



**IDENTITY THEFT
*TOOLKIT*** //////////////////////////////////////

Action Plan | Reporting Log | Information

TO DO LIST

- STEP 1 – PREPARE** **2**

Get ready to recover your identity. It takes time. Stay calm and be patient. Move quickly through this step because you can come back to it. Keep good documentation.

- STEP 2 – REPORT** **5**
 - Notify all banks and credit card companies that you do business with that your identity has been compromised/stolen. Ask them to freeze or close accounts along with locking down all online access.
 - Alert your professional partners (i.e., accountant, attorney, financial advisor, broker) that your identity has been compromised.
 - Change all passwords and PINS to your online accounts.
 - File a police report with your local police department. If online fraud was committed, file a complaint with IC3, a division of the FBI.
 - Get a free credit report from the credit bureaus and place a fraud alert or freeze with the credit bureaus. You only need to report to one bureau for fraud alerts and they will share the information with the other two. For freezes, each bureau will need to be contacted.
 - Report the identity theft to the FTC and other state and federal agencies.
 - Notify friends and family members that could be impacted considering the information that was compromised (phone, email) including contact information (phone numbers, email address), pictures, and other information that may be at risk.

- STEP 3 - INVESTIGATE** **13**
 - Review account activity for suspicious transactions and report any unauthorized activity to the provider.
 - Bank accounts
 - Credit card accounts
 - Venmo, Zelle, PayPal
 - Digital wallets (i.e., Apple Pay)

- STEP 4 – DISPUTE** **15**

File disputes with the providers for all fraudulent transactions or accounts identified. Identify short-term solutions like Tradition Capital Bank's *Identity Theft Recovery Loan*.

- STEP 5 – MONITOR** **18**

Keep an eye on your bank accounts, credit card statements and free credit reports to identify any additional fraud.

- STEP 6 – PREVENT** **19**

Additional services are available, including monitoring subscriptions, to help prevent this from happening again.

STEP 1 – PREPARE

- Read EACH page of the Toolkit and Log. Not all pages will apply to your particular situation, but it is important to read each one so that you cover all your bases.
- Get two folders, large envelopes, or other containers in which to keep documents.
- Label one “ORIGINALS.” In it keep the originals of all materials you compile. Do not send your original documents to anyone. Keep them safe.
- Label the second folder “COPIES.” In it keep copies of everything relevant to your identity theft.
- Use this Toolkit and Log to document your progress.
- Begin by making several copies of the charts and sample letters in this Toolkit and Log.
- Prepare yourself mentally and emotionally. Know that clearing your credit history may take many months and many hours of your time.
- Understand that you may not be able to speak to a live person when you make telephone calls to credit reporting companies or other businesses. Most of them use automated telephone systems.
- Send all mail certified, return receipt requested. This is expensive, but worth it because it allows you to prove that your letters were received. Our form letters have a place below the recipient’s address for you to record the certified mail number. This will help you match the postal service return cards (green cards) to your copies of the letters. When the green card is returned to you paper clip it to the copy of the letter that matches the card and keep it in your folder.
- Do not take shortcuts. Follow up phone calls with letters confirming what was said. A document speaks for itself, whereas you may not be able to prove what was discussed in a disputed telephone conversation.

STEP 1 – PREPARE: PROVING WHO YOU ARE

The first thing you will be asked to do is prove who you are. You will need copies of your driver’s license or government issued ID card, your Social Security card, and most recent utility bills. You may be asked to prove your residence address for the last 5 years. Companies prefer to use utility bills as proof of address. Contact your utility provider and request a printout showing where you have had service for the past 5 years.

INFORMATION ABOUT YOU		
FULL NAME	DOB	SSN
OTHER NAMES USED	DRIVER'S LICENSE OR ID NUMBER	
ADDRESSES FOR PAST FIVE YEARS		

STEP 1 — PREPARE: HOW DID YOU FIND OUT?

The second thing you will be asked is, “*Why do you think you are a victim of identity theft?*” Make your answer as short, yet as complete, as possible. Answer the questions below as accurately as possible. Use this chart as an outline when you speak to anyone about your identity theft. This will help you keep your communications consistent. You will use this information repeatedly in making reports and collecting evidence of your identity theft.

