FIVE KEY CFO CHALLENGES FOR ADDRESSING PAYMENTS FRAUD

It seems counterintuitive. Even as businesses spend more time and money than ever combatting payments fraud, the crime itself becomes more ubiquitous. In a new study by CFO Research, 40 percent of senior finance executives report that organizations in their industries are experiencing a much higher incidence of payments fraud than they did two years ago. Payments fraud is any fraud that involves falsely creating or diverting payments. Check fraud, credit card fraud, access fraud, and "spear-phishing" are common varieties seen by CFOs. Some finance chiefs report that the risk associated with payments fraud now approaches the materiality of foreign exchange risk and other high-value uncertainties. Indeed, beyond

CFO
An argyle. Company

kyriba™

OCTOBER 2017

the sometimes substantial hard-dollar costs, payments fraud can result in lower productivity among employees tasked with dealing with the fallout, adverse customer experiences, the actual loss of customers, a stained corporate reputation, and, for publicly traded companies, losses in stock market valuation.

For CFOs charged with safeguarding corporate coffers, there is no silver bullet that can stop payments fraud in its tracks. Managing and minimizing the problem is a discipline unto itself. Done well, it is a holistic, proactive undertaking that combines best-practice processes with dedicated detection and monitoring programs built on the latest advanced technologies. Done well, it also allows CFOs to do a better job of keeping corporate directors apprised of the risks their companies face in this area, and the safeguards in place to mitigate them.

IDENTIFYING—AND RESOLVING—THE CHALLENGES TO SUCCESS

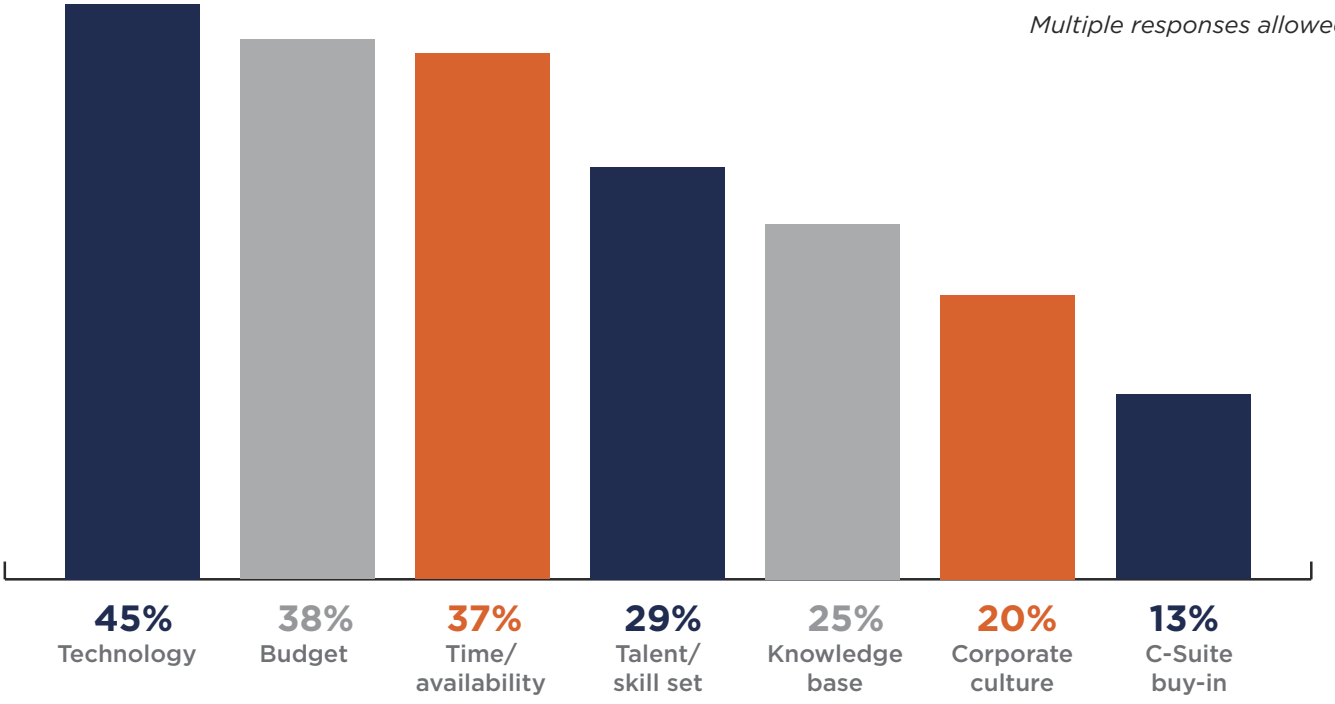
The biggest challenge that CFOs face in combatting payments fraud is finding and implementing the right technology. Technology was cited as a key challenge by nearly one-in-two (45 percent) of survey respondents in the recent CFO Research survey. Conducted in collaboration with Kyriba, the survey polled 167 U.S. finance executives at companies with more than $100 million in annual revenues across a wide range of industries. (See Figure 1).

