The Hackett Group
World Class Defined and Enabled

Finance Executive Insight
Management Issue
March 1, 2019

How CFOs Can Mitigate the Risk of Payments Fraud

By Nilly Essaides and Bryan DeGraw

Executive Summary

As custodians of the company's monetary assets, CFOs are responsible for safeguarding the enterprise from threats to its financial health, especially those that can result from processes within the finance domain, such as accounts payable and treasury. According to market research, payments fraud is rising. It is therefore critical that CFOs adopt effective strategies to alleviate the potential hit to the bottom line and investor confidence. We have identified five approaches that can help minimize fraud risk:

1. Comprehensive and enforceable payment policies and rules.
2. Embedded fraud prevention and detection procedures.
3. Automated/digitized payment processes.
4. Consolidated payments workflow.
5. Mandated education for employees about fraud detection and prevention.

Introduction

Businesses are falling victim to payments fraud at an increasing rate. In the U.S., this is in part because of the still-dominant use of paper checks as a payment medium. At the same time, and at a global level, the situation is exacerbated by fast, new electronic payment options, such as same-day automated clearing house (ACH) service. In the January 2018 edition of the Kroll Global Fraud & Risk Report, 84% of global business executives reported that their companies experienced at least one instance of fraud in the previous 12 months, up from 74% in 2017. According to statistics collected by Kyriba, a treasury system vendor, 52% of treasury teams were victims of fraud in 2018. Yet nearly one-quarter of companies have done nothing new to combat fraud risk in the past 12 months.

Payments fraud occurs when an account is compromised through a counterfeit check, unauthorized ACH transaction or electronic/wire transfer. While treasury payments are at risk, the largest exposure is in executing supplier payments due to the high volume of transactions, potentially large dollar amounts, as well as often-decentralized workflow. This is especially true for large organizations with different methods for paying vendors, complex contractual agreements, and multiple locations, business units and payment centers. The potential for fraud is compounded by rapid company growth, acquisitions and the migration of more finance activities to global business services organizations (GBS).

Most research shows that fraudulent payments are initiated by non-employees through counterfeit checks or company checks with forged signatures; unauthorized wire transfers or ACH transactions; the interception and redirection of confidential financial information through cyberattacks; forged or stolen procurement cards; and business email compromise (BEC). The latter is a sophisticated and increasingly pervasive scam targeting businesses working with foreign suppliers and businesses that regularly execute wire transfers. BEC scammers use official company emails to send seemingly valid payment instructions that direct unauthorized transfers of funds.

Of course, insiders commit fraud, too. For example, an accounts payable employee may issue checks to fictitious payees and mail them to a post-office box, where they are picked up and cashed or quickly transferred to an offshore account.

Five Steps to Limit Phony Payments

As discussed above, finance is experiencing an escalation in payments fraud incidents. There are several steps finance can take to minimizing their occurrence and effects.

1. **Develop comprehensive and enforceable payments policies and rules:** Anti-fraud policies should consider the array of potential sources of fraud and prioritize those with greatest potential impact on the business. For example, there should be stringent controls around payments made to parties in high-risk countries. At organizations with a large and dynamic supplier base, policies must govern the handling of newly established and recently modified accounts, and include screening rules that prescribe how to enforce those policies **(Fig. 1)**. As an organization's payments environment and operations evolve and become more complex, it is important to periodically review and update payments policies and detection mechanisms.

FIG. 1 Linking policies to screening rules

Payment policy	Screening rule
Payments should only go to approved suppliers in approved countries.	All payments to non-approved countries must be stopped.
Payments initiated by accounts payable in the ERP must be approved by the treasury department.	Any payments that are modified after import must be stopped.
Single or multiple payments to the same beneficiary may not exceed a specified limit.	Hold for review any payments that cumulatively exceed specified limit per day/week/month.
All payments to a new bank account must be reviewed by the treasurer.	The first payment to a new or modified bank account must be held for review.

Source: The Hackett Group

Exceptions create opportunities for fraud. Therefore, finance must stringently limit the number of irregular payments. Even payments requests from the highest levels of the organization must be channeled through defined controls and approval processes. Sometimes, asking corporate officers to personally verify unusual requests can be the quickest way to stop bogus payments. Finally, the organization must reinforce an environment of zero tolerance for fraud by unambiguously communicating its consequences, e.g., fraud incidents will be reported to the relevant legal authority and guilty parties will be punished to the full extent allowed by law.

