E-check fraud: Mitigating risks to protect your organization

Prepared by:

Vinny Troia, Director, Risk Advisory Services, McGladrey LLP
314.925.3822, vinny.troia@mcgladrey.com

Christina Churchill, Director, Management Consulting, McGladrey LLP
972.764.7049, christina.churchill@mcgladrey.com

August 2015

With an increase in data breaches and personal information falling into criminal hands, organizations are seeing a significant rise in e-check fraud. The crime is similar to stolen or fake paper checks used for goods or services; unfortunately, electronic transactions may have fewer protections in place than in-person purchases. With electronic banking's convenience and growing popularity, you must be aware of the surging fraud risks related to e-checks, and implement controls to protect your finances.

How fraud occurs

Bank account and routing numbers can be accessed in a number of ways: through a data breach, on past invoices or checks themselves. In fact, many companies distribute account numbers so vendors can directly and efficiently submit payments or transfers. That information can then be taken and used for fraudulent purposes.

From a bank's perspective, institutions have various controls in place with paper checks. Banks are required to provide reasonable care, and have policies in place to verify a signature on a check over a certain amount to confirm the transaction is legitimate. However, with an e-check, there is no reasonable way to perform the same level of verification.

Responsibility and verification

The key issue with e-checks is presentment. If someone fraudulently uses a credit card at a vendor, the vendor bears responsibility for the fraud because they should check the signature. With a physical check, the bank has responsibility because it is required to verify the signature if the transaction is over a certain amount. However, with an electronic transaction, your company has the ultimate responsibility, because the options for verification are limited.

Banks are not responsible for money taken from accounts during e-check fraud because there is no way they can know that the transaction is fraudulent. A low-end verification process only verifies that a routing number is valid before processing the transaction. The next level verifies that the routing number, the account number and the name on the account are correct.
The highest level of verification requires actual confirmation of ownership for both accounts; the one that funds are withdrawn from and the one that is receiving the transfer. However, that level of security is typically only found with transactions completed within a financial institution, such as paying a mortgage or auto loan.

The highest level of verification causes significant processing issues for most merchants. In fact, many merchants do not want to implement a high level of protection, as they could flag legitimate purchases. For example, individuals or organizations can process many transactions in a short amount of time, and recurring payments can utilize multiple accounts, such as a parent paying a child’s credit card bill.

A PIN number may seem like a beneficial step for additional verification; however, adding that measure is not currently possible, as instantaneous verification cannot occur between banks. It would require a fundamental change to the entire banking system. Without a higher level of checks and balances to prevent fraudulent transactions, companies must implement protective measures on their end to safeguard accounts and save time spent on recovering lost funds.

Who is at risk?

Large companies often have automatic reconciliation systems that can identify and flag unusual transactions, leading to more effective fraud controls. Small organizations simply process fewer transactions, so irregular transactions and missing funds are easily spotted. Therefore, in many cases, midsize companies have the most difficulty recognizing and addressing e-check fraud.

As companies begin to grow, and bank activity accelerates, going line-by-line to ensure transactions are valid becomes more difficult. They may not have reached the level where it is financially feasible to implement automatic reconciliation processes, but manual practices may have become lax or overwhelming to current personnel.

Putting mitigation techniques to the test: Can we withdraw money from McGladrey’s accounts?

Let’s be honest, it wouldn’t be fair to offer mitigation strategies without proof that they actually work, which is why we put them to the test—against ourselves.

In a controlled test, we attempted to withdraw small amounts of money from several of McGladrey’s accounts. As part of the test, we initiated withdrawals of varying amounts of money from three McGladrey checking accounts, to three of our own external accounts.

In each of the tests, the transactions appeared to go through because the banks had no initial way to verify their authenticity. The balances appeared in the external accounts in a “pending or suspense” status. However, within 24 hours, each of the three transactions had been declined by our external banks, as we utilize Positive Pay and ACH blocking.

Mitigating e-check fraud—how did we do it?

Your organization can take advantage of several strategies to protect finances and discourage e-check fraud. You should start by talking to your financial institution to discuss appropriate controls and protective measures. Strengthening reconciliation practices is your major line of defense against e-check fraud; if you are not performing reconciliations in a timely and thorough manner, instances of fraud can go undetected.
You may need to strengthen reconciliation practices or leverage external resources to improve processes and observe transaction activity. Your organization also may want to consider making adjustments to reconciliation parameters to target large and small suspicious transactions. Many companies have suffered significant financial losses from a series of small fraudulent transactions that went undetected because they fell below the reconciliation threshold.

You can also limit your susceptibility to e-check fraud by only allowing deposits into certain accounts, and locking them so funds can only go in; even if account and routing numbers are compromised, a criminal cannot withdraw funds. For example, many organizations create separate accounts for payroll, accounts payable and operations to add additional controls, and ensure that their primary cash accounts don’t allow e-transactions. Additionally, Positive Pay or like solutions limit allowed transactions by your financial institution.

Using the example of payroll again, transferring only the amount of the payroll into that account in advance of payday, limits your liability if someone tried to use the routing and account number from a payroll check in e-fraud. The risk levels are limited if only the outgoing funds, or a manageable balance, are deposited in the account.

The number of paper checks being issued is dramatically decreasing because of the efficiency of electronic banking and ACH transfers. However, with increased convenience comes increased risk to your organization. Banking information is under attack, and as more systems are upgraded, e-check fraud will become even more prevalent. Implementing additional security controls, and strengthening reconciliations will help identify criminal activity and protect funds.

**What to do if you are the victim of e-check fraud**

If you notice suspicious activity in your bank accounts or believe that your organization has suffered e-check fraud, you must file a police report to begin the process of recovering funds. In addition, submit a claim to your insurance company, depending on the level of suspected damages. Some companies have also purchased cybersecurity insurance policies in the midst of several high-profile security breaches; those can be leveraged following e-check fraud.