QUESTION	ANSWER
HOW DID YOU FIND OUT YOUR IDENTITY WAS STOLEN? <i>Examples: I was turned down for a car loan, or I got calls from a bill collector.</i>	
WHEN DID YOU FIND OUT THAT YOUR IDENTITY HAD BEEN STOLEN?	
WHAT ACCOUNTS, INFORMATION, OR PROPERTY WAS TAKEN AND IN WHAT AMOUNT? <i>Include as much information as you have. You will add to this later.</i>	
WHAT ACCOUNTS WERE OPENED FRAUDULENTLY USING YOUR IDENTITY? <i>Include as much information as you have.</i>	
DO YOU HAVE WRITTEN PROOF OF THE IDENTITY THEFT YET? <i>Example: A letter from a collection agency.</i>	

STEP 2 – REPORT

Reporting your identity theft takes several steps, and it may feel overwhelming. Each step is important, so do not be tempted to omit a step.

YOUR BANK(S), CREDIT CARD, PAYMENT SERVICE AND CHECK VERIFICATION COMPANIES

- If an identity thief has passed checks in your name or used your bank account, notify your bank(s), credit card companies, payment services and the major check verification companies. Ask your bank to change your account number and issue new checks.
- Contact check verification companies to make a report of identity theft and request that they notify retailers not to accept checks with the old account number on them. You may also be able to get a free annual credit report from these companies.

COMPANY	PHONE NUMBER + ADDRESS	DATE	CONTACT PERSON (NAME + TITLE)	NOTES OF CONTACT	DATE LETTER SENT
YOUR BANK	Tradition Capital Bank 952-806-6600 7601 France Ave S, Ste 140 Edina, MN 55435				
YOUR BANK					
YOUR BANK					
CREDIT CARD					
CREDIT CARD					

CREDIT CARD					
CREDIT CARD					
VENMO					
ZELLE					
PAYPAL					
CHEX SYSTEMS	800-428-9623 12005 Ford Rd. Dallas, TX 75234				
TELECHECK (CHECK VERIFICATION SERVICE)	800-710-9898 P.O. Box 4451 Houston, TX 77210 https://getassistance.telecheck.com/forgery-or-identity-theft/				
CERTEGY, INC. (CHECK VERIFICATION SERVICE)	800-237-3826 11601 N. Roosevelt Blvd. St. Petersburg, FL 33716 https://certegy.com/contact-us-consumer/				

STEP 2 — REPORT: LAW ENFORCEMENT

Notify your local police or sheriff's department (for the jurisdiction of your residence) that you are a victim of identity theft/financial fraud. Ask to make a complaint. Request that an official written incident report be made and ask for an official copy suitable for sending to creditors. This copy should be provided to you at no cost. If you have an identity theft affidavit or complaint report from the Federal Trade Commission (FTC), ask that a copy be attached to your police report. Also request that your name be submitted to the FBI's NCIC Identity Theft File, which provides a means for law enforcement to flag stolen identities and identify imposters when they are encountered.

You may encounter resistance initially. If so, be polite but firm. Advise the agency that you will provide additional information as it becomes available. State laws allow for the filing of this complaint in the jurisdiction where you live even if the crime occurred elsewhere (Minnesota Statutes section 609.527, subdivision 5(b); Arizona Statutes 13-2008).

If the crime was committed using the Internet, complete an online complaint form with the Internet Crime Complaint Center (IC3). IC3 will research and refer your complaint to law enforcement and or regulatory agencies for any investigation they deem to be appropriate.

AGENCY	PHONE NUMBER	TIME	DATE	CONTACT PERSON (NAME + TITLE)	NOTES OF CONTACT	REPORT TAKEN	COPY REQUESTED	COPY RECEIVED
LOCAL POLICE DEPARTMENT						<input type="checkbox"/> YES <input type="checkbox"/> NO	<input type="checkbox"/> YES <input type="checkbox"/> NO	<input type="checkbox"/> YES <input type="checkbox"/> NO
COUNTY SHERIFF'S						<input type="checkbox"/> YES <input type="checkbox"/> NO	<input type="checkbox"/> YES <input type="checkbox"/> NO	<input type="checkbox"/> YES <input type="checkbox"/> NO
OTHER						<input type="checkbox"/> YES <input type="checkbox"/> NO	<input type="checkbox"/> YES <input type="checkbox"/> NO	<input type="checkbox"/> YES <input type="checkbox"/> NO

FBI - NATIONAL WHITE COLLAR CRIME CENTER	METHOD OF CONTACT	TIME	DATE	NOTES OF CONTACT	REPORT TAKEN	COPY REQUESTED	COPY RECEIVED
ONLINE COMPLAINT FORM FOR INTERNET CRIMES ONLY: WWW.IC3.GOV	<input type="checkbox"/> ONLINE <input type="checkbox"/> PHONE <input type="checkbox"/> MAIL				<input type="checkbox"/> YES <input type="checkbox"/> NO	<input type="checkbox"/> YES <input type="checkbox"/> NO	<input type="checkbox"/> YES <input type="checkbox"/> NO

