LAWYERS JOURNAL

LAW PRACTICE MANAGEMENT

Eleven ways to protect your business from payment fraud

Adopt smart strategies designed to stop cybercriminals in their tracks

By Dollar Bank

Judy Murtha

Cyberthieves target businesses of all types and sizes with payment fraud – illegal transactions using stolen information to make purchases or direct funds to unauthorized accounts. Bad actors are quick to zero in on vulnerabilities, so companies are tasked with making their financial operations as airtight as possible.

"Businesses are required to protect themselves. They are not covered by the Consumer Protection Act," says Judy Murtha, Executive Vice President, Treasury Management, Dollar Bank, who has a front row seat to schemes and scams carried out against businesses by cybercriminals. "If your business falls victim to a fraudulent transaction, it will bear the brunt of that loss. It's up to you to put safeguards into place."

Murtha shares her insights into eleven of these safeguards. Some are fairly easy to implement; others require dedicated resources and collaboration across your teams.

With Your Bank

1. Use positive pay. This automated cash management service is offered by banks to reduce companies' exposure to check and ACH fraud. Here's how it works: When your company issues checks, you upload a file listing those checks – including each check number, payee, and dollar amount – to the bank. The bank stores that information for verification as checks come in for payment. If any information does not align, the bank issues an exception for you to approve or deny the transaction.

2. Request dollar-limit reviews. Set a dollar limit with your bank that lets them know when you should be called to verify ACH transactions to be paid from your account. Any transaction request exceeding that limit should trigger a call to you before funds are released.

3. Sign up for text message alerts. Just as they work for personal accounts, text message alerts can let you know when transactions occur in your corporate account. Some companies set up these alerts to be received by multiple individuals to ensure the appropriate level of oversight.

4. Move toward electronic payments. Companies continue to write a great number of checks, yet account information is more vulnerable to theft when it is physically circulating than when secure electronic payments are made.

Within Your Business

5. Limit physical access to data. Protecting the data in your office, as well as employee workstations, is particularly important when members of your team are working remotely and come into the office infrequently. Accumulating mail and other exposed information may be at risk. Know who is going into your business space and make sure customer data and other information is not accessible.

6. Use dedicated PCs for online banking. Many companies assign a designated computer for banking transactions. This computer is reserved exclusively for banking transactions; users are prohibited from doing any internet research, thus limiting the amount of malware that can be installed on that PC.

7. Create separation of duties. In a secure environment, no individual has sole responsibility over a particular function from end to end. Specifically, a business should assign custody of assets, authorization of payments and documentation of those payments to different employees.

8. Tighten up administrative rights. Who has administrative rights to your computers? Keep in mind that these people can download and install programs, change the way systems operate, add accounts, and carry out a host of other activities that may be harmful to your business. It's important to limit how many and which people have this access; administrative rights must be carefully monitored.

9. Implement online banking controls. Similarly, it's important to know and control who in your firm has access to online banking. When someone has access to your online banking systems, they can figure out how to send a transaction to your bank that, from the bank's perspective, looks legitimate.

If you're sending money via ACH or wire, it's smart to use two-factor authentication, where the user must provide not only a username and password but also carry a security token or reference a randomly generated number delivered to a separate device to authorize access. This helps ensure that unauthorized parties cannot get between you and your bank to originate a transaction.

The dual control method, where one person initiates a transaction and a second person approves it, offers important protections, too, not only from internal fraud but from external fraud that has compromised one employee's credentials. Like separation of duties, dual controls help ensure the integrity of transactions.

10. Strengthen company password rules. While you might think everyone knows by now not to use their child's birthday or their pet's name as a password for logging in to your network, that's not always the case. Murtha reports that the most popular password is actually "password"; that makes it incredibly easy for a cyberthief to gain access to a network. Password controls are easy to put into place and essential to network security.

11. Focus on employee education. Quarterly security awareness training is a critical component of a secure business environment. Employees are the first line of defense in the fight against cybercrime, so they need to be fully prepared to recognize and report suspected phishing schemes, and other types of social engineering cyberattacks; to understand IT best practices and model their behaviors to these standards; and to be aware of, and comply with, data privacy regulations. Employee education should include not only training but also testing. Send test phishing emails to employees, for example, and measure their success in responding. If they fail the test, get them back into training to ensure your team can be duly diligent.

Murtha recommends that business leaders stay up-to-date on new protective protocols and tools as payment fraud scams and tactics continue to evolve. "Crooks are never going to stop," she says. "We need to be one step ahead at all times." ■

Judy Murtha is the Managing Director of Dollar Bank's Treasury Management Group. She is responsible for providing the strategic direction and execution of all cash management services for corporate and small business clients in Dollar Bank's primary markets of Pennsylvania, Ohio and Virginia. She has over 30 years of financial services experience with a focus on educating businesses on security concerns and ways to protect business accounts.