



## What is Identity Theft?

Identity theft occurs when someone uses your personal information to commit fraud. Identity theft can happen to anyone and is quickly becoming a major problem in our nation. Being a victim could cost you substantial time, money, and resources to clear your name. There are various ways fraudsters steal identities: steal your mail with personal information on it, call you pretending to be from your financial institution, or falsifying change of address documents.

Another form of identity theft commonly used is "phishing". "Phishing" is a new scam where e-mail is sent from a seemingly legitimate financial institution asking for personal and financial information. Information provided to these sources will be redirected to the fraudsters.

### What are a few things you can do to prevent identity theft?

- Never reply to an e-mail or click on a link from within an e-mail asking you to update your account information unless you confirm the e-mail actually originated from your financial institution. You should call your financial institution using commonly used telephone numbers, found in the telephone book or a monthly statement, to confirm the authenticity of the e-mail message.
- Unless you initiate the call, you should never provide account or personal information to someone claiming to be an employee of Pearl Harbor Federal Credit Union or any other financial institution.
- Use different passwords for online banking, e-mail, PIN numbers and other online accounts. Refrain from using easily guessed passwords, such as your name, your pet's name, or your spouse's birthday.
- Regularly update antivirus software and operating system updates to reduce computer threats.
- Drop mail off at U.S. Postal Service collection boxes rather than leaving your mail in your mailbox overnight or over the weekend.
- Tear up or shred mail and documents with personal information before throwing it away. Fraudsters have been known to steal

information from household garbage, commonly called "dumpster diving".

- Promptly review monthly statements and bills for suspicious transactions and large or unexplained purchases. Review your credit report annually.
- If you don't receive your monthly statement or bill for the month, call the financial institution or company to inquire if it was sent out and verify your mailing address with them.

### **What is Pearl Harbor Federal Credit Union doing to prevent identity theft?**

- PHFCU will never give account information to a requesting person without proper identification.
- PHFCU will electronically store picture identification and signatures. Visit any PHFCU branch for more information.
- PHFCU does not save passwords for our online banking and member telephone service. PHFCU will reset passwords only after you have sufficiently answered a series of questions to verify your identity.
- PHFCU's online banking system is secured with 128-bit data encryption to provide a secure transfer of information between your computer and PHFCU's online system.
- PHFCU will never request personal and/or account information via e-mail or telephone. If you receive an e-mail or phone call from PHFCU requesting account information, please forward the e-mail to [fraud@phfcu.com](mailto:fraud@phfcu.com) or call (808) 73-PHFCU (737-4328) to report incident immediately.

### **What can you do if you're a victim of identity theft?**

Contact TransUnion, Equifax, or Experian to place a fraud alert. When you place a request with of the credit bureaus, the request will be shared and updated amongst the three bureaus.

A fraud alert is an indicator placed on your credit report record by the major credit bureaus. When you or someone else attempts to open a credit account (credit card, loan, etc.) and you have a fraud alert in place, you will be contacted to verify your intent to open this account. If you cannot be reached by phone, the credit account will not be opened.

Once the fraud alert is established, your name is removed from all pre-approved credit and insurance offers for two years and a credit report will be mailed to you within two weeks.

You should also let your financial institutions know about the fraud and change all account numbers, ATM/Debit cards, and credit cards.

For additional tips on how to prevent identity theft or what to do if you're a victim, you can contact a Postal Inspector at the United States Postal Inspection Service.

Additionally, download the ID Theft affidavit at the Federal Trade Commission's "Fighting Back Against Identity Theft" website. The affidavit will help you report the fraud to other institutions with one form. You can also contact the Federal Trade Commission to report the fraud at 1-877-ID-THEFT (1-877-438-4338). They will process your complaint, help clear fraudulent activities, and guide you with further steps to stop the fraud.