Other commonly cited obstacles include securing the budget for anti-fraud initiatives (38 percent), and finding the time to pursue them (37 percent). Rounding out the top five challenges, finance executives say it's a challenge to assemble a team with the skill sets (29 percent) and knowledge base (25 percent) needed to fight payments fraud effectively. And, anecdotally, some respondents

FIGURE 1

The biggest challenges my finance team faces in trying to combat payments fraud

Multiple responses allowed



also suggest that companies aren't doing enough on the front lines to fight fraud.

"Work with the clerks and managers that are likely to be the first people to be contacted or become aware of a fraud attempt," one survey respondent advises. "They can stop attempts before they get to the payment phase."

Another finance executive suggests it is simply time to buckle down to the task at hand and do a better job of it. "Set aside sufficient budget, do the proper research, then employ the right specialists to get this in place," the respondent admonishes.

"Invest in strong technology and air-tight workflow," writes another. "Allocate the people and resources to combat and reduce fraud—(the) benefits fall to the bottom line," writes still another.

REPORT FROM THE FRONT: FRAUD IS ON THE RISE

Payments fraud is on the rise. Four in ten (40 percent) of survey respondents say organizations in their industries are experiencing a much higher incidence of payments fraud than they did just two years ago. Another 15 percent say they can't confirm or rebut the idea, leaving open the possibility that increases in payments fraud are broader still.

These findings are directionally consistent with other studies, including the 2017 AFP Payments Fraud and Control Survey conducted by the Association for Financial Professionals. It found that 74 percent of organizations had experienced attempted or actual payments fraud in 2016, up from 62 percent in 2014 and the highest level recorded since the AFP began tracking the problem in 2006.

Contrary to what one might expect, it isn't always smaller, less sophisticated enterprises that are being impacted by payments fraud. In 2016, the AFP survey found, organizations with at least $1 billion in annual revenue were actually more likely than their smaller counterparts to have been hit by the crime. And while the majority of the respondents to that survey reported that their company's direct payments-fraud losses were relatively small—less than $100,000—32 percent of financial professionals at companies with at least $1 billion in revenue and more than 100 payment accounts reported losses exceeding $500,000. Within that group, 16 percent said their losses exceeded $2 million.

The reason behind the growing incidence of payments fraud isn't hard to fathom. Throughout history, criminals have demonstrated a remarkable dedication to trying to outsmart their victims, and the advent of new technologies such as social media and mobile shopping and mobile banking have simply widened the field of opportunity. While check fraud remains the most common type of payments fraud, for example, criminals today are increasingly exploiting the digital technologies that make it faster and easier for companies and consumers to interact with each other. Last June, the Federal Bureau of Investigation felt compelled to issue an alert warning about the growing problem of "business email compromise," in which fraudsters target businesses working with foreign suppliers, or businesses that regularly make wire transfer payments.

The relentless enthusiasm exhibited by criminals searching for new ways to defraud businesses means that businesses must combat their efforts with equally relentless countermeasures.