STEP 2 — REPORT: CREDIT REPORTING COMPANIES: NOTIFY EQUIFAX, EXPERIAN, OR TRANSUNION

Report that you are an identity theft victim and request that a *90-day fraud alert* be placed on your credit report. That company should notify the other two, although it is recommended to contact all three. A fraud alert is a simple note that lets creditors know someone may be fraudulently applying for credit with your information. Notify *Innovis* separately because it does not currently share information with the other companies. During the phone call, request a free copy of your credit report. Request that the first 5 numbers of your Social Security Number be blocked from your credit report. After you have compiled more information, send a letter confirming your conversation and disputing all fraudulent activity on your credit report. At that point, you will be able to request an extended *7-year fraud alert* or a *credit freeze* at no cost. If you have Internet access, you can get an instant credit report at www.annualcreditreport.com. If your credit report has had a lot of imposter activity, though, it may take up to two weeks to receive it by mail.

AGENCY	PHONE NUMBER + ADDRESS	CONTACT DATE	CONTACT PERSON (NAME + TITLE)	NOTES OF CONTACT	DATE DISPUTE LETTER MAILED
EQUIFAX	800-685-1111 P.O. Box 740241 Atlanta, GA 30374 Equifax.com/personal/credit-report-services				
EXPERIAN	888-397-3742 P.O. Box 9532 Allen, TX 75013 https://www.experian.com/help				
TRANSUNION	888-909-8872 P.O. Box 6790 Fullerton, CA 92834 https://www.transunion.com/credit-help				
INNOVIS	1-800-540-2505 P.O. Box 1358 Columbus, OH 43216 http://www.innovis.com/				

STEP 2 — REPORT: FEDERAL TRADE COMMISSION (FTC)

It is important to file a complaint with the FTC. The FTC will not investigate your case, but after making a report, your information will be entered into the Identity Theft Data Clearinghouse, a nationwide data bank that documents instances of identity theft in the U.S. to assist law enforcement in the investigation and prosecution of identity thieves. The FTC prefers that complaints be filed online; however, if you do not have computer access, you may file a complaint by telephone or mail. If you file a complaint online, you can print out a copy of your report. Take the printed report to a notary public and sign it. Then, you will have an identity theft affidavit that can be copied and sent to local law enforcement agencies, creditors, and credit reporting companies.

FEDERAL TRADE COMMISSION	METHOD OF CONTACT	TIME	DATE	CONTACT PERSON (NAME + TITLE)	REPORT TAKEN	COPY REQUESTED	COPY RECEIVED
<p>FTC ONLINE FORM: WWW.FTC.GOV/IDTHEFT</p> <p>Phone: 877-438-4338 TTY: 866-653-4261</p> <p>Identity Theft Clearinghouse Federal Trade Commission 600 Pennsylvania Ave. NW Washington, DC 20580</p>	<input type="checkbox"/> ONLINE <input type="checkbox"/> PHONE <input type="checkbox"/> MAIL				<input type="checkbox"/> YES <input type="checkbox"/> NO	<input type="checkbox"/> YES <input type="checkbox"/> NO	<input type="checkbox"/> YES <input type="checkbox"/> NO
<p>NOTES OF CONTACT</p>							

If you did not print your FTC complaint, complete an FTC ID Theft Affidavit, which is available from the FTC. Fill in the blanks as completely as possible. Do not sign it until you are in front of a notary public.

STEP 2 — REPORT: OTHER REPORTS

EMPLOYER:

Consider notifying your employer if your Social Security number was compromised. Also, depending on the level of identity theft (i.e., purse/wallet), consider ordering new business cards.

U.S. SOCIAL SECURITY ADMINISTRATION:

For information regarding lost or stolen social security cards, go to the Social Security Administration Website (www.ssa.gov) or call 800-772-1213. Order a copy of your Social Security earnings record, which will be mailed to you for a fee, or obtain an immediate free copy at your local Social Security office. Go in person to the local office to report any discrepancies in your earnings and to ask for a corrected earnings report to be issued.

U.S. INTERNAL REVENUE SERVICE (IRS):

If you learn that somebody has been using your Social Security number for employment, contact the Identity Protection Specialized Unit at the IRS at 1-800-908-4490 to assist you with tax related problems that may arise and to have your Social Security number flagged to alert auditors to your stolen identity. If you experience tax problems due to your identity theft, complete an IRS form 911, available on the IRS Website (www.irs.gov) and send it to the address listed on the form to receive assistance from the U.S. Taxpayer Advocate. You can also reach the Taxpayer Advocate at 1-877-777-4778.

