TREASURY MANAGEMENT SERVICES
ACH FRAUD PREVENTION TIPS

WHAT IS ACH PAYMENT FRAUD?

ACH payments were introduced in the early 1970s to facilitate money movement between bank accounts at different financial institutions. In the U.S., the National Automated Clearing House Association (NACHA) oversees the ACH network.

ACH fraud is the unauthorized or fraudulent transfer of funds through the ACH network. Criminals engaging in this type of fraud need only two pieces of information: a bank account number and a bank routing number. With these details, they can illicitly transfer funds from a victim's account.

Minimal credential requirements are not the only reason the ACH system attracts fraud. ACH payments are consolidated and processed in batches at specified times. Batch processing is efficient and cost-effective, but it introduces a time delay in transaction settlement, typically one to two business days.

During this period, the funds are in transit and not immediately debited or credited to the respective accounts, creating a window where unauthorized transfers may go undetected.

HOW DO ACH FRAUD SCAMS WORK?

ACH scams focus on obtaining the two pieces of information needed to carry out an ACH payment: bank account and bank routing numbers. Criminals use a range of technological and psychological tactics to obtain these details.

- **Phishing**: One of the most common methods, phishing involves sending fake emails or texts that appear to be from legitimate organizations. These messages trick victims into revealing sensitive account details by mimicking the look and feel of communications from trusted sources.
- **Malware**: Botnets install malicious software on victims' devices without their knowledge. The malware then steals account numbers and login credentials stored on the infected system
- **Data Breaches**: When retailers or other businesses with large customer databases experience a data breach, account numbers can be compromised and sold on the dark web
- **Skimming**: Skimmers are physical devices illicitly installed on ATMs, gas pumps, and other card readers. They copy card data, which can then be used to generate or access account numbers
- **Social Engineering**: This method involves manipulating authorized users, like employees, into making unauthorized transfers, often by exploiting their trust and lack of awareness
- **Insiders**: Sometimes, the threat comes from within. Dishonest insiders at banks or businesses may abuse their access to confidential information to steal account data.

ACH scams are often orchestrated by criminal networks, with teams responsible for stealing account details and executing fraudulent transactions. They may also use mules, individuals whose bank accounts receive fraudulent payments before the money is sent to accounts under the criminals' direct control.

WHO ARE VICTIMS OF ACH FRAUD?

Any business or consumer with a checking, savings, credit union, or peer-to-peer payment account may be at risk. ACH fraud impacts many victims, each with unique vulnerabilities and consequences.

The list of victims most at risk includes:

- **Individuals**: Particularly at risk are elderly individuals who may be more prone to falling for social engineering tactics. These tactics often involve manipulating the victim into divulging account information, either through confidence tricks or deceptive requests that seem legitimate.
- **Small Businesses**: Small companies frequently lack the advanced cybersecurity measures that larger corporations might have. This makes them more susceptible to phishing attacks and malware. Small business accounts often carry sufficient funds to be attractive targets for fraudsters.
- **Non-Profits and Charities**: The charitable nature of these organizations can make them targets for fraud. They may be tricked into making unauthorized transfers under the guise of genuine requests for donations or funding.
- **Government Entities**: Public sector bodies are not immune to ACH fraud. Those involved in collecting payments or distributing benefits, such as tax authorities or social welfare agencies, can be targeted for their substantial financial transactions.
- **ACH Transfer Originators**: This group includes banks, lenders, and merchants regularly initiating ACH transfers. They risk having their credentials compromised, often through malware.

TREASURY MANAGEMENT SERVICES
ACH FRAUD PREVENTION TIPS

BEST PRACTICES AGAINST ACH FRAUD

Along with best practices from National Automated Clearing House Association (NACHA), below are some tips to help protect your company from falling victim to ACH fraud.

- **Verify by phone before sending funds**: ALWAYS call the vendor, business partner, or colleague directly to verify the payment information. Use previously known numbers you know are correct and not the numbers provided in an email or text request. Never initiate any changes based only on email or text communication.
- **Be cautious of new payment information.** Beware of email requests instructing a routine wire payment to be sent to a new account.
- **Match your payment to a legitimate invoice before paying.** Quite frequently, fraudsters tend to pose as trusted vendors requesting payment. Prior to sending payments, ensure the payment requested matches a legitimate invoice.
- **Verify before clicking on a link or opening an attachment in an email or text.** It may appear to be from someone you know, but it may be a fraudster phishing your password, business bank account, or other sensitive information. Extra caution: The link may contain malware.
- **Double-check the email address.** Fraudsters are tricky and can create email addresses that look very similar to the legitimate account. They often find naming conventions for a company's email accounts on its website and use those to fool you — inspect closely!
- **Do not respond to email as verification.** Don't reply to the requester by email. The fraudster either controls the spoof email account or has gotten access to the valid email account and can write back, making it appear legitimate when it is not.
- **Beware of a sense of urgency.** Usually, fraudsters will indicate that the funds need to be wired right away. These requests often ask that the client be contacted only through email instead of other channels.
- **Know and trust who you are working with.** Before doing business with a new company, search the company's name online with the term "scam" or "complaint." Read what others are saying about the company. Only purchase merchandise from reputable dealers or establishments.
- **Be wary of using free, web-based email accounts for your business**, which are more susceptible to being hacked. Make sure at least two-factor authentication is available.
- **Be careful when posting information to social media** and company websites, as fraudsters may use this information to deploy new tactics.
- **Keep the processing of your financial activities limited** to as few machines as possible and limit activities such as web surfing on those machines.
- **Consider financial security procedures** that include a two-factor authentication process or dual control for electronic funds transfers.
- **Create intrusion detection system rules** that flag emails with extensions that are similar to company email but not exactly the same (for example, .co instead of .com). If possible, register all Internet domains that are slightly different from the actual company domain.
- **Know the habits of your customers,** including the reason, detail, and amount of payments. Beware of any significant changes.
- **Consider frequent and regular patching** of your business systems.
- **Use a quality next-gen antivirus solution** — one that watches for behavior anomalies and not just signatures.

SCAMS TO BE AWARE

- **Business email compromise (BEC) and phishing scams**. BEC scams target companies that may make wire transfers to suppliers and businesses. BEC scams begin with a criminal sending a phishing email to a company which seems to be from someone they know. The employee clicks a link, or provides their password, business bank account, or other sensitive information, and the fraudster gains access to the employee's email account. The fraudster will monitor that employee's email for a period of time and determine who initiates wires and who requests them.
- **Senior executive spoofing scams**. In this type of scam, a company employee will receive a transfer request via email from what appears to be a high-level executive. The domain will look very close to the company's domain (see our fourth point above) and appears to be an email from the CEO or similar company manager. However, the request is coming from a hacked email account, or an account that has been "spoofed" to appear legitimate. The fraudster creates a sense of urgency and rushes the employee into making a quick decision to send the transfer before researching and verbally confirming the request.
- **Overpayment scams.** Another example of a fraudster posing as a trusted vendor, fraudsters can send a check for more than the agreed upon amount of an actual vendor and then insist that the overpayment be wired back to them. Later, the check gets returned, leaving you liable for the entire amount.
- **Vendor spoofing scams**. An employee receives an email or phone call from a trusted vendor requesting a change in payment instructions. Without due diligence and validation processes to confirm the request, the employee transfers the funds to the fraudster's bank account. Usually, these wire requests closely mimic a legitimate request that you'd typically receive from that supplier.