epcor
Electronic Payments Core of Knowledge

PAYMENTS INSIDER

The inside scoop on payments for businesses of all sizes

'Tis the Season to Stay Fraud-Free

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

It's no surprise fraudsters made Santa's naughty list. The year-end rush means higher transaction volumes, more vendor payments and plenty of opportunities for criminals to slip scams through unnoticed. Your business could be at greater risk this season as employees make more purchases, approve last-minute invoices or send digital payments to partners and customers.

Help protect your organization from unwanted surprises—or lumps of coal—from landing on your year-end statements with these simple fraud prevention tips:

Check business accounts daily.

Monitoring transactions frequently helps spot fraud early, prevent further unauthorized activity and ensure issues are reported within required timeframes.

Set up account alerts and card controls.

Real-time notifications can flag unusual activity right away. Remind employees to review and update their alert preferences periodically to stay protected. Encourage cardholders to utilize expansive card controls (if offered) or protections in the form of limits, restrictions on merchants or types of transactions and locations.

Avoid mailing checks to vendors or partners.

Mail theft and check fraud increase significantly during the holidays, and stolen checks can be easily altered or counterfeited. Whenever possible, use secure electronic payment options, such as ACH, instead.

Keep company cards and devices secure while shopping or traveling.

This is a prime time for theft and skimming. Employees should safeguard corporate cards, avoid leaving personal belongings unattended and use trusted payment devices or networks.

Inspect card terminals before using them.

Fraudsters sometimes install skimming devices that steal card data and PINs. Before inserting or swiping a card, check for loose or suspicious parts. Tap-to-pay methods using tokenization offer safer alternatives.

Be cautious with online purchases or invoice payments.

Stick to verified websites and legitimate vendors. Fraudsters often mimic real businesses with fake domains or invoices, so always double-check payee information before approving a transaction.

Protect sensitive business information.

Never share payment or account details over unsolicited emails or calls. Remind staff that legitimate vendors or partners won't ask for confidential information they already have.

Verify recipients before sending digital payments.

Always confirm payment requests through a known and trusted contact or a verified phone number. Fraudsters are increasingly using fake payment accounts or AI-generated messages to create a sense of urgency and trick employees into sending funds.

Watch for business email compromise and phishing scams.

Cybercriminals frequently impersonate executives, vendors or IT support during the busy season. When in doubt, stop, think and verify (just like EPCOR's *Did You Know* video says) before sending payments or clicking links. For ACH, accepting account information by email is contrary to secure/encrypted transmission standards in *Section 1.7* and applicable legal requirements for credit authorizations in *Subsection 2.3.2.1* of the *ACH Rules*.

Watch for atypical origination requests versus recurring previous history.

Most ACH and wire transfer originations are sent repeatedly to the same Receivers, whether employees, vendors, utilities or lenders. Both originators and financial institutions should perform extra due diligence on payments sent to a brand-new Receiver or to an existing Receiver who suddenly updates their account information.

Utilize dual control for originated digital payments.

It's easier for a fraudster to compromise a single person than two. With dual control, one team member enters or uploads the payment while a second reviews it. The reviewer should carefully verify any new routing numbers or account combinations and question the source whenever something seems unusual.

If it sounds too good to be true, it probably is—especially with investment or crypto.

According to the FBI's 2024 IC3 Report, known investment scams resulted in over $6.5 billion in losses, while cryptocurrency-related scams caused more than $9.2 billion in losses. Fraudsters are becoming increasingly sophisticated, often impersonating trusted sources to target victims. Many schemes aim to drain long-term savings, Home Equity Lines of Credit (HELOCs), personal investments and 401(k) accounts.

While the holiday season can be hectic, your organization must remain vigilant with how payment information is used and shared. Encourage your team to stop, think and verify before approving payments or disclosing sensitive data. A few extra moments of caution can prevent significant losses and keep fraudsters exactly where they belong: on the naughty list.

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
800.500.0100 | 816.474.5630