U.S. CITIZENSHIP AND IMMIGRATION SERVICES (USCIS) AND/OR U.S. DEPARTMENT OF STATE:

If your naturalization or citizenship certificate or your green card has been lost or stolen, go to the USCIS Website at www.uscis.gov or call 1-800-375-5283. For information about lost or stolen passports, visas, or arrival/departure records, visit the U.S. Department of State Website at www.state.gov for information. If you are not a United States citizen, you must contact your consulate to replace your passport. Some consulates will request a law enforcement report.

MINNESOTA DRIVER AND VEHICLE SERVICES:

If an identity thief has used your driver's license or state ID card or obtained either form of identification using your information, notify Driver and Vehicle Services to obtain a replacement. Complete a Confirmation of Identity Form at <https://dps.mn.gov/divisions/dvs/forms-documents/Documents/VictimofIdentityTheft.pdf> to request a "driving record flag" that will alert law enforcement officers that someone else may be using your identity. For more information, contact the Minnesota Department of Public Safety Driver and Vehicle Services, 445 Minnesota Street, Suite 170, St. Paul, MN 55101-5170, 651-297-3298, TTY 651-282-2463.

ARIZONA MOTOR VEHICLE DIVISION:

If an identity has used your driver's license or state ID card or obtained either form of identification using your information, notify Motor Vehicle Division to obtain a replacement. For more information, contact Arizona Department of Transportation, Motor Vehicle Division, 602-255-0072 or at <https://azdot.gov/mvd/contact-mvd>.

MINNESOTA BUREAU OF CRIMINAL APPREHENSION:

If someone has used your identity in a criminal prosecution, contact the Bureau of Criminal Apprehension (BCA) to question the identity on the criminal record. For information, go to the BCA Website (<https://dps.mn.gov/divisions/bca/Pages/criminal-history.aspx>) or call 651-793-2400. You will be asked to complete a Questioned Identity Form (<https://dps.mn.gov/divisions/bca/Documents/questioned-identity.pdf>). Additional information on how to deal with criminal identity theft can be found in the Criminal Identity Theft Road Map (<https://dps.mn.gov/divisions/ojp/forms-documents/Documents/Criminal%20Identity%20Theft%20Guide.pdf>).

ARIZONA DEPARTMENT OF PUBLIC SAFETY:

If you suspect that someone has used your identity in a criminal prosecution, contact the Department of Public Safety (DPS) to request a Record Review Packet to review the accuracy of your record. For information, go to the DPS (<https://www.azdps.gov/criminal-history-records>) or call 602-223-2222.

MINNESOTA FRAUD ENFORCEMENT PARTNERSHIP:

To report phone, mail, or email fraud and scams, contact the Minnesota Fraud Enforcement Partnership 1-866-347-0911 or at report@mnsccams.org.

ARIZONA ATTORNEY GENERAL:

To report phone, mail, or email fraud and scams, contact the Arizona Attorney General's Office at <https://www.azag.gov/complaints/consumer>.

STEP 2 — REPORT: ADDITIONAL RESOURCES

No publication can cover every conceivable situation that may arise for a victim of identity theft or financial fraud. You may have questions that are not answered in this publication. Help is available.

MINNESOTA OFFICE OF JUSTICE PROGRAMS:

Crime Victim Justice Unit
1-800-247-0390, ext. 3
445 Minnesota Street, Suite 2300; St. Paul, MN 55101-1515
<http://ojp.dps.mn.gov>

MINNESOTA ATTORNEY GENERAL'S OFFICE:

1-800-657-3787
TTY:1-800-366-4812
1400 Bremer Tower; 445 Minnesota Street St. Paul, MN 55101
<https://www.ag.state.mn.us/>

CITY OF PHOENIX POLICE DEPARTMENT:

Financial Crimes Detail
602-534-5940
200 W Washington Street; Phoenix, AZ 85003
<https://www.phoenix.gov/policesite/Pages/Financial-Crimes.aspx>

FTC'S CONSUMER RESPONSE CENTER:

1-877-ID-THEFT (438-4338)
Consumer Response Center
Federal Trade Commission
600 Pennsylvania Ave, NW; Washington, DC 20580
www.ftc.gov

IDENTITY THEFT RESOURCE CENTER:

1-888-400-5530
www.idtheftcenter.org

PRIVACY RIGHTS CLEARINGHOUSE:

www.privacyrights.org

MONEY SCAM PREVENTION:

www.fakechecks.org

NATIONAL CONSUMER'S LEAGUE FRAUD CENTER:

1-800-876-7060
www.fraud.org

REPORT SPAM:

spam@uce.gov

MEDICARE FRAUD:

1-800-633-4227
www.medicare.gov

CYBER EVENT RESOURCE:

CONSTANGY, BROOKS, SMITH & PROPHETE LLP

877.DTA.BRCH (877-382-2724)

