with debt collectors for purchases you did not make. They can find you in a SSN search.

IF YOU BELIEVE YOU MAY BECOME VICTIM

Once identity thieves have your personal information they can cause you a great deal of trouble. They can drain your bank account, run up charges on your credit cards, open new utility accounts, get medical treatment on your health insurance, file a tax refund in your name and get your refund, your name to the police during an arrest, etc.

If you believe your personal information has been compromised, don't wait until you become a victim to report it. Contact all companies and government agencies that might get involved. For example, because there is so much income tax fraud, if you believe your SSN has been compromised contact the IRS Identity Protection Specialized Unit (IPSU) at **(800) 908-4490**. The IPSU will suggest that you file an IRS Form 14039, Identity Theft Affidavit. This will alert the IRS that someone might use your SSN to get a job or file a tax return to receive a refund. It will authorize the IRS to put a marker on your account that will help it protect you from identity theft and resolve future identity theft issues. You should also go to **www.irs.gov/privacy/article/0,,id=186436,00.html** for links to information on protecting your identity and a guide for identity theft victims.

Or if your purse or wallet is lost or stolen, you should do the following:

- File a police report in the jurisdiction where your wallet was lost or stolen. Also file one in the jurisdiction where you live. Get a copy of the report. You many need to send copies elsewhere.
- Report the loss to one of the three CCRBs. And request that an initial fraud alert be placed on your credit files. The CCRB you call is required to notify the other two. In doing this you will be entitled to free copies of your credit report from each CCRB. Order them a few weeks after your loss and review them carefully. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain.
- Alert your banks of the loss and request new account numbers, checks, ATM cards, and PINs. Also provide new passwords and stop payment on any missing checks.
- Contact all your creditors by phone and in writing to inform them of the loss.
- Call your credit card companies and request account number changes. Don't ask to cancel or close your accounts; that can hurt your credit score, especially if you have outstanding balances. Say you want a new numbers issued so your old numbers will not show up as being "cancelled by consumer" on your credit reports.
- Call the security or fraud departments of each company you have a charge account with to close any accounts that have been tampered with or established fraudulently. Follow up the request in writing and ask for written verification that the accounts have been closed and any fraudulent debts discharged. Keep copies of all documents and records of all conversations about the loss. If you still want a charge account, request a new number.
- If your Social Security card or any other card with your SSN on it was in your purse or wallet, contact your local police and the IRS as suggested above. Also contact the Social Security Administration (SSA) at **(800) 772-1213** to request a replacement card or go to **www.ssa.gov/ssnumber** to apply for one online.
- If your Medicare card or any other card with your Medicare number on it was in your purse or wallet, contact your local police and the IRS as suggested above. Also contact the SSA at **(800) 772-1213** to request a replacement card. Or to obtain one online, you need to first create a My Social Security account as explained at **https://faq.ssa.gov/ics/support/kbanswer.asp?deptID=34019&task=knowledge&questionID=3708**.
- If your driver license was lost, contact the California DMV Fraud Hotline at **(866) 658-5758** to report the loss, request a replacement license, ask that a stolen/lost warning be placed in your file, and check that another license has not been issued in your name.
- If your library card was lost, contact the library immediately. Otherwise you could be held financially responsible for any material borrowed after the loss.
- If you lose your automobile, homeowners, or health insurance cards, notify the companies and request replacements.
- If your passport was lost or stolen in the United States, report it to the U. S. Department of State by calling **(877) 487-2778**. Operators are available from 8 a.m. to 10 p.m. ET, weekdays excluding Federal holidays. Or you complete, sign, and submit Form DS-64, Statement Regarding a Lost or Stolen Passport, to the U. S. Department of State, Passport Services, Consular Lost/Stolen Passport Section, 1111 19th St. NW, Ste. 500, Washington DC 20036. If it was lost or stolen overseas contact the nearest U. S. Embassy or Consulate.
- To replace a lost or stolen passport in the United States submit Forms DS-11, Application for a U. S. Passport and DS-64 in person at a Passport Agency or Acceptance Facility. If you are overseas, go to the nearest U. S. Embassy or Consulate if you are overseas to replace it.