2. **Employ best-of-breed fraud detection and prevention practices:** Screening and detection are critical elements of the payments workflow. They ensure compliance with established rules and identify and quarantine suspicious activity. Today, tools including AI and robotic process automation can automate the screening process.

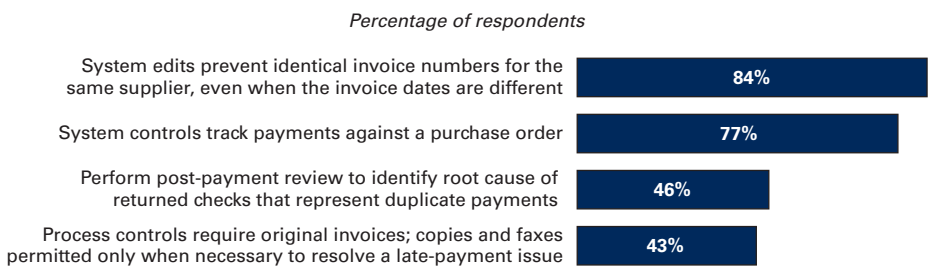
   It is also important that approvers watch out for red flags. For example:

   - Cases in which there are two or more vendors with the same address and/or phone number.
   - When vendors have names that are similar but not identical to those of familiar partners of the organization.
   - Vendor accounts with no phone number, an unlisted phone number, a non-business phone number such as a mobile phone, or a number that is always answered by a machine or voicemail.
   - Situations when the address is a post office box or mail drop, or when the address is the same as the home address of an employee.
   - Incidents when a vendor's master data records have not been updated in a year or more.
   - invoice abnormalities, e.g., two or more invoices with the same ID number, or that are from the same vendor but are not sequentially numbered, photocopied or scanned.
   - Duplicate payment requests.
   - Payments that vary from historical levels in dollar amount and/or volume of invoices.
   - Invoices for amounts that are just below the threshold that requires additional review.
   - Vendors presenting a large number (or higher-than-average percentage) of invoices with rounded dollar amounts.

3. **Deploy smart automation to permit real-time screening and detection:** As payments volumes increase, employees cannot be the only line of defense for identifying and stopping suspicious activities. Rather, finance leaders must enhance protections by automating payments processes while streamlining different activities into a single, well-governed workflow. Digital transformation may increase the speed with which fraud can occur and open fresh avenues for infiltrating the payments process, but companies can also wield digital technology to fight back, integrating payments and automatically scanning all activity using both defined and open parameters.

   Most respondents to The Hackett Group's Purchase-to-Pay Performance Study report that they already have systems to conduct specific activities, for example, to quickly identify and stop payments for identical invoice numbers for the same supplier (84%), as well as track payments against a purchase order (77%). However, less than half conduct an automated post-payment review to analyze returned checks that represent duplicate payments (Fig. 2).

FIG. 2 Practices for managing compliance across accounts payable



Source: Purchase-to-Pay Performance Study, The Hackett Group, 2015

Cyber risk

Cybersecurity is the leading business risk in 2019, according to finance executives participating in The Hackett Group's 2019 Key Issues Study. It also experienced the highest percentage rise in ranking from the 2018 edition of the study, reflecting the sense of urgency business executives currently have about it.

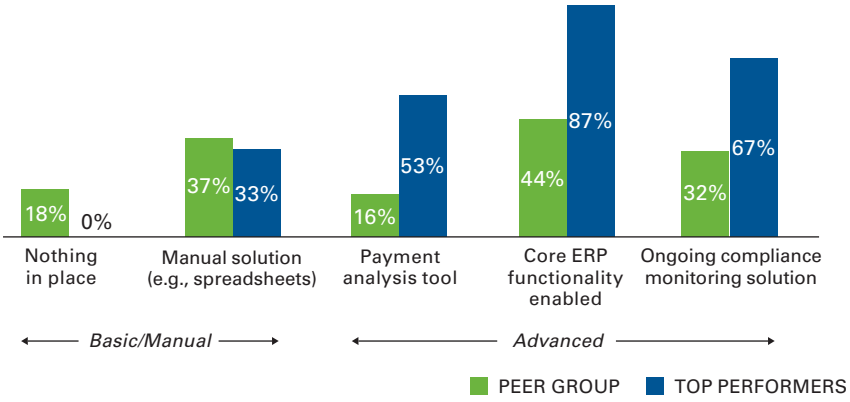
The introduction of digital technology and cloud-based payments platforms requires companies to pay extra attention to information security and controls. While many cloud-based tools incorporate strong security protocols, not all cloud service providers have the same approach to or level of security.

