Valley Bank of Nevada
TRADITION WITH VISION

U.S. consumers lose millions of dollars each year to fraudsters using wire transfers as part of their scams. Hackers target email accounts of realtors, title companies, business brokers, banks and law firms; they may even search social media for new targets.

Below are best practice tips provided by the FBI for security and implementation procedures:

- **Out of Band Communication:** Establish other communication channels, such as telephone calls, to verify wire transactions. When using phone verification, use previously known numbers, not a number provided in an e-mail requesting a wire transfer or changing wire instructions.
- **Two-Factor Verification**: Arrange a second factor authentication early in the relationship and outside of the e-mail environment to avoid interception by a hacker. Examples include code words, passwords or authentication numbers. A phone call to verify modified wire instructions after the scam is in motion may be too late. If your company uses a VoIP internet phone system, a hacker who has penetrated your email system may also be able to access the VoIP system. The hacker may have the ability to intercept and redirect phone calls placed to verified phone numbers from the intended recipient to the hacker.
- **Forward vs. Reply**: Do not use the "Reply" option to respond to any business e-mails. Instead, use the Forward" option and either type in the correct e-mail address or select it from your existing e-mail address book to ensure the intended recipient's correct e-mail address is used.
- **Train Employees to Delete Spam:** Immediately report and delete unsolicited e-mail (spam) from unknown parties. DO NOT open spam email, click on links in the e-mail, or open attachments. These often contain malware that will give hackers access to your computer system.
- **Two Factor Authentication (TFA):** Consider implementing TFA for corporate e-mail accounts. Requiring two pieces of information to login: something you know (a password) and something you have (such as a dynamic PIN or code) reduces the likelihood of access to an employee's e-mail account through a weak or compromised password.

What to Do If You Are a Victim

If funds are transferred to a fraudulent account, it is important to act quickly:

- Immediately contact the corresponding financial institution where the fraudulent transfer was sent.
- Contact your local Federal Bureau of Investigation (FBI) office if the wire is recent. The FBI, working with the United States Department of Treasury Financial Crimes Enforcement Network, might be able to help return or freeze the funds.
- File a complaint at www.IC3.gov