Learn How To Protect Yourself

Online fraud occurs when someone poses as a legitimate source (like your bank, favorite shopping site or internet service provider) in order to obtain your personal information. This information is then used to conduct transactions on existing accounts. Methods used by fraudsters to commit online fraud are typically fake emails, pop-up messages and/or web sites.

Your Relationship With Home Loan State Bank

Home Loan State Bank will never ask you to provide, verify or update your personal information by sending an email, a text or using a pop-up message or link. If you receive such a message that appears to be from Home Loan State Bank requesting you to provide or validate personal information, DO NOT RESPOND.

Home Loan State Bank representatives may call you regarding activity on your account or you may be contacted through our automated systems to verify transaction activity on your account(s), such as debit card or eBanking activity. For your protection, we may ask you to verify your zip code and transaction activity.

Online Fraud

Another type of fraud can occur when you sell something online. If the buyer of your product or service wishes to write a larger check than the original selling price, be suspicious. In this type of fraud, after the buyer issues the larger check, he or she will ask the seller to remit the difference back to the purchaser. This is typically in the form of a wire payment. Often, the check originally used to make the 'overpayment' and purchase of the product or service is fraudulent. As a result, the seller is not only out the item sold, but also any money that was returned to the purchaser as an "overpayment." You should be suspicious even if the check is a money order or a government-issued check.

- Stay vigilant! Always keep your private information safe.
- When providing sensitive, private information such as account numbers, PINs, and card numbers, always be cautious.
- Keep your password confidential.
- Change passwords regularly using a combination of numbers, letters and special characters.
- Avoid using obvious passwords like mother's maiden name, children or pet names, Social Security Number or date of birth.
- Regular anti-virus updates and security patches should be installed on your PC and mobile devices. This is especially vital for any devices you use for eBanking or shopping.
- Install anti-spyware on your computer to prevent your personal and account information from being collected without your knowledge.
- We ask our clients not to send Home Loan State Bank any personal details or account information through email. If If you should need to do so, please only use secure messaging in our secure eBanking portal.
- Do not open—and immediately delete—any suspicious emails from unknown sources.
- If you should open any type of suspicious email from an unknown source, do not click on any links or attachments included with the email.

- Stay vigilant for any emails alerting you of fraudulent activity or charges to your account(s). Often, this type of fraudulent email will direct you to respond with your personal information and/or a “click here” option re-directing you to a fictitious site. This is another way cyber-criminals wish to gather and obtain your personal information.
- When conducting any type of online financial transaction, ensure it is trusted by finding the secure padlock icon in the lower right-hand corner. Simply double-click the padlock icon if you wish to view the security certificate.
- If you are conducting financial transactions, always look for the "https" in the URL of your website browser. This ensures your data will be encrypted throughout the communication.
- We also need to remember old-fashioned basic security rules, such as knowing your surroundings, if you are utilizing your laptop or mobile device in a public area. Be aware of ‘shoulder-surfers’ who may be watching you enter your passwords or User ID’s.
- Whether you use e-statements or paper statements, promptly and regularly review them for any suspicious activity or transactions. Report any to your financial services provider.
- It’s important to wipe, or clean, the hard drive of your computer before disposing of it.

Regulation E and Your Online Accounts

Regulation E is a consumer protection regulation which provides a basic framework to establish the rights, liabilities, and responsibilities of consumers in electronic fund transfer systems such as eBanking.

A consumer’s liability for unauthorized eBanking transactions is limited when the transactions are reported to us within specific time frames. Sole proprietorships and other types of businesses are not protected by Regulation E liability limits.

These protections apply to transfers (between Home Loan State Bank accounts), bill payments, personal payments and account-to-account transfers (between an account at Home Loan State Bank and accounts at other financial institutions) that are processed through eBanking.

Reporting Unauthorized Transactions

Tell us at once if you believe your eBanking user credentials been compromised or if someone has transferred or may transfer money from your account without your permission.

The best way to minimize your loss is to call us immediately. The unauthorized use of your eBanking services could cause you to lose all of your money in your accounts, plus any amount available under your overdraft protection plan.

You will have no liability for unauthorized transactions if you notify us within 60 days after the statement showing the transaction has been mailed to you (or 90 days if the transaction was from an account maintained at another financial institution). If you do not, you may not get back any of the money you lost from any unauthorized transaction that occurs after the close of the 60-day period (or 90 day period if the transaction was from an account maintained at another financial institution), if we can show that we could have stopped the transaction if you had notified us in time. If a good reason (such as a long trip or hospital stay) kept you from telling us, we may extend the time periods.

Your Account Statement

Promptly review your account statements. If you determine fraudulent activity has occurred on your account. Provide your name and account number and describe the transaction and amount in question

and explain why you believe it is an error. Contact us with this information immediately by one of the following methods (do not use email to report these incidents):

- Call us at 970-243-6600
- Visit or call your local Home Loan State Bank Branch
- Send us a Message via eBanking
- Write Us at: Home Loan State Bank – Main Branch – 205 N 4th Street – Grand Junction, CO 81501

eBanking

To protect your Home Loan State Bank accounts from unauthorized eBanking transactions follow these important steps.

- Do not share your User ID and Password used to access eBanking with anyone
- Your User ID and Password identify and authenticate you to Home Loan State Bank when you use Home Loan State Bank's eBanking service
- When you give someone your eBanking User ID and Password, any eBanking transaction that person conducts is considered authorized by you even if you did not intend or want the transactions conducted
- In order to revoke the authorization you must notify us you no longer wish to allow the person to use your eBanking credentials. We can attempt to return transactions conducted by the person; however, you are liable for any funds we are not able to return.
- If you tell us about fraudulent activity committed by someone you authorized to access your eBanking account, we will verify any pending payments or transfers to determine which items are not legitimate, so we can prohibit additional items from being processed against your account. We will require your Password to be reset and may require you to choose a new User ID.
- Regularly review your account activity, pending payments and transfers, and payment and transfer history
- Contact us immediately by one of the methods above if you believe fraudulent activity has occurred
- Take advantage of our optional automatic alerts function to notify you of eBanking transaction activity
- Never leave your computer or mobile device unattended while using eBanking
- Never leave your account information displayed where it may be viewed by others
- Avoid using public computers (like those at the Library, Internet cafes) to access eBanking
- Always exit the system by logging out and closing your browser or mobile app

For businesses, Regulation E does not provide liability protections if fraudulent activity occurs on their accounts. This includes transfers (between two Home Loan State Bank accounts), bill payments, personal payments and account-to-account transfers (between an account at Home Loan State Bank and an account at another Financial Institution) that are processed on their accounts through eBanking.

Commercial eBanking customers are encouraged to periodically perform a risk assessment, which includes a threat assessment as it relates to their eBanking activities. Controls to mitigate those risks should be considered and enhanced, if determined necessary, as part of the assessment.

Remember, Home Loan State Bank will never ask you to provide and/or update personal or account information such as, account number, PIN, User ID or password, social security number, by phone call, automated phone message, email or a pop-up message. A bank representative may call you to verify activity on your account (Debit Card transactions, bill payment, personal payment and/or account-to-account transfers) that appears suspicious or to provide you with information about products and services we offer.

When you contact us, we may ask for personal information in order to authenticate you before releasing any account information.

Questions? Contact Us

Your security is important to us. When communicating via email please do not include any personal, business or confidential account information. Thank you!