Finance needs to collaborate with the IT organization to ensure that it makes appropriate choices when integrating technology into the payment process. This should include assessing:

- Application security.
- Physical security.
- Vendors' security measures.
- Process security.

The same study revealed that top-performing purchase-to-pay organizations are leading the transition to more advanced solutions for fraud and error detection, including payments analysis tools, enabling more core ERP functionalities, and implementing an ongoing compliance monitoring solution (Fig. 3).

FIG. 3 System functionality to detect and report recovery/error/fraud risks



Source: Purchase-to-Pay Performance Study, The Hackett Group, 2015

Our research and work with clients also show that companies are increasingly deploying customer-facing technologies, which also play a role in preventing payment fraud. For example, supplier portals require vendors to enter and maintain all of their master data records (e.g., name, address, tax ID and bank routing information) so that information can be automatically verified by comparing the details to external databases. Meanwhile, e-invoicing solutions build an additional barrier by eliminating paper invoices and facilitating three-way matching of purchase orders, receipts and invoices. Both supplier portals and e-invoicing enable organizations to block unauthorized users upfront, and eliminate risks inherent in less codified processes such as triggering payments through internal email communications. The digital transformation of the payments process can also simplify the interface with financial institutions, by creating a common payments format and approval procedures. Finance must educate its bank partners about its internal policies and always keep and share its updated list of authorized users.

4. **Consolidate the payments workflow:** Many organizations maintain separate processes and oversight for treasury payments and accounts payable, and even within AP in different regions. To strengthen controls without hampering efficiency, finance needs to overhaul currently siloed practices to merge payments workflows using virtual payment factories, which pull all transactions from the ERP (AP) and treasury into a single processing engine equipped with the latest fraud-detection capabilities.

   By consolidating workflows, finance can standardize fraud prevention and detection practices that cover payment requests, initiation, approval, documentation and transmission. Further, by combining all payment activities, best-practice payments policies and procedures can be applied consistently across all forms of payment, in all geographies, by all staff involved in payments processes, and within specific payments systems. At the same time, finance can adapt more quickly to evolving bank interchange requirements, such as compliance with the Foreign Corrupt Practices Act and Know Your Customer regulations. In addition, the payments process output can be reformatted to meet global banking requirements like those issued by SWIFT dealing with bank-to-bank and corporate-to-bank connectivity.

5. **Employee education on fraud detection and prevention:** Staff involved in the payments workflow must receive training on payments policies and procedures. That requirement should extend to employees responsible for recording vendor data in the company system. The curriculum should include practical information about

Best practices in fraud prevention

The following practices are proven ways to prevent fraudulent payments:

1. **Monthly reconciliation and auditing of accounts payable and the company's checkbook:** Helps catche potential problems, such as missing check numbers or gaps in reconciled check numbers.
2. **ACH debit block:** Eliminates posting of ACH debits based on selected criteria. For example, the company can block all ACH debits, or those above a certain amount or from specific companies.
3. **ACH transaction review:** Enables finance to validate ACH debit and credit transactions that post to the account on a case-by-case basis.
4. **Positive pay:** Maps information about checks to the actual checks presented for payment. Any mismatches are marked as exceptions, and the company can then decide whether they should be paid or returned.
5. **Payee name verification:** Ensures that the person or entity presenting the check for payment is authorized to do so.
6. **Teller positive pay:** Helps prevent check fraud at the branch. Tellers' systems automatically and continuously update check-related information on positive-pay accounts. If an exception is detected, the teller does not cash the check, instead referring the person presenting the check to its issuer.
7. **Post-no-check service:** Ability to reject and return any check presented against an account that does not come with check-writing permission and mark it for additional monitoring.
8. **Reverse positive pay:** Ability to set triggers for further inspection of any checks over a predetermined amount.
9. **Encashment settings:** Protects the company's account at the teller level by preventing non-customers from cashing checks above a predetermined threshold.

when employees should escalate the incident before processing a payment. It should also encourage them to ask questions, for example when a vendor is unwilling to provide complete information (e.g., address or phone). Given that fraud risk and policies are constantly evolving, training should be conducted at least once a year.

