Country Club Bank Member FDIC
epcor Electronic Payments Core of Knowledge
PAYMENTS INSIDER
The inside scoop on payments for businesses of all sizes

Fighting Email Compromise and Impersonation Scams

by Trevor Witchey, AAP, NCP, Senior Director, Payments Education, EPCOR

Fraud attempts with ACH, wire and presumably FedNow®/RTP® payments often occur when a member of an organization falls for a scam impersonating an employee, HR official or vendor. Whether it be through a fraudulent email or some other means of digital communication, businesses like yours are losing funds every single day.

Fraudsters are constantly searching for their next victim, and while steps can be put in place to mitigate certain attacks such as adding tough layers of security to online platforms to prevent account takeover or keystroke logging malware, fraudsters have moved on to coercing the users of those online platforms to willingly give up their credentials or send fraudulent payments on their behalf.

Nacha is currently in the process of implementing new *ACH Rules* to help reduce credit-push type fraud seen on their network. And, while online attacks from fraudsters are not new, most financial institutions have implemented new systems, more detailed procedures and more interrogative callback processes while having the most commercially reasonable security protections on their online platforms. Although these security measures are certainly helpful, it's still very common for those who use email as their primary form of communication to fall for impersonation scams asking for login credentials or requesting the individual to send a fraudulent payment.

It's Time to Try a Different Approach

Regardless of the kind of payments your organization sends, there is always a chance you could fall victim to fraud.

Most ACH Originators send payroll credits or utility debits to the same individuals repeatedly, while most businesses send the same ACH or wire payments to the same vendors or suppliers. To make things efficient and reduce errors, many reuse templates on online platforms or have a fixed list that helps generate an ACH file reusing the same account information. Sound familiar? If so, this could become an issue if the account information suddenly changes.

If the payment you're sending is to a new account, a more elaborate set of procedures should be performed by your organization before forwarding that payment to your financial institution. The checklist below can assist your organization in confirming the legitimacy of the payment information before any funds are transmitted.

Yes/No	Questions to Ask Before Sending
	Has due diligence been performed on the Receiver/Beneficiary?
	Did you verify the identity of the Receiver/Beneficiary?
	Do you know the beneficial owner(s) or any relevant company official to verify the legitimacy of the Receiver/Beneficiary?
	Did you perform secondary communication with Receiver/Beneficiary to verify instructions?
	Did you verify with another employee of the commercial Receiver/Beneficiary?
	Was an invoice received legitimately and then verified with secondary communication?
	If recurring Receiver/Beneficiary, were they contacted as to why account information has changed?
	For recurring Receiver/Beneficiary, did you verify with known contact about changed info?
	Any contact with the Receiving or Beneficiary financial institution about newer account info?
	Is this payment within the normal scope of operations?
	Are you convinced this is a legitimate payment and won't take a loss for it?
	Is upper management aware of this account change?

If the majority of checkmarks are missing from a list like the above, then really question the risk of sending a payment to the new account. It's better to ask questions first than act hastily and regret the decision later.

The key to mitigating fraud is to think and perform more procedures regarding payment requests to brand new account information or new clientele. The more thorough you are, and the more serious you take verifying the legitimacy of account information, the better off your organization will be.

Electronic Payments Core of Knowledge

EPCOR is a not-for-profit payments association which provides payments expertise through education, advice and member representation. EPCOR assists banks, credit unions, thrifts and affiliated organizations in maintaining compliance, reducing risk and enhancing the overall operational efficiency of the payment systems. Through our affiliation with industry partners and other associations, EPCOR fosters and promotes improvement of the payments systems which are in the best interest of our members.
For more information on EPCOR, visit www.epcor.org.

Nacha® Direct Member

The Nacha Direct Member mark signifies that through their individual direct memberships in Nacha, Payments Associations are specially recognized and licensed providers of ACH education, publications and advocacy.

www.epcor.org
2345 Grand Blvd., Ste. 1700, Kansas City, MO 64108
800.500.0100 | 816.474.5630 | fax: 816.471.7665