HAWAII STATE
FEDERAL CREDIT UNION

ONLINE FRAUD PREVENTION GUIDE – JUNE 1, 2020

ONLINE BANKING SECURITY

At Hawaii State FCU, the safety and security of your financial information is of utmost importance to us. It is equally important for YOU to be educated and informed about the types of online fraud and theft that could compromise your personal information and finances. Please read the following important information on how to keep your accounts safe.

MEMBER CONTACT

Hawaii State FCU or any of its employees will never call, email or otherwise contact you and ask for your user name, password or other online banking credentials. If you are contacted by anyone requesting this information, DO NOT provide the information. Instead, hang up and call our Member Service Center immediately at **(808) 587-2700** (Oahu) or toll-free **1-888-586-1056**. You may be the victim of a fraudster.

If you suspect fraud on your account, notify Hawaii State FCU immediately so that we may take action to protect your account. You may use Online Banking to review account transactions or call our Member Service Center.

ACCESSING ONLINE BANKING

To access your account using Online Banking, you will need to use your User ID and password. You may change your password within Online Banking by clicking on the My Settings link. We recommend that you change your password regularly. For security purposes, it is recommended that you memorize your password and do not write it down. You are responsible for keeping your password, account number, and other account data confidential. This is extremely important to prevent unauthorized use of your account. You agree that you will be responsible for all transfers and payments made from your account by anyone to whom you give your user ID and password, even if their use is beyond your instructions.

BUSINESS ACCOUNTS

Business members must implement sound security practices within your place of business to reduce the risk of fraud and unauthorized transactions. Such practices may include frequent online review of your accounts because business accounts do not have the same consumer protection rights as consumer accounts.

CONSUMER ACCOUNTS

If you believe your password has been lost or stolen and you notify us within two business days after you learn of the loss or theft, you can lose no more than $50 if someone used your Password to conduct unauthorized electronic funds transfers without your permission. If you do NOT notify us within two business days after you learn of the loss or theft of your Password, and we can prove we could have stopped someone from using your Password to conduct unauthorized electronic funds transfers without your permission if you had told us, you could lose as much as $500. After 60 days, you could be legally liable for the full amount. The Consumer Electronic Fund Transfers Agreement and Disclosure provides detailed information. Please let us know if you would like another copy.

BEWARE OF PHISHING EMAILS

Phishing e-mail messages and the websites they link to typically use familiar logos and familiar graphics to deceive individuals into thinking the sender or website owner is a government agency or a company they know. Sometimes the phisher urges intended victims to “confirm” account information that has been “stolen” or “lost.” Other times, the phisher entices victims to reveal personal or account information by telling them they have won special prizes, earned exciting rewards, or that information is needed to deposit funds into the account. There is no way to completely eliminate the risk of receiving a phishing attempt. The most important thing to remember is not to respond.

OTHER IMPORTANT TIPS TO CONSIDER

Here are some other important tips to help you better protect yourself:

- Create “strong” passwords on all your financial, email and online retail accounts. The passwords should have numbers, upper- and lower-case letters and symbols. Avoid using your first or last name as a user ID.
- Never use for a password the last four digits of your social security number, your maiden name, date of birth, middle name, child’s name, pet’s name or anything else easily discovered or guessed.
- Never share User IDs, passwords, PIN numbers, dynamic tokens, etc. with anyone. Do not leave them in an area that is not locked or secured.
- Do not use the same login or password on any other website or software.
- Obtain and install antivirus, anti-malware and anti-spyware software, and consider installation of a firewall and make sure it is automatically updated by the vendor or take necessary steps to keep it updated.
- Limit or eliminate unnecessary web surfing and/or email activity on computers used for online banking.
- Clear the internet browser’s cache before and after visiting websites.
- Verify use of a secure session (https:// and not http:///) for online banking sessions.
- Avoid saving passwords to a computer.
- Never leave a computer unattended when using any online banking service, and always lock your computer when away.
- Be cautious of accessing a financial institution’s website for online banking from a public computer such as at a hotel, library, coffee shop or other public wireless (WiFi) access point.
- Online and mobile phone applications, text messages, instant messages and calls from unfamiliar or suspicious sources that request personal financial information and passwords should be declined and, when appropriate, promptly deleted. Do not open any links that the message may contain.
- Be suspicious of any employment position that requires use of a personal account for business purposes. Such offers for employment as a mystery shopper, payment processor, etc. where you are required to use your personal account for someone else’s business purposes, may not be legitimate.
- Be cautious of requests to move business funds through personal accounts.
- If you are approached to participate in such schemes, immediately contact local law enforcement, the FBI or the Secret Service to let them know.
- Educate family members and company personnel on good cyber security practices, including the information in this guide.

BEWARE OF COMMON PLOYS

Funds credited to your account may be available for your use before we receive final payment. If we do not receive final payment, you are responsible for any deficiency in your account. For example, credit for an ACH or electronic transfer or check deposited to your account may be reversed if it is fraudulent, made in error, or there are insufficient funds in the originating account. *It may be sixty days (and sometimes a year or longer) before the Credit Union receives final payment, depending on how funds are deposited into your account*.

A common ploy used by fraudsters may be to make a fraudulent ACH deposit into your account, or to send you a fictitious cashier's, government or other check. The fraudster may hire you to be a "mystery shopper"; may tell you they need help receiving payment or a refund; or may pay you extra for goods or services that you're selling. Sometimes the fraudster may pretend to have a romantic relationship or befriend you.

The fraudster may ask you to send a wire, ACH, gift card or money order after the fraudulent funds are deposited to your account. Sometimes, the fraudster may "allow" you to keep a portion of the funds. Ultimately, the amount credited to your account is reversed because the original deposit was fraudulent. As a result, your account will have a deficit because of the funds you sent to the fraudster. *You remain responsible for the deficiency in your account.*

The sooner you notify the Credit Union, the sooner we can take action to try to stop a transaction and to limit your loss.

INCORRECT DEPOSITS

If you are aware that funds that you are not legally entitled to have been deposited into your account, you are required by law to take reasonable measures to discover and notify the owner of the funds. You also should notify the Credit Union so that we can reverse any incorrect ACH deposits. It is a criminal offense punishable by fine or imprisonment to withdraw funds from an account knowing that the funds were deposited under a mistake as to identity or other facts. See Haw. Rev. Stat. § 708-830(3).

You can learn more about online safety at the following government websites:

www.consumer.ftc.gov/features/scam-alerts
www.idtheft.gov
www.onguardonline.gov