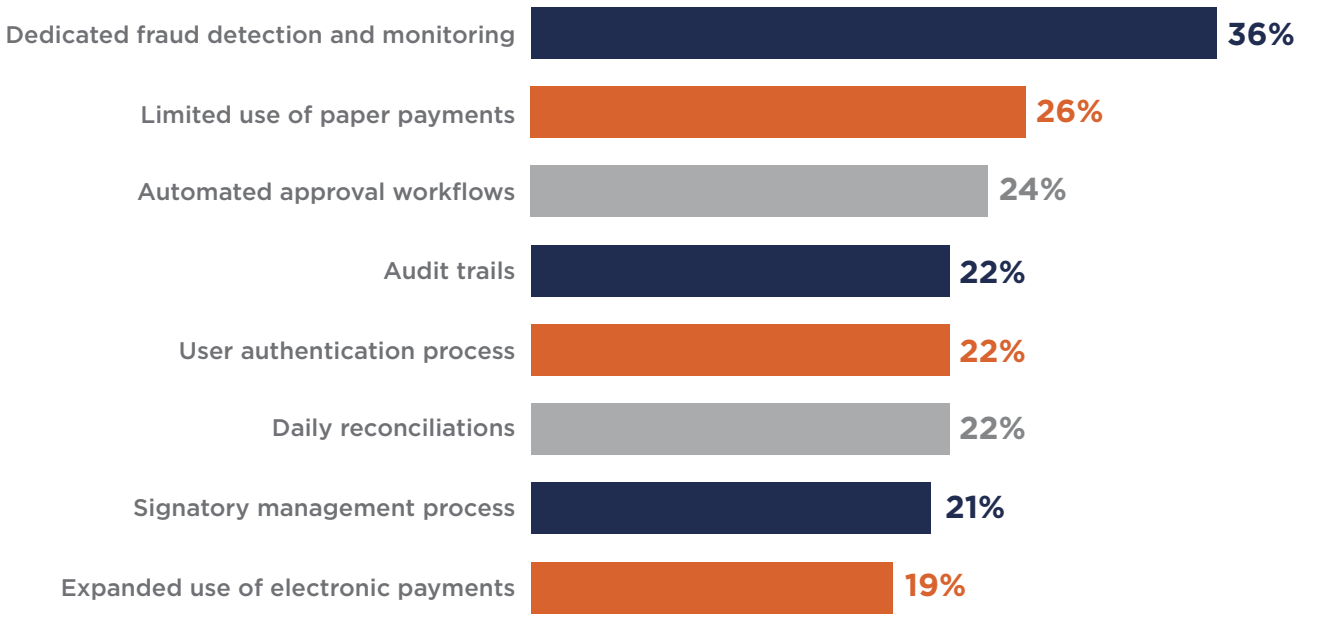
ELEVATING PAYMENTS FRAUD DETECTION TO A FIRST-ORDER PRIORITY

Only 10 percent of the executives in the CFO Research survey feel strongly that most finance teams in their industry have strong processes and technologies in place to capably and efficiently detect fraud or ensure fraud-related compliance. It is a weak endorsement of current

FIGURE 2

Tactics for managing payments fraud that my finance team should substantially improve

Multiple responses allowed



strategies for managing payments fraud.

And where companies do seek to battle back, the tactics they use often are aimed at historical threats rather than evolving fraud strategies. Asked which are the most important tactics used by their companies, 45 percent of survey respondents cite auditing (audit trails). That's followed by expanded use of electronic payments (41 percent) and daily reconciliations (35 percent). All three are valuable tools, to be sure. By contrast, consider that only about one-third of survey respondents (34 percent) say they employ dedicated fraud detection and monitoring systems that can proactively ferret out fraud attempts. The CFO too often appears to be checking the rear-view mirror instead of scanning the road ahead for trouble.

Many finance executives also admit that they need to be doing more to support their boards of directors in this area. Asked where their boards most often fail to receive critical information and decision-support data from the CFO, 43 percent list fraud monitoring and mitigation—more than any other area. Thirty-seven percent also say their organizations lack the tools or technology to enable the board to make good decisions on this issue.

THE WAY FORWARD: FRAUD DETECTION

Where to begin? Dedicated fraud detection and monitoring systems top that list of tactics that the finance team should substantially improve. Cited by 36 percent of survey respondents, fraud detection and monitoring handily outpaces other tools and practices that include limiting the use of paper payments (26 percent), automated approval workflows (24 percent), audit trails (22 percent) and daily reconciliations (22 percent). (See Figure 2).

continued on page 6

Ten Best Practices for Combatting Payments Fraud

1. Understand your vulnerabilities. With so many types of payments fraud, it's impossible to do a good job of combatting them without understanding what they are. Examples include external threats such as hacking of treasury systems by third parties, as well as a raft of internal threats. The latter include fraudulent payments sent by employees to a company's bank, either willfully or as an unknowing consequence of a spear-phishing attack; and fraudulent purchase orders and invoices created by employees that are then paid out to related third parties.

