D.L. Evans | BANK

ACH Fraud

ACH fraud is a type of financial fraud that involves the Automated Clearing House (ACH) network, which is used to transfer money from one bank account to another. A fraudster needs two pieces of information to carry out ACH fraud – a bank account number and a bank routing number. With this information, they can transfer money from the victim's account, either as a lump sum or as recurring payments. They can also make unauthorized payments for goods or services. To complicate things, businesses only have 2 days to report a fraudulent ACH transaction and recover the stolen money.

Criminals often gain access to customer credentials via a data breach. In this scenario, fraudsters log into bank accounts with bought or stolen information from the dark web before withdrawing funds through the ACH network. When a customer clicks a link in a phishing email, which sends them to a malicious website that infects their computer with malware, fraudsters can track the customer's keystrokes and discover their banking credentials.

What is ACH or Invoice Payment Fraud?

A fraudster impersonates a vendor; often through business email compromise or an account takeover and contacts an organization's accounts payable department to update payment information to a fraudulent account. In doing so, the accounts payable department thinks that they are paying their vendor when in fact, they are paying the fraudster. Once the accounts payable department realizes they've initiated payment to a fraudster, the funds are long gone.

How to Mitigate ACH Fraud

To protect against ACH fraud, organizations should utilize a combination of prevention and detection strategies. Some methods include creating strong passwords for electronic banking accounts, verifying all transactions by multiple individuals, and creating a system for flagging suspicious activity.

Here are 7 methods to combat ACH fraud:

Strong internal controls

Internal controls reduce the risk of fraud by ensuring that only authorized personnel have access to financial information. Additionally, organizations

should implement limits on who within the organization can approve or initiate ACH and wire transfers. Dollar limits can be set on how much can be withdrawn from the organization's accounts through ACH payments.

Segregation of Duties

Segregation of duties means that one person is responsible for queueing up business payments, and one person is responsible for approving those payments before funds are released.

While invoice payments can be time sensitive, and sometimes it is both quicker and simpler for an accounts payable employee to carry an invoice payment from start to finish on their own, this leaves the door open for fraud.

Positive Pay

Use Positive Pay which verifies new check or ACH requests against records and parameters submitted by your organization. If an unreported check or an ACH payment from an unauthorized vendor tries to clear your account, the bank will alert you and confirm if you approve of the transaction.

Utilize Dual-Factor Authentication

Dual-Factor Authentication adds another layer of security by requiring employees who approve payments to enter a unique security code that they receive via text or email every time they release funds. This extra layer of security mitigates the risk of fraud by discouraging fraudsters that are constantly on the lookout for businesses that lack vigilance around cybersecurity.

Close monitoring

Reconcile accounts daily, reviewing payments for any inconsistencies or out of the ordinary activity. Scammers will often continue making fraudulent transactions until their attempts are blocked, so detecting fraud immediately typically helps prevent future fraudulent transactions.

Vendor verification

Organizations should ensure that all vendor information is accurate and up to date. This includes verifying the bank account numbers associated with each

payment request, to ensure that payments are always sent to the correct recipient. Confirm changes to vendor accounts directly with the vendor in writing or by phone from a number you have on file and not through email or text.

Employee training

It is important for organizations to educate their employees on the potential risks associated with ACH payments. They should also share tips to identify suspicious activity or transactions.

Important Information

D.L. Evans Bank will not request personal or sensitive information (full social security number, passwords, full debit/credit card number, or PINs) when contacting you. However, D.L. Evans Bank or our authorized Fraud Department may contact you regarding suspicious transactions on your account and request information to verify your identity. If you are suspicious of these automated phone calls, you are welcome to call us to ensure the phone call was indeed valid. We can be reached at 208-678-2552 or 1-866-661-5463, Monday through Friday from 8:00am – 5:00 pm.