THE CFO'S GUIDE

To Digitizing B2B Payments

August/September 2020

PYMNTS.com | COMDATA

TABLE OF CONTENTS

PYMNTS.com | COMDATA

THE CFO'S GUIDE

To Digitizing B2B Payments

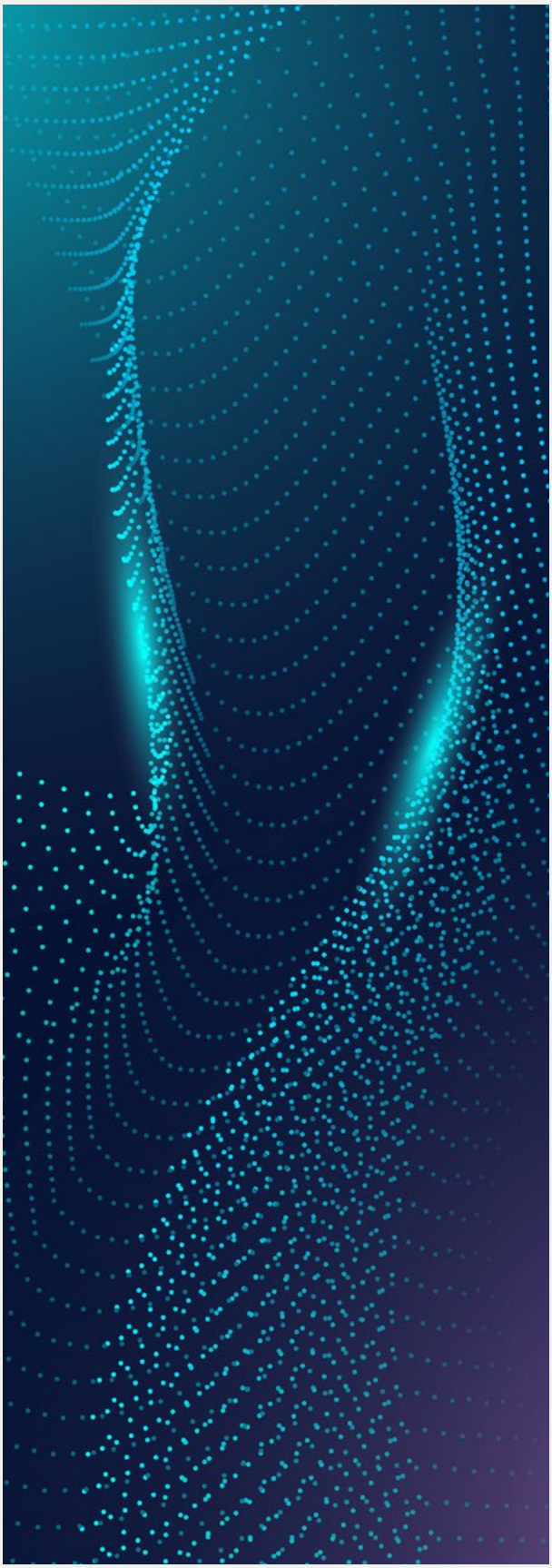
ACKNOWLEDGMENT

The CFO's Guide To Digitizing B2B Payments was done in collaboration with Comdata, and PYMNTS is grateful for the company's support and insight. PYMNTS.com retains full editorial control over the following findings, methodology and data analysis.

WHAT'S INSIDE

Companies are eagerly implementing accounts payable (AP) upgrades and eyeing ways to improve their business-to-business (B2B) payments, especially given the COVID-19 pandemic. They must ensure they do so securely, however, as each new technology can introduce vulnerabilities alongside its benefits if it is not properly guarded against fraud.

Many organizations are examining faster payments technologies, for example, with all but 9 percent of respondents in a recent survey of United States businesses saying that they intended to leverage The Clearing House's Real-Time Payments (RTP) rail. This will enable money and payments data to transfer instantly from buyers to their suppliers, but the U.S. Faster Payments Council (FPC) recently warned that more work must be done to prevent fraudsters from taking advantage of such offerings' rapid pace. The council explained that financial companies need to detect and react to threats faster than ever as RTP use expands.



Businesses already face fraud attacks including external phishing attempts and internal schemes perpetrated by unscrupulous AP employees. The pandemic has strained companies' budgets, but businesses are likely to find that investing in AP is more important now than ever, according to some financial players. AP automation can help detect fraud attempts and catch honest errors, foiling would-be thefts and helping funds move smoothly at a time when businesses cannot afford losses.