WEBSITE: <https://www.constangy.com/practices-Cybersecurity-Data-Privacy>

EMAIL: BreachResponse@constangy.com

STEP 2 – REPORT: CHART FOR RECORDING CONTACTS WITH OTHER FEDERAL AND STATE AGENCIES

AGENCY NAME	PHONE NUMBER + ADDRESS	CONTACT DATE	CONTACT PERSON (NAME + TITLE)	NOTES OF CONTACT

STEP 3 — INVESTIGATE

Next, you need to discover and document how extensively the thief has used your identity. Start by reviewing your last few bank or financial account statements, your credit card bills, and your credit reports. Mark any activity or accounts that do not belong to you. Record information about any fraudulent activity or accounts in the following table. Contact law enforcement agencies and credit reporting companies to update your reports with any information received since making your original reports.

Legal protections are in place to help limit your financial loss for fraudulent transactions. The bank generally has up to 10 business days to investigate your claim of unauthorized electronic transactions (i.e., ACH, debit card). For more complex issues, they can take up to 45 days, but need to let you know why they need more time. If the bank cannot complete its investigation within 10 business days, they must temporarily put the disputed amount back into your account until they resolve the issue. This temporary refund is called “provisional credit.” If the bank finds that there was indeed an unauthorized transaction, the provisional credit becomes permanent. If the bank determines that the transaction was not unauthorized, they will take the provisional credit back. You will be notified when their investigation is complete along with their results.

A chart for recording this information is found on the next page of this Toolkit.

STEP 3 – INVESTIGATE: CHART FOR RECORDING UNAUTHORIZED TRANSACTIONS

COMPANY, BANK, OR OTHER INSTITUTION	PHONE NUMBER + ADDRESS	FRAUDULENT ACCOUNT NUMBER	AMOUNT INVOLVED	NOTES OF CONTACT

STEP 4 – DISPUTE

Write the fraud or security department of each credit reporting company and each creditor, company, debt collector, or financial institution associated with each fraudulent account. Request that each fraudulently used account be closed and removed from your credit report. You should also request a copy of all applications or business transaction records relating to your identity theft; the Fair Credit Reporting Act allows you to receive this information. You can use the form letters in this packet. Your letters must include the following:

1. Proof of your identity, such as a copy of your government issued ID card, (example: your driver's license);
2. Copy of your ID theft report from police and an executed ID Theft Affidavit (as a practical matter, we recommend sending ***BOTH*** a police report and an ID theft affidavit because some police reports do not include complete information);
3. List of each fraudulent item on your credit report.

If you follow this procedure, the credit reporting companies must remove fraudulent accounts from your credit report within 4 days unless they perform an investigation that proves the accounts to be yours. Within 30 days, creditors must also send you copies of their records regarding accounts and transactions that are the result of identity theft. Follow this procedure for every account or transaction that is not yours. Send your letters by certified mail, return receipt requested, and keep a copy.

A chart for recording this information is found on the next page of this Toolkit.

STEP 4 – DISPUTE: LOG OF DISPUTE LETTERS

Recording Dispute Letters to Credit Bureaus, Creditors, Debt Collectors, and Financial Institutions.

INFORMATION ABOUT BUSINESS OR FINANCIAL INSTITUTION (BANK, CREDIT CARD COMPANY, BUSINESS, DEBT COLLECTOR)		NOTES OF CONTACT
NAME OF COMPANY		
PHONE + ADDRESS		
ACCOUNT NUMBER		
CONTACT PERSON (NAME/TITLE)		
CONTACT DATE:		DATE OF FOLLOW-UP LETTER:

INFORMATION ABOUT BUSINESS OR FINANCIAL INSTITUTION (BANK, CREDIT CARD COMPANY, BUSINESS, DEBT COLLECTOR)		NOTES OF CONTACT
NAME OF COMPANY		
PHONE + ADDRESS		
ACCOUNT NUMBER		
CONTACT PERSON (NAME/TITLE)		
CONTACT DATE:		DATE OF FOLLOW-UP LETTER:

Make copies of these forms, as necessary.



STEP 4 – DISPUTE: IDENTITY THEFT RECOVERY LOAN

Tradition Capital Bank can help you meet your short-term cash needs while you work on recovering your identity and money that was stolen from your account.

If you need funds to fill your car with gas or get some groceries, contact us to apply for an *Identity Theft Recovery Loan*.*

**For more information, please contact a member of the Tradition Capital Bank team at (952)-806-6600. Offer of credit is subject to credit approval.*

STEP 5 – MONITOR:

Because you can get one free report per credit reporting company per year, it is a good idea to stagger your report requests. Ask for a free credit report from a different company every three to four months so that you can continuously monitor your credit. Make sure that you review all bank and credit card statements monthly and dispute fraudulent items immediately. Keep an accurate record of all people and businesses that contact you regarding your identity theft and any follow-up contacts that you make. Keep a copy of all letters that you send and all information that you receive.

