STATE OF CALIFORNIA

Department of Financial Protection and Innovation

GOVERNOR **Gavin Newsom** · COMMISSIONER **KC Mohseni**

ESCROW BULLETIN

DATE: February 11, 2025

Social Engineering Scams Targeting Licensed Escrow Companies

In recent years, social engineering scams have significantly impacted California's real estate, title, and escrow industries, posing substantial challenges to the security of transactions and the protection of sensitive information. California-licensed escrow companies must take appropriate actions to battle social engineering scams that target them.

Criminals are increasingly targeting the escrow industry with various social engineering tactics, such as phishing and business email compromise (BEC) scams. These attacks often involve impersonating legitimate parties involved in real estate transactions, including principals to escrow transactions, real estate agents, title officers, or escrow agents, to deceive victims into wiring funds to fraudulent accounts or disclosing confidential information. As a result, unsuspecting homebuyers, sellers, and industry professionals have fallen victim to thefts and data breaches.

In the past five years, the DFPI has investigated many cases where licensed escrow companies fell prey to social engineering scams. For example, in 2023, a licensed escrow company received a call from a fraudster who claimed to be an IT employee of the bank. The fraudster instructed the escrow company to log into its online trust bank account for data migration. Within 15 minutes of receiving the phone call, the company's internet service was disconnected. Shortly after the internet service was restored, the company found multiple outgoing wires were initiated to divert close to $2 million trust and general account funds to various bank accounts. The escrow company was unable to halt all the outgoing wires or replace the trust shortage caused by the outgoing wires. As a result, the company was taken over by the DFPI under conservatorship.

Another common scam faced by California's real estate, title, and escrow companies is email spoofing, in which a fraudster intercepts communications between an escrow agent and its customers and provides fraudulent instructions to the escrow agent to wire funds to the fraudster's bank account. Many escrow companies have implemented procedures to prevent email spoofing, such as requiring amended wire instructions to be notarized, calling customers at a confirmed phone number to verify amended wire instructions, or educating customers by

placing a warning message regarding wire fraud at the bottom of escrow agents' emails. Social engineering involves tactics that target psychological vulnerabilities and manipulate individuals or groups into divulging confidential information, performing actions, or making decisions that are not in their best interests. It can take various forms, including phishing emails, pretexting phone calls, impersonation, baiting with false promises or threats, and manipulation through social media or online platforms.

What Licensees Can Do to Reduce Their Risks

1. Read Commissioner's 2018 Release No. 66-FS to be familiar with ways to protect computers and systems from intrusion.
2. Immediately report scams or trust shortages to the DFPI.
3. If subject to a cyber-attack, contact the FBI's Internet Crime Complaint Center (IC3), and local law enforcement.
4. Provide comprehensive training to employees about common social engineering techniques.
5. Require employees to verify the identity of the individuals they interact with and to be skeptical of unsolicited requests for sensitive information or actions.
6. Implement strict procedures for verifying the identity of clients, business partners, and vendors before initiating any financial transactions or releasing funds.
7. Use secure communication channels, such as encrypted emails or secure messaging platforms, for transmitting sensitive information or discussing financial transactions.
8. Avoid conducting business-related communications over unsecured channels like public Wi-Fi networks or personal email accounts.
9. Implement multi-factor authentication (MFA) for accessing internal systems, sensitive database, and financial transaction platforms. MFA adds an extra layer of security by requiring users to verify their identity using multiple authentication factors, such as passwords, biometrics, or one-time codes.
10. Conduct regular security audits and assessments to identify potential vulnerabilities in systems, processes, and employee behaviors. Address any weaknesses promptly and implement appropriate security measures to mitigate risks effectively.
11. Develop and regularly update an incident response plan to guide employees on how to respond to suspected social engineering attacks or security breaches effectively. Ensure that employees know whom to contact and what steps to take in the event of a security incident or suspected fraud attempt.
12. Provide ongoing education and awareness programs to keep employees informed about emerging social engineering tactics and cybersecurity best practices. Encourage a culture of security consciousness and empower employees to report any suspicious activities or communications promptly.
13. Also refer to the FBI's April 11, 2024 Public Service Announcement titled Cyber Criminals Target Victims Using Social Engineering Techniques for additional information and guidance.

What Licensees Should Do in Case of a Trust Shortage

In addition to the actions noted above, licensees with trust account shortages as a result of social engineering attacks should consider the follow actions:

1. Immediately contact law enforcement authorities, such as the local police department or the FBI's Internet Crime Complaint Center (IC3), to report the incident and initiate an investigation;
2. Notify their bank or financial institution to halt any transfers, if possible; and
3. Communicate transparently with affected parties, such as customers or business partners.

Additionally, licensees should also report the incident to the DFPI and the Escrow Agents' Fidelity Corporation (EAFC) pursuant to Fin. Code section 17414. Failure to comply with this reporting requirements may subject licensees to administrative action, such as issuance of a discontinuance order and/or license suspension or revocation. (Fin. Code, §§ 17602, 17602.5, 17603, 17608.)

Licensees may also be subject to enforcement action for knowingly or recklessly disbursing escrow funds resulting in a debit balance in a trust account and/or failing to immediately report a trust account shortage to the DFPI. (Fin. Code, § 17414; Cal. Code Regs., tit. 10, §§ 1738, 1738.1, 1738.2.) The DFPI may also take possession of a licensee's property and business if it appears upon examination or investigation that the licensee is operating in an insolvent condition or conducting business in an unsafe or unauthorized manner. (Fin. Code, § 17621.)