AROUND THE B2B PAYMENTS WORLD

Business email compromise (BEC) schemes — in which fraudsters pretend to be executives when interacting with AP staff members via email — are growing more prevalent during the health crisis. Cybercriminals launching these schemes attempt to persuade staff to change suppliers' payment details so that money will flow into fraudsters' bank accounts rather than those of the actual vendors. Companies must be on high alert for such ploys, too, as BEC-based payment and invoice fraud grew 200 percent between April and May.

Businesses that have manual, paper-based payment methods also face internal fraud risks, Neal Anderson, CEO and president of AP and accounts receivable (AR) automation company OnPay Solutions, said in a recent interview. Some companies have even sent staff home with check printers to enable them to keep issuing payments during the pandemic, but this could tempt them to print extra checks for personal use, for example.

Adopting more AP solutions can help firms catch both honest errors and deliberate fraud. Three-way invoice-matching solutions are one example as these tools enable companies to compare details on invoices, receipts and purchase orders to ensupe all details match and are correct, preventing companies from facing prices that were higher than those upon which they agreed or charges for items that were never delivered.

For more on these stories and other headlines from the B2B payments space, check out the Guide's News and Trends section (p. 10).

USING AP AUTOMATION, WORKFLOW STANDARDIZATION TO BATTLE BEC SCHEMES

Translation companies need to manage cross-border payouts to independently contracted language professionals worldwide, all while fending off fraudsters' attempts to steal those funds. Bad actors are eager to trick AP staff with BEC scams and faked invoices and even honest human errors can cause unwary companies to lose money by paying off duplicate invoices. In this month's Feature Story (p. 7), Toni Tornell, controller at language services provider United Language Group (ULG), explains how clear payments approval protocols can help financial staff members evade fraudsters' manipulations and outlines how AP and ERP systems can catch invoicing mistakes.

DEEP DIVE: HOW CFOs TAKE ON AP FRAUD AND DATA SECURITY

Financial teams need to fend off hackers' attempts to steal their sensitive data as well as trick AP employees into sending them money, and chief financial officers (CFOs) are looking to get ahead of these threats and protect their firms. This month's Deep Dive (p. 16) explores these threats' severity and detail how companies can leverage new strategies and automated technologies to improve their fraud detection and prevention efforts.

EXECUTIVE INSIGHT

What kinds of AP technologies and strategies can help companies improve their security and better combat fraudsters?

"Even in ordinary circumstances, accounts Payable departments have a lot of responsibility for managing a company's payment obligations: processing invoices from vendors, matching them to purchase orders and vendor contracts, ensuring payment terms are adhered to, selecting the optimal payment method and, of course, working to reduce risk and protect against fraudsters. Compounding those responsibilities by now having to work remotely without physical access to workplace resources can make an already challenging job even more so.

Companies who have already invested in digital transformation … are ahead of the game. One tried-and-true strategy is to utilize virtual credit cards to not only transform the procure-to-pay process but to reduce risk and create a new revenue stream in the process. Paying vendors through a single-use account, a virtual card solution, saves time [and] reduces risk, as one-time transactions can be restricted by date, amount and … vendor. In fact, a recent study found that '[single-use accounts] experience the lowest fraud rate of any commercial card product, below the average rate of 0.0012 percent for electronic payment solutions.'

In these trying economic times, every business is looking for opportunities to gain efficiencies, drive revenue and reduce risk. Optimizing your accounts payable process is a critical business strategy, and incorporating a virtual commercial card program can help you make tangible gains toward cost savings, realizing incremental revenue and lowering fraud risk. Best of all, these fully digital programs can be operated remotely, making those accounts payable folks' jobs just a bit easier."

Tad Fordyce
senior vice president of product at Comdata

FAST FIVE FACTS

5

PYMNTS.com | COMDATA

1,000

Number of companies targeted in a recent BEC attack

200%

Rise in BEC attacks attempting payments and invoice fraud between April and May

75%

Share of CFOs who had to make significant updates to enable AP staff to go remote

68%

Portion of CFOs and vice presidents of finance who said in 2019 that they prioritized data security