COMPANY, BANK, OR OTHER INSTITUTION NAME	PHONE NUMBER + ADDRESS	CONTACT PERSON (NAME + TITLE)	DATE OF CONTACT	NOTES OF CONTACT

STEP 6 – PREVENT

Take the following actions to prevent future identity thefts.

WATCH YOUR TRASH:

Shred any documents with account or identity information before you throw them away or recycle them. This includes bills, account statements, bank statements, tax returns, and credit card offers.

WATCH YOUR MAIL:

If possible, install a mailbox that locks so that thieves cannot steal your mail. When you go out of town, contact your local post office and ask that your mail be held until you return.

CONSIDER A CREDIT FREEZE:

A credit freeze makes your credit report unavailable for viewing by most potential creditors unless you take steps to thaw it. It takes about 3 business days to thaw a credit freeze. When a potential creditor makes a request to see your credit report, the reporting agency notifies the potential creditor that your report cannot be viewed unless you take steps to release your credit report. If you are a victim of identity theft, there should be no charge for placing a freeze on your credit; however, if you are not a victim or if you are requesting a thaw, you may be charged a nominal fee. You can request a credit freeze in writing with each credit reporting company. Send your request by certified mail.

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013

Trans Union Security Freeze

P.O. Box 6790
Fullerton, CA 92834-6790

Innovis Security Freeze

P.O. Box 1373
Columbus, OH 43216-1373

OPT OUT OF CREDIT CARD OFFERS:

Visit www.optoutprescreen.com and follow the instructions or call 1-888-5-OPT-OUT (1-888-567-8688).

GET ON THE FEDERAL “NO CALL” LIST:

Visit <https://www.donotcall.gov/> or call 1-888-382-1222 to register your home and cell phone numbers. After your numbers have been placed in the registry for 31 days, most telemarketers should not call you. Charities, political organizations, and businesses with whom you currently do business are exempt and are generally allowed to contact you unless you specifically ask them not to.

SURF SAFELY:

Protect email and other online accounts with passwords. Do not use passwords that are easily guessed, examples: your name, your birthdate, or your telephone number. Do not keep a list of your passwords on your computer or near your computer. Do not open or respond to emails unless you know the sender. Do not respond to emails asking for passwords or personal information. Find out more at <https://consumer.ftc.gov/identity-theft-and-online-security/online-privacy-and-security>.

VERIFY CHARITIES BEFORE YOU DONATE:

Visit GuideStar at <https://www.guidestar.org> (1-800-421-8656) or Charity Watch at www.charitywatch.org (773-529-2300) before donating to make sure the charity is legitimate.

STRENGTHEN PASSWORDS:

A password is only helpful if it cannot be guessed or accessed by others. As simple as that sounds, it is a basic tenet that few users follow. There have been countless stories of significant cyber breaches where the password used was Password1234 or Admin1234. Basic, default, easy to remember, often used passwords are typically the first try of anyone attempting to access an account they do not have the right to see.

- **USE STRONG PASSWORDS.** Passwords are a series of characters, numbers, letters, and symbols. Skip using the obvious ones or ones easily associated with you (meaning, easily guessable). Do not use birthdates or anniversaries, pet names, or recognizable famous words. Strong passwords should not be easy to remember or imagine.

- Strong passwords exceed the recommended character minimums
- Strong passwords use phrases, not just words, to make them more memorable, yet less predictable
- Strong passwords alternate numbers or special characters for letters where applicable
- Strong passwords have combinations of letters, numbers, special characters in them
- Strong passwords do not have your username, your family name, easily associated dates in them
- Strong passwords are real passwords, not defaults such as Password1234 or Admin1234, or variations of such
- Strong passwords are unique to you, and should be protected, not shared

- **CHANGE YOUR PASSWORD FREQUENTLY.** The longer you use a password, the more opportunities there are to be hacked. By frequently changing your password, it restarts the process of anyone trying to guess it or hack it. Many companies and services require changing passwords at regular intervals, such as every three to six months, and even block you from reusing previous passwords.

- **DO NOT REUSE PASSWORDS.** We are drawn to consistency, especially when it makes our lives easier. That is why so many users repeat passwords or have a cycle of several that they use in combination or variation across most sites, apps, and services. Cybercriminals know this, which means they know that they likely can access other accounts if they can access one.

