

FRAUD PREVENTION IN BANKING:

How to protect your payments today

Author: Chad Rottmund, Commercial Content Enablement Consultant

In today's fast-moving digital economy, payments fraud has become one of the most pressing threats facing business owners. In 2024, reported losses to cyber-enabled fraud reached \$16.6 billion, and almost 80% of organizations claimed that they were either targeted or a victim of payments fraud. Fraud prevention can feel overwhelming, complex, and expensive. But for many organizations, the challenge is not recognizing the risk; it's knowing where to begin.

Protecting your organization from payments fraud does not require a fully mature, enterprise-grade program on day one. The most effective strategies begin with small, practical steps that reduce risk quickly and can be expanded over time. By focusing first on the most cost-effective and impactful layers of protection, you can build a solid foundation for long-term fraud resilience.

Fraudster's Newest Targets

While traditional forms of payments fraud remain prevalent, there's a noticeable shift in tactics. Bad actors are increasingly targeting what is often the weakest link in a company's defenses: untrained employees.

Today's financial losses are less about system failures or technical breaches and more about social engineering. These tactics manipulate individuals into authorizing seemingly legitimate transactions under false and malicious pretenses. Fraudsters know that people are easier to exploit than technology. Compounding the issue is the sheer amount of personal and professional information available online. Bad actors can easily impersonate a CEO, customer, banker, or IT support representative, creating a believable scenario that pressures an employee into acting quickly.

With enough data and a manufactured sense of urgency, even well-trained staff can miss subtle red flags and fall victim to payments fraud.

Secure Your Payment System

There is no one silver bullet that will protect your organization from payments fraud and potential monetary loss. Rather than attempting to implement every control at once, a more effective strategy is to build layered defenses over time—creating a security culture that employees can understand, adopt, and sustain.

Start small, focusing on high impact/low-cost areas first. The most effective controls are those that introduce friction at the right moments. Controls do not need to be complex; they only need to be consistently applied.

Fulton Bank

A resilient organization empowers its employees to slow down payments especially when something seems off. If you're looking to "just get started," the areas that can deliver the best bang for your buck and provide immediate value fall into three buckets:

- **Employee Education.** The most effective training focuses on situational awareness and decision-making. Employees do not need to become fraud specialists, but they should learn how to recognize risk when something feels suspicious, like an urgent payment request, unsolicited call, or email requesting sensitive information. When something is off, they should have clearly defined escalation paths and understand the potential impact of fraud on your business.
- **Process Controls.** Controls like dual control or segregation of duties can reduce the risk of human error, internal misconduct, and external attacks. Without them, your business is more vulnerable to schemes like fake invoices, phishing, or unauthorized fund transfers that can drain resources and damage your reputation.
- **Bank Tools.** These tools work alongside good education and processes to keep your accounts secure. Traditional fraud services such as check and ACH positive pay give you control over what clears your account. However, taking full advantage of your online banking's built in alerts and user entitlement settings are paramount to mitigate the risks that we are seeing today.

The Bottom Line

Fraud prevention is a continuous process and progress beats perfection. You don't need a flawless system to start making an impact. By learning how to recognize risk and leverage built-in safeguards, businesses can significantly reduce their exposure to fraud, protect customer trust, and create a more secure payment environment for the long term.

A trusted banking partner can help identify practical starting points and guide your organization as your fraud prevention strategy matures. Payments fraud is not going away, but a layered defense can materially reduce your exposure and help your employees respond quickly and confidently when something feels wrong.

###