To be fully aligned with finance payments policies and procedures, employees must understand that fraud can originate from a variety of sources, for example, bogus but official-looking email instructions, which come from a web-based email account. It's important to verify that the company's domain is used in company personnel emails, and take a second look at domain names that are similar, but not identical, to the company's official name. The "reply" option should never be used when authenticating emailed payment requests; rather, staff should be required to forward the request by typing in the address or selecting from an official company address list. Staff should never share passwords, user names, authentication credentials, or account information when contacted by employees or individuals pretending to work at a partner bank or a vendor.

Conclusion and Recommendations

Too often, payments fraud is not painful enough for companies to do something about it. In fact, some may not even realize it has even occurred. Nevertheless, as risks and costs rise, CFOs must be prepared to prove that fraud-prevention controls are embedded in their governance structure and are in line with internal compliance and risk policies. Here are three actions to minimize the risk of payments fraud:

1. **Finance should not wait for a fraud incident or assume the organization is fully sheltered from fraud risk:** Past actions to halt payments emanating from a specific fraud type may not suffice in other areas. Thus, finance must continuously update its controls and adapt to new fraud patterns. As cyber risk grows, collaborate with the IT organization to deploy new defenses.
2. **Finance should conduct a baseline assessment of its payments-fraud defenses, develop a list of future/desired capabilities, and prioritize new initiatives:** These include process redesign, consolidation of payments activities, and adoption of smart technologies and tools.
3. **Finance must apply common fraud-prevention policies and procedures across the enterprise and for different payment types**: A big step in this direction is consolidating activities in a payments hub or the company's GBS organization and deploying smart technologies to standardize workflows and controls.

Related Hackett Group Research

Tracking the Links Between E-Invoicing and E-Payments, November 2017

Introducing a Methodical Approach to Digital Service Delivery Value Management, July 2017

About the Advisors

Nilly Essaides

Senior Research Director

Ms. Essaides has over 25 years of experience researching, writing, and speaking about finance and treasury issues, with a focus on the way finance adds value to the enterprise through excellence in financial management and planning processes. Previously, she worked at the Association for Financial Professionals, where she led the FP&A practice. Ms. Essaides, a prolific blogger with thousands of LinkedIn followers, writes for external publications such as *Digitalist Magazine*. In addition, she co-authored a book about the internal transfer of best practices, *If Only We Knew What We Know* (Simon & Schuster, 1998).

Bryan DeGraw

Senior Director, Finance Advisory Services

In his current role, Mr. DeGraw conducts topical research, supports client inquiries, leads member webcasts, performs client briefings, and speaks at conferences on topics including working capital, purchase-to-pay and customer-to-cash processes. His expertise includes credit/risk modeling, customer segmentation, collection strategies, supplier risk analysis, buy/ pay transactional strategy, and leverage of automation. He has over 20 years of corporate and consulting experience in business process creation and reengineering, cost reduction/management, planning, budgeting and financial analysis. Mr. DeGraw's previous experience with The Hackett Group has included managing and delivering finance, procurement and other benchmark projects for clients in both the public and private sector.

The Hackett Group (NASDAQ: HCKT), a global strategic business advisory and operations improvement consulting firm, is a leader in best practice advisory, business benchmarking, and transformation consulting services including strategy and operations, working capital management, and globalization advice.

Utilizing best practices and implementation insights from more than 10,000 benchmarking studies, executives use The Hackett Group's empirically-based approach to quickly define and implement initiatives that enable world-class performance. Through its REL group, The Hackett Group offers working capital solutions focused on delivering significant cash flow improvements. Through its Archstone Consulting group, The Hackett Group offers Strategy & Operations consulting services in the Consumer and Industrial Products, Pharmaceutical, Manufacturing, and Financial Services industry sectors. Through its Hackett Technology Solutions group, The Hackett Group offers business application consulting services that help maximize returns on IT investments. The Hackett Group has completed benchmark studies with over 3,500 major corporations and government agencies, including 93% of the Dow Jones Industrials, 83% of the Fortune 100, 87% of the DAX 30 and 48% of the FTSE 100.

Founded in 1991, The Hackett Group was acquired by Answerthink, Inc. in 1997. Answerthink was renamed The Hackett Group, Inc. in 2008. The Hackett Group has global offices in the United States, Europe and Asia/Pacific and is publicly traded on the NASDAQ as HCKT.

The Hackett Group
World Class Defined and Enabled

Email: info@thehackettgroup.com
www.thehackettgroup.com

Atlanta +1 770 225 3600
London +44 20 7398 9100
Sydney +61 2 9299 8830

Amsterdam, Atlanta, British Columbia, Chicago, Frankfurt, Hyderabad, London, New York, Paris, Philadelphia, San Francisco, Sydney