‘Tis the Season (for Fraud): How Businesses Can Be On-Guard

ARTICLE 12.05.25 JEFF KOLBFLEISCH, MSFFE, CFE, CCI

Fourth quarter brings year-end closing, bonus calculations, and other annual tasks that create the kind of “let’s just get it done” energy that fraudsters love — and actively exploit. For many small businesses across the U.S., this is when oversight thins and dual approvals turn into a quick “can you just sign it?” Fatigue becomes the silent co-conspirator. The items that would normally trigger a second review in July now slide right through.

The result? Companies become prime targets for bad actors who understand timing even better than accountants do. While we hear daily about consumer-facing scams — porch pirates, counterfeit goods, fake charities — the quieter casualties are the small businesses hit with bogus invoices, hijacked vendor payments, or phantom orders that disappear faster than an Amazon truck on Christmas Eve. These losses rarely make the news, but they cut where it hurts most: working capital, client trust, and the balance sheet.

The Holiday Frauds That Hit Businesses Hardest

Every December, fraudsters adjust their playbooks to match the rhythm of legitimate business operations. During a time when companies are buried under reconciliations and client deadlines, even disciplined teams may overlook subtle cues of deception. These schemes are effective not because they’re complex, but because they’re familiar — mimicking the everyday transactions and workflows that keep business moving.

Here are some of the most common and costly forms of year-end fraud impacting small and mid-sized businesses:

1. Invoice & Vendor Impersonation

Attackers pose as legitimate suppliers and send realistic-looking invoices or payment requests with altered banking details or email addresses. This scam thrives on internal haste, especially when accounting teams are closing the books. Once funds are wired to the fraudulent account, they’re quickly transferred elsewhere — often beyond recovery.

2. Business Email Compromise (BEC)

A long-time favorite of fraudsters, BEC attacks spoof a CEO, CFO, or managing partner with messages like “Are you at your desk?” followed by urgent payment instructions. These attacks increasingly mimic internal phrasing or imitate

real email chains. With executives out of office and approvals delegated, these fakes slip through more easily in December.

3. Seasonal Employment & Payroll Scams

Temporary staffing needs can overload HR departments. Fraudsters exploit this with fake job applications using stolen identities, overpayment scams involving fraudulent checks, or phishing portals designed to steal onboarding credentials. The result: payroll fraud, W-2 data theft, and redirected direct deposits — a data breach waiting to happen.

Why it Spikes Now

Fraud thrives on a simple formula: **volume + velocity + distraction**. December offers all three. Even with sound controls, human attention is finite — and exhaustion is a powerful vulnerability.

Add in seasonal staff, remote approvals, impatient customers, and tight shipping timelines, and you've created the perfect environment for social engineering. As one FBI analyst noted, "Cybercriminals appreciate overtime too."

Fortify Before Festivities

The holiday season requires cheer — and increased discipline. Fraud prevention doesn't come from paranoia but from preparation. Businesses should treat December as an annual audit of their anti-fraud posture, tightening processes that may weaken under year-end pressure.

Below are practical measures that significantly reduce exposure without slowing operations:

1. Slow Down the "Urgent."

Any request to change payment details or approve a wire outside normal processes should trigger verification by phone or secure messaging. Fraudsters weaponize urgency because it disrupts logic. A brief pause can prevent a major loss.

2. Dual-Control Everything.

Require two-person approval for high-value transactions, new vendor setups, or wire transfers. Dual authorization isn't bureaucracy — it's risk mitigation and a deterrent to both external and internal fraud.

3. Seasonal Access Reviews

Remove temporary system access when contracts end or roles shift. Expired credentials are open invitations for misuse. Establish a December 15 "access freeze" to ensure permissions are reviewed before the holiday rush.

4. Educate Before It Costs You.

Conduct short, focused fraud-awareness briefings. Share real phishing attempts or vendor fraud emails your company has received. Employees remember stories better than slides — and skepticism is a superpower.

5. Monitor and Document.

Review late-December and early-January transactions for unusual activity: duplicate payments, new vendors, or changed bank details. Document every verification step; it's invaluable if auditors, regulators, or insurers come calling.

6. Test Your Controls.

Conduct a surprise “holiday audit” each year by simulating a fraudulent invoice or spoofed email. The goal isn’t to expose mistakes — it’s to build reflexes for when it matters.

7. Engage Advisors Early.

Forensic accountants, CPAs, and legal counsel can review processes before an issue arises. A 30-minute pre-holiday control check-up costs far less than a six-figure forensic investigation in January

Advisors, Make Fraud Prevention a Client Gift

For attorneys, accountants, and consultants, year-end presents both a duty and an opportunity. A five-minute client reminder about holiday fraud exposure can save thousands — while reinforcing your value.

Share a checklist, host a December webinar, or include a short article in your next client newsletter. Clients may forget the holiday cookie tin, but they won’t forget who protected their balance sheet.

Final Thoughts

Fraud doesn’t take holidays — it just changes costumes. Keep your controls crisp, verifications formal, and your skepticism merry and bright.