2. Erect roadblocks to unauthorized access to corporate information systems. Deploy robust login and user authentication procedures, including dual-factor and in some cases multi-factor authentication.

3. Move finance data to the cloud. While data security has long been cited as a reason for not moving data to the cloud, the growing consensus today is that cloud providers, for whom security is a core competency, offer greater, not weaker, security systems and protocols than most companies can deliver on their own. Because a significant percentage of payments fraud originates internally, moving corporate finance data to the cloud can reduce the opportunity for it to occur.

4. Boost control over global bank accounts. Maintaining a handle on bank accounts becomes more difficult as companies grow and expand globally, but it's a task that can't be ignored. Companies need to make sure they have systems that can provide transparency into accounts, authorized signers and account documentation; track all bank activity; and efficiently reconcile accounts with banking partners.

5. Make use of digital signatures. All commerce and banking today is electronic at some point in the payments cycle. Digital signatures, which can help authenticate transmitted payment files, can minimize opportunities for payments fraud.

6. Centralize payments activity in a single system. Coupled with multiple, standardized and electronic approvals, an integrated payments system allows for a complete and detailed electronic paper trail for all payments, minimizing opportunities for fraud.

7. Standardize settlement instructions for financial trades. For any kind of investment transaction, including foreign exchange and derivatives transactions, embedding standardized settlement instructions in corporate financial systems can not only improve efficiency but also help block any redirection of funds to unauthorized accounts.

8. Educate employees. Even the best anti-fraud program will spot fraud only after it's occurred. That's still extraordinarily valuable, especially when the system is able to spot the fraud quickly. But one of the best ways to prevent payments fraud is to educate employees about the various types of fraudulent schemes they may encounter, so that they can avoid being duped by them and prevent fraud from occurring in the first place.

9. Update and test your fraud-detection capabilities. Corporations should review their payments-fraud detection/monitoring systems and protocols to make sure they're working. Some companies may have the resources to do this internally, but many will find it makes sense to engage a third-party expert to both create defense systems and to test them regularly.

10. Regularly participate in opportunities to share with and learn from other organizations. Few "industries" adapt and evolve faster than the payments-fraud industry. A company can no more allow its fraud detection and prevention program to remain static than it could allow its products or services to remain unchanged. Companies should make sure the finance function, and any others that touch on the payments process, participate in conferences and workshops where they can share with and learn from other organizations combatting the same challenges.

continued from page 4

Several survey respondents noted that the ever-shifting and expanding payments-fraud landscape is sufficiently daunting that they advise turning over the work—particularly fraud detection and monitoring activities—to third-party providers for whom it is a core capability. As one survey respondent puts it, "Outsource much of the fraud function to companies that have strong controls. Third parties may be better at this than your team."

CONCLUSION

Focusing on the five core challenges to addressing payments fraud is a strong way to get started. Technology, Budget, Time, Skills, and Knowledge are all critical components to developing and implementing an effective strategy. The sidebar, "Ten Best Practices for Combatting Payments Fraud" adds some tactical specificity to the CFO's search for an answer to payments fraud.

No matter which route CFOs take, it's clear that getting going sooner rather than later makes sense—especially if they count their own organizations among those that are only modestly effective at managing payments-fraud risk today. CFOs increasingly feel that fraud detection and monitoring must become one of their core responsibilities, because it is the only chance they have of staying at least even with an evolving threat. And that threat is not only about the money; it is about the customer, and the brand, and the business.

"YOU NEED TO START ALREADY. **THE CRIMINALS ARE ADAPTING FASTER THAN WE ARE."**

"You need to start already," concludes one survey respondent. "The criminals are adapting faster than we are."

ABOUT THE SPONSOR

Kyriba is the #1 provider of cloud treasury and financial management solutions. Kyriba empowers financial leaders and their teams with award-winning solutions for cash and risk management, payments and supply chain finance. Kyriba delivers a highly secure, 100% SaaS platform, superior bank connectivity and a seamlessly integrated solution set for tackling today's most complex financial challenges. More than 1,600 companies, including many of the world's largest organizations, rely on Kyriba to streamline key processes, enhance fraud protection and compliance, and accelerate growth opportunities through improved decision support. Kyriba is headquartered in New York, with offices in San Diego, Paris, London, Tokyo, Dubai and other major locations. For more information, visit **www.kyriba.com.**