

Understanding and Preventing Electronic Banking Fraud

Imagine opening your bank statement and discovering unauthorized transfers out of your account. Now imagine that the bank or other financial institution has no responsibility for them. As incredible as it sounds, this is exactly what some entities have experienced.

While electronic banking offers convenience, unfortunately it also provides new opportunities for fraud. Understanding the increased risks and how to mitigate them is essential to protecting your organization's assets.

A would-be criminal doesn't need a blank check to draw from your account. Payments can be made by phone or over the internet as long as the criminal has your account information. While the bank can sometimes retrieve the funds, you should be aware that this isn't always the case.

The key is to prevent unauthorized payments or transfers from occurring. One of the most basic steps you can take is to protect your account information. Keep it confidential. Don't leave bank statements or passwords out where anyone can access them.

Talk to your bank about other safeguards. Various programs are available through banks to help you prevent and detect unauthorized payments.

Positive Pay

Positive pay programs are designed to prevent unauthorized checks from being drawn on your account. With a positive pay program, you regularly provide the bank with lists of authorized checks. Any checks presented for payment that are not on the authorized list are reported to you daily, allowing you to immediately halt processing on a fraudulent check. The positive pay program would catch an unauthorized electronic payment only if a check number was used in the transaction.

Limited approval

Many banks allow you to require approval from a second individual before processing an electronic transaction. Under this arrangement, one user is authorized to set up transactions and a second user is authorized to approve them. Both steps are necessary before a transaction can be completed.

Restricted access and dollar limits

Access to information can be restricted for individuals within your organization so that they see only what they need to. This assists in keeping certain information confidential.

In addition, the dollar amount of electronic transactions can be limited. This won't necessarily prevent unauthorized transactions, but it can mitigate the damage if they occur.

continued on next page

Alerts

Timing is crucial in retrieving funds. When money is transferred to another financial institution, the bank can request return of the funds as long as the money is still there. If the money has been withdrawn from the receiving account, there is nothing available to return. This is why banks generally require you to report unauthorized electronic transactions within 24 hours. Unless you check your account activity online at least once every day, you run the risk of missing a deadline.

You may be able to arrange for the bank to send electronic notification to one or more individuals whenever a wire transfer is made on your account. This won't prevent an unauthorized transfer, but it will allow you to notify the bank in time for your funds to be retrieved.

Pre-Note Service

Some banks require a pre-note for Automated Clearing House (ACH) transactions, which are electronic transactions to and from financial institutions. A "pre-note" is a zero dollar test transaction that occurs approximately six business days before the real electronic transaction is completed. When an electronic transaction with a new account or payee is initiated, the bank completes the transaction as requested, except for the dollar amount. The account/payee name used for the pre-note appears in your online banking information (ACH payee list). During the six business day period, no actual transactions can occur between your account and the account/payee used in the pre-note. This allows you six business days to notice the new account/payee that has been added to your ACH payee list and notify the bank if it is unauthorized. Since no money leaves your account during the six days, you avoid the risk of not being able to retrieve it. While this arrangement still requires you to regularly check your account information online, it expands the amount of time you have to detect and report an unauthorized account/payee and prevent a fraudulent transaction.

Your own bank or financial institution can provide you with more detailed information on these and other available programs. These programs are not provided automatically, and there is often a fee involved for the various services. However, if your organization keeps large amounts of cash in bank accounts that can be accessed electronically, you may decide that the additional safeguards are well worth the cost.

We recommend that you consider your organization's risk of loss from unauthorized electronic transactions and discuss your situation with your bank or other financial institution.

Please contact Partner Louise M. King, CPA with any questions at lking@legacycpas.com or 219-836-1065.