84%

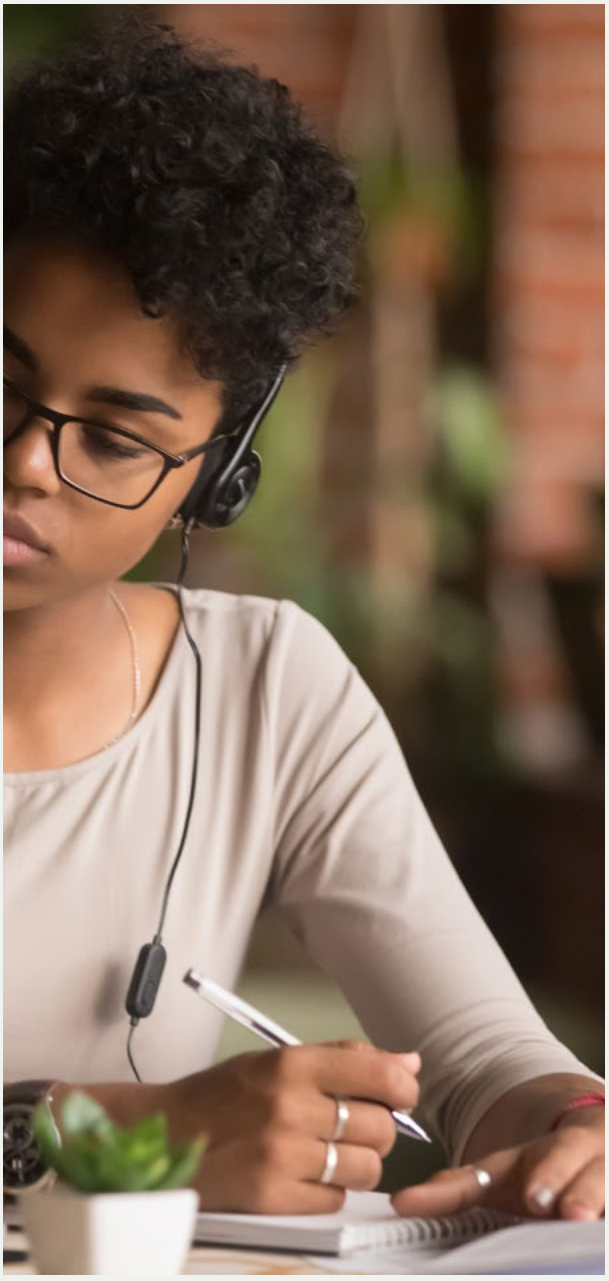
Share of SMBs that expect AP updates to save them time

THE CFO'S GUIDE

To Digitizing B2B Payments

HOW AP TEAMS CAN PROTECT INDEPENDENT CONTRACTOR PAYOUTS FROM FRAUD

FEATURE STORY



The global language services market was valued at $46.9 billion in 2019 and businesses seeking to claim a bigger share of it must have the right payment tools on hand. Translation companies must smoothly and securely deliver payouts to thousands of freelance linguists around the world, for example, and supply the preferred currency and payment method for each. Fraudsters may attempt to take control of these transaction flows and divert funds, however, and the COVID-19 pandemic has encouraged many criminals to redouble their efforts to trick AP departments and make off with money.

Clear, standardized protocols and workflows — and the software systems that underpin them — can help AP teams keep independent contractors paid and fraudsters frustrated, according to Toni Tornell, controller at translation services provider United Language Group. Tornell recently spoke to PYMNTS about how AP automation tools and policies can bolster companies' efforts to prevent targeted crime and human errors from disrupting independent contractor payouts.

CATCHING NEW INVOICE FRAUD

Bad actors have put their BEC schemes into overdrive during the pandemic, seeking to manipulate staff members who are adjusting to remote work operations. Tornell said she and her team frequently receive fraudulent messages purporting to be from top executives and instructing the AP staff to quickly pay off invoices. These messages may be missing critical details, however, such as the intended recipients' tax ID numbers or other elements.

"I personally get emails all the time that look like they're coming from executives — and they're not — asking me to process an invoice immediately and [saying] they'll get me details later. But I know that's not our policy," Tornell said. "No one will ever say, 'Process this immediately, and I'll get you the details later.' The only people who are doing that are fraudsters."

Criminals using such scams manufacture a sense of urgency to trick staff into acting without thinking. Warding off such attacks requires AP departments to institute clear rules prohibiting staff from initiating payments until complete details have been provided and transactions have received the appropriate sign-offs, Tornell said. Having strong supporting policies and procedures can help cut through the confusion of the moment.

