Check Fraud

Check fraud refers to any deceptive act involving checks to illegally obtain money. This can include altering legitimate checks, forging signatures, creating counterfeit checks, or using stolen checks to make unauthorized transactions.

Counterfeit Checks

Checks that are fabricated to resemble legitimate checks issued by banks or businesses. In some cases, all the information on the check is fake, but in other situations, the fraudster will create counterfeit checks using real account and routing numbers. They often use advanced printers and graphic design tools to replicate the look and feel of authentic checks.

The most common method criminals use to obtain legitimate checks in order to perpetrate check fraud is mail theft. Tips to avoid mail theft include:

- Deposit mail in collection boxes as close to the indicated pickup time as possible or take it inside the post office for mailing.
- If you choose to leave outgoing mail in your mailbox, don't put the flag up.
- Try not to leave incoming or outgoing mail sitting in your mailbox for an extended time, particularly overnight.
- Sign up for *Informed Delivery*. With this free service, the USPS will email you images of everything that will be delivered to your home that day, so you'll know what to expect (and what's missing when the carrier drops off your mail).

Other Types of Check Fraud

There are several other types of check fraud. Here are some examples:

- Paperhanging: Paperhanging may involve a fraudster writing a bad check and quickly withdrawing funds or making purchases before the

check is returned as insufficient funds. The fraudster's goal is to exploit the delay between check writing and processing, which can allow a fraudster to conduct transactions before the bank detects the fraud.

- Check washing: This is when a scammer steals a check — typically from the mail — and then chemically removes the ink to alter the payee's name, the amount, or other details. They then rewrite the check so they can easily deposit it or cash it themselves.

- Check kiting: This fraud occurs when a scammer uses several bank accounts to write bad checks. For example, they may deposit a check into one bank account, even though there are insufficient funds to cover it. Before the check clears, they transfer funds from another account or write a bad check from another account to cover the first check. This creates a temporary illusion of sufficient funds, exploiting the delay in the check clearing process.

- Forgery with stolen checks: Criminals may steal blank checks from someone's home, office, or mailbox. Once they have these checks, they can alter the details and forge a signature.

- E-check fraud: Fraudsters may utilize digital methods to exploit people and defraud them. E-check fraud may include a variety of methods, such as ACH fraud, account takeovers, or malware attacks, wherein they fraudulently gain access to a person's account and initiate e-check transactions without consent. Mobile deposit fraud — consisting of depositing the same check into multiple accounts — or using remote deposit capture with stolen or counterfeit checks are other common methods.

Important Information

D.L. Evans Bank will not request personal or sensitive information (full social security number, passwords, full debit/credit card number, or PINs) when contacting you. However, D.L. Evans Bank or our authorized Fraud Department may contact you regarding suspicious transactions on your account and request information to verify your identity. If you are suspicious of these automated phone calls, you are welcome to call us to ensure the phone call was indeed valid. We can be reached at 208-678-2552 or 1-866-661-5463, Monday through Friday from 8:00am – 5:00 pm.