If you are on active duty in the military you should contact one of the CCRBs and place an active duty fraud alert on your credit files. This is similar to the ordinary fraud alert in that it requires an inquiring creditor to verify that it is you who is attempting to open a line of credit. The difference is, unlike the 90-day fraud alert, this alert lasts for a year. You can download a copy of the letter asking for an active duty fraud alert at **www.idtheftcenter.org/images/documents/LF-133.pdf**. Additionally, if you are deployed out of the country and cannot be contacted, you may appoint somebody you trust to act as your representative.

IF YOU BECOME A VICTIM

File a police report as soon as possible if you become a victim of identity theft, i.e., when someone has obtained your personal information and used it for an unlawful purpose. Call the SDPD non-emergency number, **(619) 531-2000** or **(858) 484-3154**, and give the dispatcher a description of the theft. An officer will call to take a full report,

including any information you may have on suspects and witnesses, and give you a case number. Then do the following:

- Set up a folder where you can keep a log of all your reports and supporting documents, and contacts and their phone numbers. You will need to refer to the case number when you have contacts with any business or law enforcement agencies concerning your case.
- Report the theft to the FTC at **www.IdentityTheft.gov** to get help in recovering from it. (The FTC is the federal clearinghouse of complaints of victims of identity theft. It received over 490,000 identity theft complaints in 2015, a nearly 50 percent increase over the number in 2014.) After answering some questions about your situation, you'll be told what to do right away, what to do next, and what other possible steps to take to create a personal recovery plan. Then you can create an account and be walked through each recovery step, have your plan updated as needed, have your progress tracked, and have pre-fill forms and letters generated for you.
- Report the theft to the fraud unit of Equifax, Experian, or TransUnion and request an extended fraud alert be placed on your credit files. The company you call is required to inform the other two. Extended fraud alerts are free and good for seven years. For this you will have to provide a copy of a police report and proof of your identity. You may also have to fill out a request form. When you request an extended fraud alert you are entitled to two free copies of your credit reports within 12 months from each CCRB. Review them carefully and look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain. Also, your name will also be taken off marketing lists for pre-screened credit offers for five years unless you ask them to put your name back on the list. This fraud alert permits some creditors to get your report as long as they take steps to verify your identity, which may include contacting you in person. Like an initial fraud alert, an extended alert may prevent someone from opening a new account in your name but it will not prevent misuse of your existing accounts.
- An alternative to an extended fraud alert is a security freeze. A freeze generally stops all access to your credit files, but like a fraud alert, it may not stop misuse of your existing accounts or other types of identity theft.
- Alert your banks of the theft and request new account numbers with new checks, ATM cards, and PINs. Also provide new passwords and stop payment on any missing checks.
- Contact all your creditors by phone and in writing to inform them of the theft.
- Call your credit card companies and request account number changes. Don't ask to cancel or close your accounts; that can hurt your credit score, especially if you have outstanding balances. Say you want a new numbers issued so your old numbers will not show up as being "cancelled by consumer" on your credit reports. Also change your PINs and passwords.
- Call the security or fraud departments of each company you have a charge account with to close any accounts that have been tampered with or established fraudulently. Follow up the request in writing and ask for written verification that the accounts have been closed and any fraudulent debts discharged. Keep copies of all documents and records of all conversations about the theft. If you still want an account, request a new number with a new log-in and password.
- Contact your accounts that have not yet been tampered with and request new account numbers with new log-ins and passwords.
- If an identity thief has used your SSN to file a forged tax return in an attempt to get a fraudulent tax refund early in the filing season and you file your own return later, you will receive a notice or letter from the IRS that states one of the following: (1) More than one tax return has been filed for you, (2) You have to return the money paid out in your name to the identity thief, or (3) IRS records indicate you received wages from an employer not names on your return. In this case you will need to respond immediately and submit the Form 14039. If you are experiencing economic harm or the problem is not being resolved through normal channels you can get help from the Taxpayer Advocate Service (TAS) by calling **(877) 777-4778**. For more information on the TAS go to **www.irs.gov/advocate**.
- Contact the SSA on its Fraud Hotline at **(800) 269-0271** if your SSN has been compromised.
- Call the U.S. Secret Service at **(619) 557-5640** if the crime involves counterfeit credit cards or computer hacking.
- Contact the California DMV Fraud Hotline at **(866) 658-5758** to report the theft and ask that an identity theft warning be placed in your file and check that another license has not been issued in your name.
- Notify the U.S. Postal Inspector if your mail has been stolen or tampered with. Its number is **(800) 275-8777**. Or report it online at **https://postalinspectors.uspis.gov/contactUs/filecomplaint.aspx**.