SECURELY PAYING EXISTING VENDORS

A similarly careful approach has been important to detecting another form of BEC in which fraudsters masquerade as vendors who are already in companies' systems. Criminals use this pretense to ask for banking details to be updated in the company's systems with their own. ULG has fought such attacks by requiring staff to confirm any payment detail change requests directly with vendors through separate, live channels such as calling them rather than replying to the potentially fraudulent emails.

Deliberate fraud is only one factor that can misappropriate payouts, however. Companies may also be wise to implement systems that reduce opportunities for human error. ULG took such an approach by adopting a digital AP platform that features a vendor portal in which language professionals can enter and confirm their payment method preferences and transaction information. The platform enabled ULG to abandon its previous practice of having AP staff take down details over the phone, which ran the risk of payment information being misheard or misspelled as employees manually keyed it in.

INVOICE ACCURACY

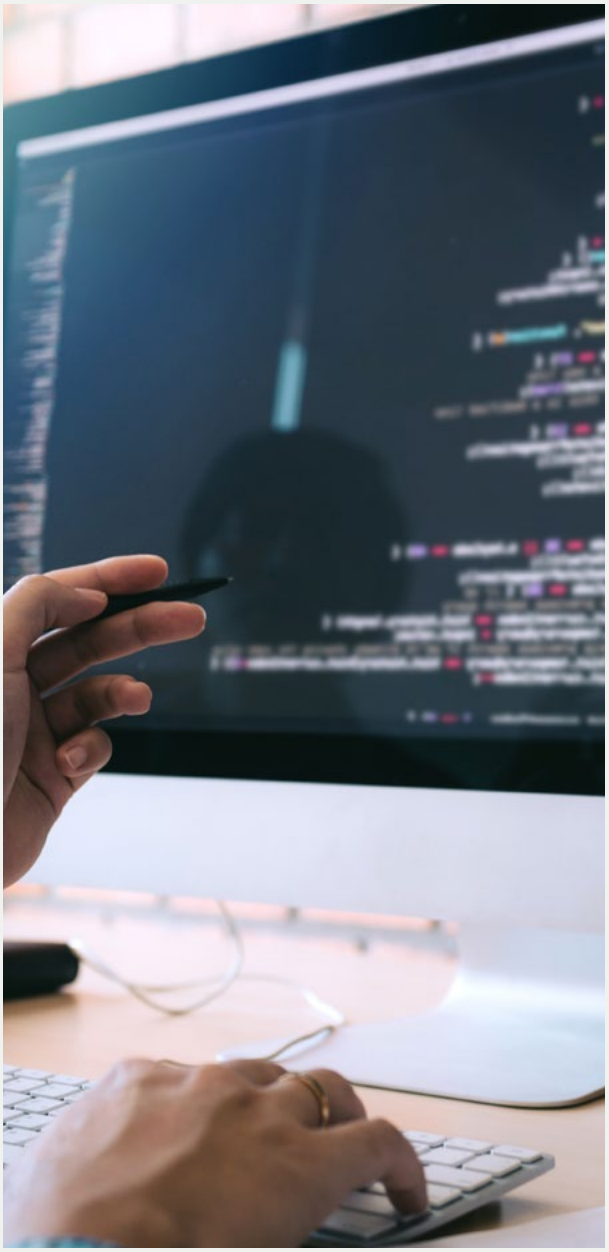
Invoice issues can challenge businesses, which must be able to detect if vendors accidentally or deliberately submitted duplicate copies of documents. Failure to catch such problems could lead to expensive overpayments. ULG adopted an ERP system that both prevents vendors from uploading copies of invoices they have already submitted and keeps internal staff from entering duplicates.

"With our new ERP system, ... we have controls in place to prevent duplicate vendor invoices from being entered in our system," Tornell said.

The ERP system also compares invoices against the purchase orders it had generated. Those that match exactly can be paid whereas those with discrepancies are flagged for further review and approval. Handling approval processes through an ERP system rather than back-and-forth emails can also help streamline the process, she said.

Accurately and securely handling a high volume of independent contractor invoices and payouts is critical to the growth plans of international businesses like language services providers. The rising rates of fraud attempts make this work challenging, but automated systems and clear policies and procedures can help minimize confusions and stamp out schemes.

