WASHINGTON TRUST®

What we value is you.®

Fraud Victim Resource Guide

If you have been targeted in a scam or ID theft scheme, you are now at higher risk to be targeted for fraud in other ways. The guidance below contains best practices we recommend to customers when faced with this type of situation.

- ❒ **If you have sent any funds to fraudsters, contact the agency or company used to send the funds and make a report** (i.e. FedEx, US Postal Service, UPS, Western Union, etc.). They may be able to assist you in recovering funds.
- ❒ **Cut off all conversation and communication with the fraudsters.** If you were involved in a scam situation, be prepared for the scammers to make threats and/or tell you that the Bank is lying, to attempt to lure you back in. Report any threats to local police.
- ❒ **You should file a police report and a report with the Internet Crime Complaint Center at www.ic3.gov**, to document the scam or ID theft attempt. This will prove valuable in the event of future ID theft attempts and will be necessary to unwind any fraudulent accounts opened in your name now or in the future. The IC3 database is also used by law enforcement to identify victims and facilitate restitution, in the event a suspect is arrested or funds are seized.

Recommendations for mitigating the impact of fraud and identity theft:

- ❒ **Review credit reports and contact Credit Reporting agencies and Chex Systems for unauthorized inquiries or accounts.** Consumers can request a free copy of their credit report from each of the 3 major credit reporting agencies (Equifax, Experian and TransUnion) one time every 12 months through the website www.annualcreditreport.com. You may also reach each bureau directly at:
  - ➤ **EQUIFAX, www.equifax.com [equifax.com], 888-766-0008**
  - ➤ **EXPERIAN, www.experian.com [experian.com], 888-397-3742**
  - ➤ **TRANS UNION, www.transunion.com [transunion.com], 800-680-7289**
  - ➤ **Chex Systems Inc., ChexSystems.com, 800-887-7652**
- ❒ **Monitor Washington Trust accounts and accounts at other financial institutions** daily for unauthorized transactions, even ones you don't regularly use.
  - Report any suspicious activity promptly to the relevant institution(s). Even if no funds have been lost, you should file a police report to document the incident
  - If you have sent any funds via a Bitcoin ATM or cryptocurrency transaction, immediately take all receipts and relevant wallet details to the State Police and file a report. They may be able to assist in tracing funds, but minutes matter, so don't wait.
- ❒ **Strengthen your Security**
  - Contact the credit bureaus to place an extended fraud alert on your credit bureau. The credit bureaus will require documentation from you to verify the claim of ID theft. The alert remains in place for 7 years and will require banks to contact you at the method you specify in the alert, prior to granting credit in your name.
  - Create a personal profile password for your accounts with Washington Trust. Your branch or our Customer Solutions Center can assist with this. This serves as an extra layer of security against account takeover.

continued on next page

❒ **Practice good password hygiene:**

- Do not reuse passwords across applications, websites or social media.
- Change online banking and email passwords frequently. If not recently changed, now is a good time.
- Use complex passwords that will be easy to remember, but difficult for a fraudster to guess.
- Avoid dictionary words (even with slight variations, like "Pa$$word"), pets names, and other information that can be gleaned from social media.
- Passphrases are a good way to create complex, but easy to remember passwords. A passphrase takes an easy sentence and shortens it down to a unique password. For example, if you're a Patriots fan, you could shorten the phrase "Former Patriots quarterback Tom Brady has 7 Superbowl rings" to "FPqTBh7$r" by taking the first letter of each word and substituting the "s" for a "$".
- Take advantage of multi-factor authentication tools for your financial accounts, email and cell phone accounts. Contact your providers to inquire about available options.
- Never provide one-time passwords to anyone calling or texting you, as this is a common tactic to break into your accounts.
- Be discerning about what you post on social media. For example, if you want to use your high school mascot, pet's name or street you lived on as a child as a password or security question, make sure you're not posting that detail on Facebook!
- Be wary of anyone contacting you for any reason requesting return of funds or telling you to send or deposit funds to another account. It's almost always a scam. If it sounds too good, or too bad to be true, it probably is!

If You've Become The Victim of Theft

In addition to the above recommendations, **notify your bank of the theft immediately** and ask about proactive security measures you can use to protect your accounts, such as passwords and multi-factor authentication. Below are some additional steps you can take to reduce your risk of fraudulent activity or identity theft, in the event of a stolen wallet or purse:

❒ **Cancel and reissue Debit and Credit cards**

❒ **Stop payment on any stolen checks**, or close the impacted account(s)

❒ **File a police report.** This may prove helpful in the event of future fraud, and for insurance purposes.

❒ **Replace your ID or Driver's license**

❒ **Replace your Social Security card**

- To obtain a new Social Security card, you can contact the Social Security Administration at 1-800-772-1213 to request a replacement card, or visit www.ssa.gov to register for a "MY Social Security" account.
- You should also report the loss of the Social Security card to the IRS at 1-800-908-4490 or www.irs.gov. This can help stop criminal from submitting a tax return in your name and receiving your refund check.

❒ **Consider changing your locks** if your keys were stolen, and can be tied to your residence or vehicle.

❒ **Change any passwords** that you had written down in your wallet or purse

❒ **Make a list of other items that may need replacing**, such as prescriptions, insurance cards, membership/discount cards.

❒ **And remember, only carry what you need!** Don't keep your social security card, passport or birth certificate in your wallet or purse. Losing these documents can greatly complicate and compound the impact of identity theft.

If you or a family member has become the victim of fraud, Washington Trust can help.
Visit your local branch or call us at 800-475-2265.