FRAUD MANAGEMENT:

Moving from ‘After the Fact’ to Fighting Back

Rethinking the Fight Against Corporate Treasury Fraud

For decades, criminals and businesses have engaged in a peculiar kind of arms race: criminals constantly devise new and different ways to commit fraud, while businesses invest in new tools and technologies to stop them. The problem is criminals adapt and adjust quickly — dropping unproductive schemes, spotting new opportunities — to continually exploit the gaps in a firm’s fraud control.

Traditional, after-the-fact fraud detection approaches have always struggled to keep up with fast-moving criminal innovations. Attacks that happen in a matter of minutes may go undiscovered for hours or days. And once stolen money walks out the door, it’s almost impossible to recover.

It’s time to consider a different approach to fighting treasury fraud. And modern technology is ready. Combined with the right business processes and organizational changes, new tools can detect fraud in real time, stopping attacks before money changes hands. A corporate treasury team can take back control of its financial systems, rather than just counting their losses.

Let’s look at some reasons why the traditional approach to dealing with treasury fraud needs to evolve. Then, we’ll explain what to look for in a modern fraud-fighting solution that turns the tables on would-be thieves.

The Fraud Control Status Quo: Spending More, Getting Less

It's never a good thing when a business keeps spending more to solve a problem that keeps getting worse. In many cases, however, that's exactly what companies are doing with their current security investments. Here are three serious issues with current fraud control measures:

1 **Security spending continues to increase.** Corporate treasury departments are pouring resources into fraud and cybersecurity tools. Six times as many businesses are increasing their spending this year compared to the number of firms spending less.

Organizations are focusing much of this spending on treasury-fraud pain points that include accounts payable (AP) operations, reconciliation, account-level controls, and fraud monitoring/reporting services. Today, however, corporations must also address new attacks tied to fast-paced digital transformation initiatives. According to Juniper Research, spending on Internet of Things (IoT) cybersecurity solutions will reach $6 billion — almost a 300% increase — by 2023.[1] As organizations continue to build out vast networks of interconnected, integrated, and often autonomous devices — any one of which could provide an entry-point for free-roaming cyberthreats — the scale and scope of their security investments must keep pace.

2 **The number and severity of treasury fraud attacks continue to grow.** Over the past three years, incidents of treasury fraud have become more common: 57% of companies say they've been targeted in the last 12 months, compared to 52% who said that in 2017 and just 40% in 2016.

A closer look at the fraud landscape reveals some notable trends:

- The number of organizations reporting ransomware attacks tripled over the past year.
- 75% of organizations reported business email compromise (BEC) attacks.
- Almost 30% of system-level wire fraud attacks resulted in a financial loss.

Treasury departments are acutely aware of the attention they're getting from criminals: 84% believe the threat they face from cyber or payment fraud attacks increased during the past year.

In addition, a growing number of organizations recognize the risk they face from insider attacks: 53% say they experienced at least one insider attack last year, and 27% say insider attacks are getting more frequent.[2] While current employees are the most commonly cited source of insider attacks, former employees and current/former suppliers all contribute to the insider threat. And while many companies are gaining a clear picture of their exposure to insider vs. external attacks, many others struggle to consistently make this distinction.

3

Complacency is taking a toll. Currently, 61% of companies say they're in a better position to fight fraud this year versus the year before. That's already a dubious assumption, given a growing fraud threat and relatively high success rates for criminals. To make matters worse, the current focus on AP payments and other high-profile pain points may come at the expense of other fundamental fraud-fighting capabilities.

The number of treasury departments with real-time visibility into business accounts — a key to stopping fraud before losses occur — is no longer increasing and has held steady at 70% since 2016.

The number that perform daily account reconciliation, another basic anti-fraud capability, fell to 35% this year from a high of 45% in 2016.

Just 31% of companies still use partially automated reconciliation processes, while 22% perform reconciliation entirely by hand.

Many of these trends point to the same underlying problem: organizations are addressing treasury fraud in a piecemeal fashion, rather than taking a holistic approach to combat it. It's a form of tunnel vision that supports a rosy view of their fraud and security investments, even as threats multiply and basic fraud-prevention capabilities begin to atrophy.

The Alternative: A Proactive Formula for a Real-Time Fraud Defense

It's no mystery what needs to happen to make treasury fraud a less lucrative game for criminals: preventing fraud-related loss by blocking transfers before money changes hands. And this, in turn, requires the ability to identify attacks and to take countermeasures nearly in real time — not hours or days after the fact.

Solutions that achieve accurate, real-time fraud prevention are built on four core capabilities:

1. **Don't take basic security practices for granted.** Some cyber attacks are truly subtle and sophisticated, but many exploit overlooked gaps in anti-fraud practices. Locking down your cash visibility and reconciliations, for example, gives your organization a solid foundation for its anti-fraud strategy.

2. **Take anomalies seriously.** Most attackers tip their hands at some point — engaging in anomalous behavior or small but significant departures from standard treasury practices. Your ability to monitor for and respond to anomalous behavior can make the difference between foiling an attack and counting your losses.

3. **Unlock the power of integration.** Modern cybersecurity solutions should sit within a comprehensive control framework that enables real-time fraud prevention and stops attacks before they result in losses.

4. **Embrace the human factor in cybersecurity.** An organization's employees are its first line of defense against cybercrime, yet just 53% of firms offer formal anti-fraud training programs. In addition to technology-related training, an organization should consider introducing treasury- and payment-specific security training that equips employees to recognize and respond to these types of attacks, as well as encourage best practices like daily reconciliation.

Stop Fraud and Cut Losses

Treasury departments that implement anti-fraud systems built on these pillars are well-positioned to move away from passive, after-the-fact fraud detection models. Instead, these organizations can implement a proactive, real-time approach that prevents fraud-related losses.

Such a shift is truly revolutionary in terms of its ability to give treasury departments a decisive advantage over would-be attackers.

LEARN MORE

All data points, unless otherwise noted, are from the 2018 Treasury Fraud & Controls Survey Report by Strategic Treasurer and Bottomline.

[1] PYMNTS.com, "IoT Security Solutions to Hit $6B by 2023," July 11, 2018
[2] CA Technologies, 2018 Insider Threat Report, 2018