NEWS & TRENDS



Security and fraud

THE IMPORTANCE OF LEAVING SPACE IN THE BUDGET FOR AP SECURITY, PERSONNEL

The COVID-19 pandemic is overturning standard business operations and companies are moving quickly as they attempt to reestablish normalcy. Businesses that have watched long-time suppliers close during the economic downturn may be eager to quickly onboard others to fill those gaps, for example, but those making such moves must still proceed carefully, Ben Kaye-Smith, senior vice president of ethics risk and compliance at gene therapy development firm AveXis, said in a recent Q&A discussion. Some firms are eager to rapidly onboard to avoid going without suppliers for long, but Kaye-Smith explained that failing to thoroughly vet new partners can lead them to ally with third parties that have poor security practices, ultimately leading to greater fraud risks.

John Hanson, managing director at accounting and tax advisory company BDO, offered similar warnings during the discussion. Companies facing budgetary strains may consider laying off workers, consolidating positions or trimming investments in back-office operations, he said, but these actions could create fraud losses. Hanson explained that businesses

would be better protected if they maintained robust staffing levels that allowed them to continue implementing adequate internal controls and safeguards over aspects of operations like payments approvals. Companies should also continue to fund back-office systems that detect and respond to fraud.

HOW BUSINESSES CAN CONFRONT 'DUMMY COMPANY FRAUD'

Keeping any one staff member from obtaining too much control can be especially important as work-from-home arrangements create more opportunities for bad actors to take advantage of their companies. One financial forensics firm recently warned that some internal fraudsters are abusing access to their companies' enterprise resource planning (ERP) systems to create fake supplier accounts, for example. Fraudsters initiating these so-called "dummy company fraud" schemes enter their own bank account information as though they were vendors, then send themselves money under the guise of paying these purported suppliers. Unscrupulous employees could even create fake purchase orders and invoices to build out their cover stories.

Scammers who keep their purchase order values small enough to stay under certain transaction review thresholds are likelier to get away with their misdeeds, but there are ways for companies to curb such actions. Firms can establish strong oversight capabilities, restrict ERP system access and determine how much control users have, for example.

Business email compromise schemes

FIRMS COMBAT INTERNAL FRAUD AND BEC SCAMS DURING PANDEMIC

Companies often employ different approaches to prevent malicious AP staff members from perpetrating schemes. Not all firms have ERP systems, for example, and some companies that have stuck with legacy processes are now facing greater threats from one of the oldest payment methods around. Physical checks have remained central to many businesses' B2B transaction flows during the pandemic, even prompting some companies to send AP staff home with check printers, said Neal Anderson, CEO and president of AP and AR automation company OnPay Solutions. This arrangement can introduce fraud risks if some employees prove to be untrustworthy and abuse their in-home access to company funds, however.

Anderson said companies that have employees working from home face an even bigger threat from BEC scams. These attacks occur when fraudsters take over or spoof executives' email accounts to impersonate them and instruct AP professionals to make payments to fraudulent accounts. The confusions companies' unavoidably quick shifts to remote work have caused could make personnel more likely to fall for such scams, in part because they can no longer swiftly confirm payment requests directly with CFOs. Companies will therefore need to redouble efforts to train employees to recognize such schemes.

TREND MICRO REPORTS WIDESPREAD SPEAR-PHISHING ATTACK AGAINST CFOs, OTHER EXECUTIVES

Researchers at cybersecurity company Trend Micro recently reported that more than 1,000 companies around the world were targeted by one such scam. The firm said it had detected a spear-phishing scheme directed at executives' Microsoft Office 365 logins, with those in financial departments facing the brunt of the efforts. Fraudsters launching spear-phishing attacks attempt to compromise specific individuals rather than perpetrate wide-ranging schemes, and this tactic is often intended to trick targets into revealing sensitive information. The fraudsters Trend Micro uncovered had sent executives emails that supposedly contained voicemail links but ultimately led to a fake Office 365 site through which login details were stolen.

Cybercriminals who secure executives' information then typically use it to message lower-level staff, requesting that they pay fraudulent invoices that send funds to fraudsters rather than legitimate vendors. One fake invoice asked for nearly $1 million to be sent, though Trend Micro researchers did not reveal how many AP staff members fell for such claims or how much money actually was lost in these scams.

BEC ATTACKS INVOLVING INVOICE AND PAYMENTS FRAUD GROW 200 PERCENT BETWEEN APRIL AND MAY

More employees are beginning to catch on to fraudsters' BEC schemes, leading some bad actors to shift tactics and pretend to be existing vendors. Some of these criminals send emails to AP staff, requesting updates to payment details on file for the vendors they are impersonating, then arrange for money to be delivered into fraudulent bank accounts instead. Other scammers could send emails purporting to be from existing vendors, asking for payments for purchases that did not actually occur and containing fraudulent payment details for the alleged orders.

