Fraud Protection and ACH Payments

The Automated Clearing House (ACH) network has made transferring funds between banks, financial institutions, and their customers quick and easy. While there are many benefits to these largely automated and safe ACH payments, there remains the very real possibility that companies can fall victim to ACH fraud.

While fraudsters have a variety of tools in their arsenal, a criminal can commit ACH fraud by claiming access to just two pieces of information: your business checking account number and your bank routing number. Armed with that information, con artists can use those digits to fraudulently pay for goods or services, either by phone or online. The most common ACH fraud attempts are misrepresenting a business and the unauthorized use of business bank accounts.

This new development indicates that fraudsters are now targeting ACH transactions for their scams as they move away from cheque and wire fraud, a report by AFP states, adding that as ACH transactions are typically considered safer and more difficult to breach, the uptick in ACH fraud suggests that thieves are becoming more sophisticated.

Fraud is no doubt a major threat to any business, and by the time you realize the crime, the criminals have long disappeared – leaving you to sweep up the financial mess.

The question then: What can financial professionals do to guard against the risks of ACH fraud? In this post, we'll break down ACH fraud and what you need to be looking out for.

The Risks of ACH Fraud

A 2019 report by AFP revealed a noticeable increase in fraud activity via both ACH credits and ACH debits. Financial professionals (33%) reported their organizations' payments via ACH debits were compromised in 2018; increasing to 33% from 28% in 2017. Fraudulent activity via ACH credits also climbed 7% from 13% in 2017 to 20% in 2018.

According to the AFP analysis, 81% of organizations surveyed were targets of payment fraud in 2018, including ACH, check, as well as debit and credit card transactions. This number represented the second-highest percentage since 2009. Large organizations were particularly prone to payment fraud, registering a jump from 2018 of 7 percentage points year-on-year to 87%.

It is possible, the report adds, that in order to conduct scams via ACH transactions, fraudsters may either compromise internal systems through phishing attacks or recruit assistance from inside their target organizations to help initiate fraudulent ACH transactions.

How Does ACH Fraud Happen?

An important first step in stamping out ACH fraud is to know how it happens. As AFP President and CEO Jim Kaitz notes: “Treasury and finance professionals need to learn the latest scams and educate themselves—and perhaps more importantly—their work colleagues on how to prevent them.”

Here are three of the most common scams that you must be aware of and looking out for.

Payroll Exploits

One of the oldest ACH scams around is to fool HR administrators into transmitting payroll funds to the bank accounts of fraudsters. In this scenario, the thief steals the login credentials of a company executive. Claiming to be the employee, they then send an email to HR asking to change the direct deposit bank account details. If HR falls for the ploy, the paycheck gets deposited into the account of the scammer rather than that of the legitimate employee.

Phishing Emails

In this type of scam, a phishing email is sent to an individual, typically in the accounting office, who is authorized to perform ACH transactions. By opening the email, the individual is redirected to a website infected with malware. The malicious site then installs a trojan, a type of virus designed to steal sensitive data such as banking credentials.

Once the trojan obtains this data, ACH transfers are initiated, frequently to multiple human “mules.” Recruited via work-at-home ads, the mules receive the ACH payments and then transmit them to fraudsters, keeping a portion of the funds for themselves. In one well-known scheme of this kind, the phishing emails were purported to have been sent by the IRS and carried the subject line: "Notice of Underreported Income."

ACH Check Kiting

Another type of exploit is inspired by the check-kiting scams which used to take place when paper checks were a major way of moving money. ACH check-kiting attacks are designed to exploit the traditional lag time for ACH processing. The fraudster juggles funds to and from accounts at different banks. In this scheme, the ACH ‘checks and verifies’ the said funds but it disappears by the time the transfer completes.

In September 2016, ACH introduced one-day processing. NACHA, the ACH’s governing body, also recently added two hours to one-day processing times with the introduction of the so-called “third window.” However, less lag time also means that companies have less time to investigate suspected ACH fraud before transactions are cleared.

Tips For ACH Fraud Prevention

The good news is that you can enjoy the benefits of ACH transactions while guarding your company against fraud. Putting a system of checks and balances in place makes sense for any financial function. Another effective countermeasure to prevent employee fraud is to limit the number of individuals who are in a position to commit fraud. Using iron-clad passwords, changing them often, and limiting the use of your ACH system to those individuals who need to use the system will also help to strengthen your systems.

Here are some additional security measures to help keep your institution safe.

- **ACH blocks.** The simplest and probably the best way to prevent ACH fraud is to place a block on all your accounts. This measure will not automatically reject transactions; but, in each case, you will be required to review and approve the transaction before it can be processed.

- **Encrypt your network.** Whether your network is on-premise, cloud-enabled, or a hybrid configuration, make sure that all personal information is encrypted using HTTPS. Additionally, you should ensure that the computers that store or access financial information are free from viruses and malware.

- **Role-based access to ACH payments.** In an SMB**,** C-level execs might be the ones to manage ACH transactions. In a larger enterprise setting, we're probably talking about accounting and finance. There's really no reason why people in your sales, marketing, or manufacturing divisions should also have access to your ACH processes, except as payroll recipients.

- **Multi-factor authentication (MFA) for client logins.** Make doubly sure that employees, customers, and vendors are who they say they are. Along with a password, institute mandatory authentication requirements through fingerprint ID.

- **State-of-the-art intrusion prevention technology.** Implementing these tech tools will help protect against ransomware, phishing attacks, and other malware exploits.

- **ACH filters.** These filters will block a fraudulent transaction, automatically returning all ACH transactions for a designated account, with the exception of those that are pre-authorized.

- **ACH alerts for each customer.** These will enable the customer to monitor and stop any unauthorized ACH debit.

- **Comply with regulatory requirements.** These include Know Your Customer (KYC) regulations for the banking industry and HIPAA for health care information privacy, for example. Abiding by the NACHA Operating Rules will also help to reinforce your defense against attacks.

NatPay = Solutions. Service. Stability. Security.

Fraudsters are getting creative in impersonating clients and creating fictitious financial documents to siphon funds from your company. If you looking for the security measures you need for ACH fraud prevention, you have three choices: You can hire an institution to run your ACH processing service. Alternatively, you can take a DIY approach, purchasing software and services such as ACH block and intrusion prevention software. Your third choice, teaming up with NatPay, will prove to be the most rigorous, affordable, and effective.

With over 30 years of experience, NatPay offers you services that include processing all types of ACH payments ranging from Direct Deposits to tax payments to expense reimbursements, processing more than $115 billion annually for 228,000+ ACH clients nationwide. NatPay's services support an unlimited number of users, providing them with role-based system access for protecting confidential data. Our network adheres to industry-standard solutions for security such as 24/7 system monitoring and 128-bit encryption.

Contact us today to schedule a FREE online demonstration that is customized for your organization.