- **STORE YOUR PASSWORDS SAFELY.** Sites and browsers are always “offering” to store or save your login information. It is certainly more manageable, especially when using strong, unique passwords across multiple entities, but it increases your vulnerability. Storing all your passwords through a browser puts them at risk because if your account gets hacked, hackers have access to all your passwords by accessing one. Browser features are convenience-based, not security-driven.



You try to follow suitable password hygiene protocols, using strong, unique, random characters, but then keep them all on notes on your desk, taped to your monitor, or in an unsecured note file or spreadsheet on your computer. Do not do that.

- **CONSIDER USING A PASSWORD MANAGER.** A Password Manager is a computer program that allows users to store and manage their passwords for local applications or online services such as web applications, online shops, or social media. Ensure that the Password Manager includes these minimum security standards: 256-bit encryption and Two Factor Authentication. Make sure you use a very strong password for the master password because it is the door to the vault with all of your other passwords.

- **ENABLE TWO FACTOR AUTHENTICATION WHEN OFFERED.** Two factor authentication (2FA), sometimes referred to as two-step verification or dual-factor authentication, is a security process in which users provide two different authentication factors to verify themselves. For example, getting a text with a one-time code, along with your user ID and password.

SUBSCRIBE TO IDENTITY AND CREDIT MONITORING SERVICE:

Protect your security with identity and credit monitoring. This service not only alerts you about threats, it should also assist you to restore your identity to its pre-theft status. There are many products for you to consider. Here are some available products. *Note: Tradition Capital Bank receives no revenue from your subscription to these services and is not affiliated with these providers.*

COMPANY		
PLAN COST	\$12 TO \$32 PER MONTH FOR FAMILY PLANS, IF BILLED ANNUALLY	\$14.95 TO \$34.95 PER MONTH
PLAN TYPES	INDIVIDUAL AND FAMILY	INDIVIDUAL AND FAMILY
ID THEFT INSURANCE COVERAGE	\$1 MILLION PER ADULT	\$3 MILLION
CREDIT BUREAU MONITORING	3 CREDIT BUREAU MONITORING ON ALL PLANS	1 OR 3 CREDIT BUREAUS MONITORING AVAILABLE
FREE TRIAL PERIOD	14 DAYS; 60-DAY MONEY-BACK GUARANTEE ON ANNUAL PLANS	30 DAYS
FRAUD ALERT DELIVERY	REAL-TIME VIA TEXT, EMAIL	REAL-TIME PROTECTION
ADDITIONAL SERVICES	ANTIVIRUS, VPN WITH SAFE BROWSING, PASSWORD MANAGER	VPN, MALWARE PROTECTION, PASSWORD MANAGER
FORBES ADVISOR RATING ¹	5.0 – BEST VALUE FOR YOUR MONEY	4.3 – RESTORATION SUPPORT
BUYERSGUIDE RATING ²	10.0 – BEST OVERALL	8.3
CONTACT INFORMATION	WWW.AURA.COM 1-833-928-4823	WWW.IDSHIELD.COM 1-866-349-3735

¹Information provided on Forbes Advisor is for educational purposes only and based on a 5-point scale.

²The ratings are based on the expert opinion of BuyersGuide.org editors and on underlying technology that analyzes decisions made by similar users to provide individual, targeted recommendations on a 10-point scale.

SAMPLE LETTER TO CREDIT REPORTING COMPANIES

Sender's Name:
Sender's Address:
Sender's City/State/Zip:

Date:

Equifax
FRAUD DEPARTMENT
P.O. Box 740241
Atlanta, GA 30374
Certified mail no.

Experian
FRAUD DEPARTMENT
P.O. Box 9532
Allen, TX 75013
Certified mail no.

Transunion
FRAUD DEPARTMENT
P.O. Box 6790
Fullerton, CA 92834
Certified mail no.

Re: Dispute or File No.

This letter will confirm that I am a victim of identity theft. If you have not already done so, please place an extended seven year fraud alert on my credit report and remove the first five digits of my Social Security Number from my credit report. In reviewing my credit report, I have found the following fraudulent inquiries/accounts which are related to transactions that were not initiated by me:

I am disputing these entries to my credit report under the Fair Credit Reporting Act as amended by the Fair and Accurate Credit Transactions Act because the transactions represented by the entries were not initiated by me but by an imposter. Please block the disputed entries from my credit report because they are attributable to identity theft. If you do not remove the disputed entries, please provide proof of your reinvestigation and the reason for non-removal.

Please add the following statement to my credit report: FRAUD VICTIM! DO NOT EXTEND CREDIT WITHOUT CONTACTING ME PERSONALLY. MY DAYTIME PHONE NUMBER IS _____.

I am enclosing a copy of my police or sheriff's report, ID theft affidavit, and ID for your convenience. Please do not hesitate to contact me if you have questions regarding this matter.