- In the case of medical identity theft, request a copy of your current medical files from each health care provider, and request that all false information be removed from them and your insurance files. Enclose a copy of the police report with your requests. For more information things to do if you are a victim of medical identity theft or concerned about it go, the World Privacy Forum's website at **www.worldprivacyforum.org/category/med-id-theft**.
- Call the Health Insurance Counseling and Advocacy Program's Senior Medicare Patrol (HICAP/SMP) at **(800) 434-0222** to report any theft that involves Medicare.
- If you are contacted by a collector for a debt that resulted from identity theft, send the debt collector a letter by certified mail, return receipt requested, stating that you did not create the debt and are not responsible for it. Include a copy of the police report you filed for the identity theft crime and a completed copy of the FTC's Identity Theft Victim's Complaint and Affidavit. It can be downloaded from its website at **www.consumer.ftc.gov/articles/pdf-0094-identity-theft-affidavit.pdf**. Also write in your letter that you are giving notice to a claimant under California Civil Code Sec. 1798.93(c)(5) that a situation of identity theft exists.
- Call the SDPD Economic Crimes Section at **(619) 531-2545** and talk to the investigator if you have any questions about your case, or have more information to provide.
- Other things you should do as a victim are in the Identity Theft Victim Checklist on the website of the California Department of Justice Office of the Attorney General **at www.oag.ca.gov/idtheft/facts/victim-checklist**. They will help victims clear up their records and limit the damage done by the thief.
- The ITRC website at **www.idtheftcenter.org** also has information ranging from advice for people who have had a wallet stolen to tips for reducing the risks of identity theft. It also contains fact sheets, solutions to various identity theft problems, letter forms, scam alerts, and answers to frequently asked questions. Its toll-free victim-assistance number is **(888) 400-5530**.

IF YOU ARE NOTIFIED OF A SECURITY BREACH INVOLVING PERSONAL INFORMATION

Most states now have security breach notification laws under which a person whose personal information is compromised must be notified of the breach. The California Breach Notification Law is in Civil Code Sections 1798.29, 1798.82, and 1798.84. The first section applies to state and local government agencies; the other two apply to any person or business that conducts business in California and that owns or licenses computerized data that includes personal information. The notice requirement is triggered if the breach involves an individual's first name or first initial and last name in combination with one or more of the following data elements when either the name or the data elements are not encrypted:

- SSN
- Driver license or California identification card number
- Financial account, credit, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's account
- Medical information
- Health insurance information
- User name or e-mail address in combination with a password or security question and answer that would permit access to an online account.

If you get a breach notice you should do the following for each data element:

- SSN. Put an initial fraud alert on your credit files and order copies of your reports from the three CCRBs. Review them carefully and file a police report if you find anything suspicious. If you don't find anything suspicious at first, renew the fraud alert and check your credit reports periodically. Also report the loss to the FTC, IRS, and SSA.
- Driver license or California identification card number. Call the DMV Fraud Hotline to report the incident.
- Financial account, credit card, or debit card numbers. Call the institution to request new account numbers and PINs. And put new passwords on your accounts.
- Medical or health insurance information. Review your explanation of benefits statements and contact your insurer if you see any services you did not receive.

For additional information on this and other privacy issues visit the Privacy Rights Clearinghouse's website at **www.privacyrights.org**.