2025 Fraud Best Practices Checklist

first financial bank

According to the 2024 AFP® Payments Fraud and Control Survey, 80% of organizations were victims of payments fraud attacks in 2023. If that sounds alarming to you, you're not alone.

To help your business stay vigilant, we've put together a list of monthly tips designed to enhance your ability to identify potential fraudulent transactions and adopt a proactive approach.

January

While the focus is often on your financial system, your IT infrastructure and network is also a key point of vulnerability. For example, in a ransomware incident, a fraudster can paralyze all networked applications – from computers to machines on the production floor. Bad actors exploit a variety of points to gain this access. As a best practice, **disable unnecessary peripherals (CD/DVD/USB) and cloud access, and ensure your browsers, plugins, antivirus, and firewall protections are all current and updated.**

February

Watch out for deepfakes which are defined as "an emergent type of threat falling under the greater and more pervasive umbrella of synthetic media, utilize a form of artificial intelligence/machine learning (AI/ML) to create believable, realistic videos, pictures, audio, and text of events which never happened." In a financial situation, a bad actor can copy a senior leader's appearance or speech in order to perpetrate a fraudulent transfer of funds. Some tell-tale behaviors to watch out for include a high sense of urgency, and odd elements like jerky movements or mismatched audio and visuals.

March

Create and define a comprehensive payment policy that seeks to mitigate fraud vulnerabilities. Periodically review your payment procedures to ensure compliance with current best practices.

April

Implement good cyber processes and procedures. Social media training for employees can teach them to avoid sharing sensitive business information online that could be exploited. Train employees on cybersecurity and conduct regular phishing awareness and fraud prevention training.

May

Consult with a third-party risk management company to identify potential vulnerabilities in your systems as well as your employees' behaviors which can be exploited by fraudsters. Commit to establishing practices and policies to address these gaps.

June

If there is a change to established payment instructions, prior to payment, confirm and validate by calling a trusted source. Do not call the phone number provided on the invoice and be wary of internet searches that can turn up bogus websites with fake phone numbers. Always call a known, verified number to confirm new or updated payment instructions.

2025 Fraud Best Practices Checklist

FIRST first financial bank

July

Set up and enforce Dual Control of Payments. As a best practice, require one person to initiate and a second person to approve payments. Two layers of credentials acts as an additional barrier and makes it harder for account takeovers to divert funds.

August

Consult with your company's insurance agent and review your Cybersecurity Plan to ensure adequate coverage for fraud vulnerabilities. With ransomware on the rise, having an appropriate Plan can help mitigate what could be large losses.

September

Utilize fraud mitigation services to help prevent fraudulent activities such as "check washing". Check washing is a type of fraud where a criminal steals a check and removes the ink, then rewrites the check's amount or payee name before fraudulently depositing it. Positive Pay and Payee Positive Pay alert the customer to check alterations that can prevent financial loss.

October

Confirm payment requests are valid by calling the requester directly at a verified number. Internal business compromise is a very real threat. Fraudsters can take over a company's CEO, CFO, or other Senior leaders' email to make it look like the payment request is coming directly from them. This is an attempt to skirt established protocols and divert funds to the bad actors. When in doubt, call the requester directly using a known and verified number to validate the request.

November

Prioritize electronic payments which are more secure than physical checks. Reduce fraud by paying vendors via ACH or credit card.

December

Meet with your bankers on an annual basis to discuss unused accounts and outdated card holders, signers, and administrators. Review and update your account structure. As employees with financial responsibilities leave, immediately contact the Bank to remove that person's access. Making this a priority mitigates fraud vulnerability.

For more information, visit
bankatfirst.com/fraud-awareness
or call 877-322-6530

EQUAL OPPORTUNITY LENDER · EQUAL HOUSING LENDER · FDIC

[1]Oxford Educational resource. Increasing Threat of DeepFake Identities, Department of Homeland Security Public-Private Analytic Exchange Program, 2021, https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf