SPRING BANK

September 2023

Spring Bank Clients

RE: Increasing Check Fraud - Increased Risk for Customer Loss

The United States Postal Service reports a nationwide surge in check fraud schemes targeting the U. S. Mail. Criminals committing mail theft-related check fraud generally target the U.S. Mail in order to steal personal checks, business checks, tax refund checks, and checks related to government assistance programs, such as Social Security payments and unemployment benefits. Criminals will generally steal all types of checks in the U.S. Mail as part of a mail theft scheme, but business checks may be more valuable because business accounts are often well-funded and it may take longer for the victim to notice the fraud.

These criminals, located throughout the country, target USPS blue collection boxes, unsecured residential mailboxes, and privately-owned cluster box units at apartment complexes, planned neighborhoods, and high-density commercial buildings. Mail theft can occur through forced entry or the use of makeshift fishing devices, and increasingly involves the use of authentic or counterfeit USPS master keys, known as Arrow Keys.

Once criminals have the checks, they can "wash" them by removing the ink or create an entirely new check utilizing information contained on the original check. All it takes to wash a check is chemicals as common as the solvents in nail polish remover. "You can watch the ink literally float up off the check, and it gives you a brand-new piece of paper that you can do whatever you want to with," a convicted identity thief turned security consultant stated. So, for instance, a fraud victim might send out a check for $272 and discover it's been cashed for nearly $5,000.

The criminals also take advantage of "float," the days between when a check is accepted at a bank or business and when funds are withdrawn from the checking account. Typically, by the time the fraudulent check is detected by the account holder, the thieves and funds are often long gone.

Commercial customers have a 24-hour window (1 business day) from the time the check clears their account to notify their bank of the fraud. If the fraudulent check is not returned within the 24-hour window, the claim Spring Bank makes on your behalf to the bank of first deposit may be denied, resulting in a loss to your business.

Spring Bank recommends the following options to monitor your account:

- Utilize Business Online Banking. Log into your account daily and review the activity, including check images, that has posted to your account. Notify Spring Bank immediately of any unusual or unrecognizable activity.

- Positive Pay-Check Positive Pay matches the check number, dollar amount and account number against an electronic file provided by your business that contains a list of issued checks. Checks that don't match this list are presented within Online Banking for review. You choose whether the checks should be paid or returned.

- ACH Manager is an efficient method to issue payment instead of writing checks. ACH (Automated Clearing House) is an electronic payment delivery system that allows you to pay funds electronically through the ACH network — one of the world's safest, most reliable payment networks. With greater speed, accuracy and efficiency, ACH offers more control over the timing of payments posting to your bank accounts.

- Sign up for our "Alerts" utilizing our Notifi alerting services. You choose what alerts to receive and when to receive them. Alerts can be sent to your email or phone.

When it comes to protecting your business against fraudsters, it is a team effort. Spring Bank provides the tools for our clients to use to address fraud. We strongly recommend you consider the options presented. Please contact your Commercial Officer or our Treasury Management team at 262-754-5555 to discuss adding the above services to your relationship.

Regards,

Spring Bank