Sincerely,

Signature:
Printed name:

SAMPLE LETTER TO BUSINESSES

Sender's Name:
Sender's Address:
Sender's City/State/Zip:

Date:

Business Name:
ATTN: Collections or Fraud Department
Business Address:
Business City/State/Zip:
Certified mail no.

Re: Account or File No.

This letter will confirm that I am a victim of identity theft. I have made a report to law enforcement and have requested that an extended seven year fraud alert be placed on my credit report. In reviewing my credit report, I have found the following fraudulent inquiries, accounts, or debts at your business which are transactions that were not initiated by me:

I am disputing these inquiries, accounts, debts, and entries to my credit report under the Fair Credit Reporting Act as amended by the Fair and Accurate Credit Transactions Act because these transactions were not initiated by me. Please close the referenced accounts and take whatever steps are necessary to remove the disputed entries from my credit report because they are attributable to identity theft. Please note that the Fair Credit Reporting Act places a duty on you to transmit accurate information to credit reporting agencies including informing credit reporting agencies that I have disputed the above-referenced debts or accounts. **I am disputing both the accuracy of the alleged debt and the specific information about the debt furnished by you to credit reporting agencies.**

As a victim of identity theft, I am entitled to a copy of all documentation regarding the accounts or debts referenced above. Please provide the following to me at the above address:

- Application records
- Screen prints of internet or telephone applications
- Account statements
- Payment/charge slips
- Summary of investigation or investigator's report
- Delivery address(es)
- Telephone numbers and identifying information used to open or access the account
- Any other documents associated with the account.

I will be furnishing these documents to law enforcement agencies in order to assist with their investigation and the prosecution of my case.

Please note that the federal Fair Debt Collection Practices Act prevents you from placing a disputed debt or account with a collection agency – especially when you have been notified that a debt or account was fraudulently obtained by identity theft.

I am enclosing a copy of my police or sheriff's report for your convenience. Please do not hesitate to contact me in writing if you have questions regarding this matter.

Sincerely,

Signature:

Printed Name:

SAMPLE LETTER TO BILL COLLECTORS

Sender's Name:
Sender's Address:
Sender's City/State/Zip:

Date:

Collection Agency Name:
Address:
City/State/Zip:
Certified mail no.

CEASE AND DESIST LETTER NOTICE OF DISPUTED DEBT – IDENTITY THEFT REQUEST FOR INFORMATION

Re: Account or File No.

This letter will confirm that I am a victim of identity theft. I have made a report to law enforcement and have requested that an extended seven year fraud alert be placed on my credit report. You have contacted me regarding the above-referenced alleged debt. **This letter will serve as notice to you that the underlying transaction was not initiated by me but by an imposter, that I am disputing the above-referenced debt, and that I am a victim of identity theft.**

Under the Fair Credit Reporting Act and the Federal Fair Debt Collections Practices Act, you have a duty to report this dispute to the creditor, your client. You are prevented from making a report of this disputed debt to credit reporting agencies. If you have not already done so, please close the referenced accounts. If you have furnished information to credit reporting agencies, please take whatever steps are necessary to remove the disputed entries from my credit report because they are attributable to identity theft. Please note that the Fair Credit Reporting Act places a duty on you to transmit accurate information to credit reporting agencies including informing credit reporting agencies that I have disputed the above- referenced debts or accounts. **I am disputing both the accuracy of the alleged debt and the specific information about the debt furnished by you to credit reporting agencies.**

As a victim of identity theft, I am entitled to a copy of all documentation regarding the accounts or debts referenced above. Please provide the following to me at the above address:

- Application records
- Screen prints of internet or telephone applications
- Account statements
- Payment/charge slips
- Summary of investigation or investigator's report
- Delivery address(es)
- Telephone numbers and identifying information used to open or access the account
- Any other documents associated with the account.

I will be furnishing these documents to law enforcement agencies in order to assist with their investigation and the prosecution of my case. Their job will be easier if your records are produced in a form that can be used in court. I am enclosing a standard business records affidavit, and I respectfully request that you execute it or a similar business records affidavit to accompany the records that you send to me.

Other than providing account documentation, I request that you cease communications to me about the alleged debt referenced above. The Fair Debt Collection Practices Act requires that you honor this request.

I am enclosing a copy of my police or sheriff's report, ID theft affidavit, and photo ID for your convenience. Thank you in advance for your help in resolving this matter.

Sincerely,

Signature:

Printed Name:

RESOURCES TO HELP YOU GET ORGANIZED AND
REESTABLISH SAFETY AFTER IDENTITY FRAUD.



TRADITION
CAPITAL BANK