ID THEFT AND FRAUD MONITORING GUIDELINES

PREVENTING and LIMITING ID THEFT DAMAGE

Here are the recommended steps that you follow to help prevent any damage to your financial history:

1. Assume your personal identifying information is already compromised and waiting to be used for identity theft.

2. Go to one of the credit reporting agencies and obtain a free credit report so you can establish a "baseline" of your credit.

3. Place a ***CREDIT FREEZE*** on your credit (NOT a *fraud alert*) with each of the reporting agencies.

4. Contact each of your financial institutions (i.e., banks, investment companies, etc.) and place fraud alerts on each of your accounts.

5. In about 4-5 months get a free credit from one of the two other credit reporting agencies and watch closely for any activity that you can't account for.

6. In about 9-10 months do the same thing from the 3rd reporting agency. Continue this practice of monitoring your credit on a "rolling basis".

7. If you **HAVE** been a victim of identity theft file a report with your local agency, at **IdentityTheft.gov** and at **IC3.gov**

If you find the steps 5 & 6 burdensome, you could consider subscribing to a credit monitoring service such as LifeLock (or similar service). For a monthly fee they would take care of those steps for you.

ULTIMATE LEVEL OF PROTECTION – *Credit Freeze/Security Freeze*

This is the maximum level of protection over your credit. This feature prevents lenders from accessing your credit history without your permission unless you already have an account with them. This is a critical step to prevent criminals from opening new accounts at new institutions. In this case a request must be made with each credit reporting agency. **NOTE:** If you need to complete a credit application to obtain a loan you must first "turn off" the protection, then turn it "on" again once your loan is obtained.

CHECK SAFETY

NEVER mail a check from your home mailbox unless it is a locked mailbox. The routing numbers on the bottom of your check are a direct link to your bank account. Always place your checks & payments in secured mailboxes, but theft of mail can still occur in USPS distribution centers and elsewhere. Request that your bank electronically send checks on your behalf. ACH transactions to known recipients are inherently more secure and likely to be reimbursed than personal checks.

DEBIT/CREDIT/ATM CARD SAFETY

To reduce the chance of being a victim of "skimming" (i.e., having someone make a copy of your magnetic stripe to create a fake card with your account information) when accessing a ATM, gas pump, etc.:

1. Before you place your card in the slot, grab onto the card slot and trim pieces and try to move them back & forth. If any part moves, DO NOT use that machine.

2. Before entering your PIN, try to lift up on the edge of the keypad, especially those which are horizontal. If the keypad moves, DO NOT use that machine.

3. When entering your P.I.N. after having inserted your card, cover the keypad with your other hand, even if there is a privacy shield over the keyboard to prevent a hidden camera from recording your PIN (sometimes there is a pinhole camera in the shield).

4. Even the new "chip cards" can be skimmed because the cards have a magnetic stripe on them so they work in older card readers. Watch out for attachments to chip card readers, especially if there is a piece that seems to surround the slot or is a slightly different color. If there is one, try pulling on it to see if it moves. If it does, DO NOT use that machine.

5. Check with your credit/debit card company to see if they provide an option for text alerts. If so, set the threshold to $0 so that a text message is sent to your cell phone every time a transaction is made. **This is the very best way to be alerted in "real time" that someone is using your credit card.**

PAYING AT RESTAURANTS

Consider paying with cash at restaurants where you hand your debit or credit card to a server who takes the card out of your sight temporarily. This provides the server an opportunity to either write down, electronically skim, or simply use their cell phone to photograph both sides of your card for later use.

PEER TO PEER PAYMENTS

Payment methods such as Zelle, CashApp, Apple Pay, Venmo, PayPal, etc. are all highly vulnerable and frequently used by scammers. Only use these methods of payment with friends or family. If someone you don't personally know requests payment using this method it is likely fraud. The person who receives your money will likely go unidentified by law enforcement and you won't be reimbursed by these companies or your bank.

CRYPTOCURRENCY

Bitcoin and other such forms of cryptocurrency are commonly utilized by scammers in fraud schemes. Never withdraw cash from your bank account and deposit into a Bitcoin ATM or otherwise use your money to send money to Bitcoin wallets. These wallets are anonymous and international. The recipient of your money will not be identified and you will not be reimbursed. No legitimate company or law enforcement agency will ask you to do this.

DETECTING MAIL THEFT

Identity theft and check fraud often involve the US mail. The United States Postal Service (USPS) now offers a service called ***Informed Delivery***. This is an excellent free service that will e-mail you a photograph of each piece of mail that is expected to be delivered to your home each day. That way you will know if someone has accessed your home's mailbox and selectively removed a single piece of mail such as a statement from your bank or investment company. **Failing to sign up for this service may actually make you more vulnerable** because thieves are now signing up for this service on your behalf, thereby notifying them of the mail to be expected at your home.

Go to https://informeddelivery.usps.com to sign up.

Updated 8/22/24

IRS IMPERSONATION SCAMS

IRS Impersonation scams can be reported at the following website:

https://www.treasury.gov/tigta/contact_report_scam.shtml

INTERNET-BASED CRIMES

Go to the website *www.IC3.gov* and complete an on-line report.

PAYING AT GAS STATIONS

Gas pump skimmers are a common point of compromise. There is little you can do to detect such a skimmer which is usually installed internally at the pump furthest from the store and most out-of-view of the employees. Your best course of action is to pay with cash or consider using a prepaid gas card. In addition to skimmer protection, this would allow you to obtain the "cash price" at stations charging different prices. If your phone has a Bluetooth option, turn it on, stand near the pump for a minute or so before using it. If a new Bluetooth device suddenly appears, that may indicate a skimmer is on the pump. Don't use the pump and notify the station personnel.