The number of invoice- and payment-related BEC attacks reportedly rose 200 percent from April to May. This spike occurs as bad actors seek to take advantage of disruptions the pandemic has caused, but companies are combating it with new policies. More secure practices could include requiring AP staff to call vendors or use live channels to confirm any payment requests or updates.

AP automation upgrades

75 PERCENT OF CFOs NEEDED TO MAKE SIGNIFICANT UPDATES TO ENABLE STAFF TO GO REMOTE

The quick shift to remote work during the pandemic's onset caught many companies off guard. A recently released survey of CFOs at 250 large and mid-sized businesses revealed that just 14 percent were capable of enabling their financial teams to work entirely from home by the time the pandemic hit. Another 75 percent of CFO respondents said they had to make major operational changes before financial staff could meet all their responsibilities remotely. Those that have since invested in such updates reported that both suppliers and clients have been more satisfied: 47 percent said the customer experience improved and 40 percent said the same about the vendor experience. These shifts have not eased all concerns, however. Seventy-seven percent of CFOs noted that their financial teams were worried about being adequately prepared for newly automated processes, illustrating that additional training could be an important component of AP upgrades.

35 PERCENT OF SMBs ARE REASSESSING THEIR PAYMENTS APPROACHES DUE TO THE PANDEMIC

Results from a survey published in early June show that SMBs are also eyeing AP updates. Digital payments ubiquity has represented a big shift for many SMBs as 44 percent said they

made most of their vendor payments via non-digital methods prior to the pandemic and 79 percent said they used paper checks some of the time. Many are shifting their priorities, however, with 35 percent saying the crisis has prompted them to reconsider their payment processing approaches.

A larger share of respondents said they felt "positive about transitioning to a digital payments system," which could indicate that interest in such technologies is growing even though not all businesses are ready to act. SMBs listed various reasons for valuing AP upgrades, with respondents highlighting savings, avoidance of payment errors and streamlined processes. Sixty-eight percent believed such updates would accelerate their AP processes, 43 percent said they would boost payments' accuracy and 37 percent expected to save money in the long run.

DESIRE FOR BETTER CASH FLOW INSIGHTS AND SECURITY PROMPTS AP MODERNIZATIONS

SMBs are not the only entities focused on using AP improvements to bolster their budgets. The economic downturn has introduced cash flow strains and AP tools that provide real-time data about payments' statuses can give organizations the information they need to act swiftly. AP automation could help corporate buyers pay fast enough to earn early payment discounts from their vendors, for example.

Modernized AP tools could also help businesses prevent fraud losses that might otherwise go undetected. Three-way invoice-matching solutions can help companies ensure that the details on their invoices match those on their purchase orders and the bills of receipts, for example, preventing overpayments due to errors or deliberate fraud. AP review tools can also help detect duplicate invoices, which can be especially painful now because many organizations' budgets are strained.

Faster payments

HOW VIRTUAL CARD TRANSACTIONS CAN EASE BUYERS' AND SUPPLIERS' BUDGET PRESSURES

Not all buyers wish to pay their vendors ahead of time as some would rather have cash on hand to handle surprise needs or take advantage of sudden opportunities. This desire for flexibility can run up against suppliers' needs to be paid quickly during the health crisis, however. Some buyers are aiming to please all parties by ditching paper checks and adopting virtual cards to handle their B2B payment flows. These digital transactions can rapidly settle in recipients' accounts without immediately removing money from buyers' coffers. The payers can thus wait until their bills are due to furnish any funds and can elect to only pay the minimum amount their card companies require rather than the full bill. Virtual cards can also offer cash back rewards.

US COMPANIES GAINING INTEREST IN ADOPTING REAL-TIME PAYMENTS

Businesses are also looking at other faster payment options. A survey of 252 decision-makers at U.S. companies found that all but 9 percent plan to use The Clearing House's RTP rail. Adopting this method enables funds to travel

instantly from buyers' bank accounts to recipients and associated payments data also moves instantly. Fifty-two percent of respondents said they wanted to use RTP to improve their cash flow management and 46 percent said it would help them "conduct general accounts payable activities." Others intend to use RTP to deliver employees' payments or replace their check use.

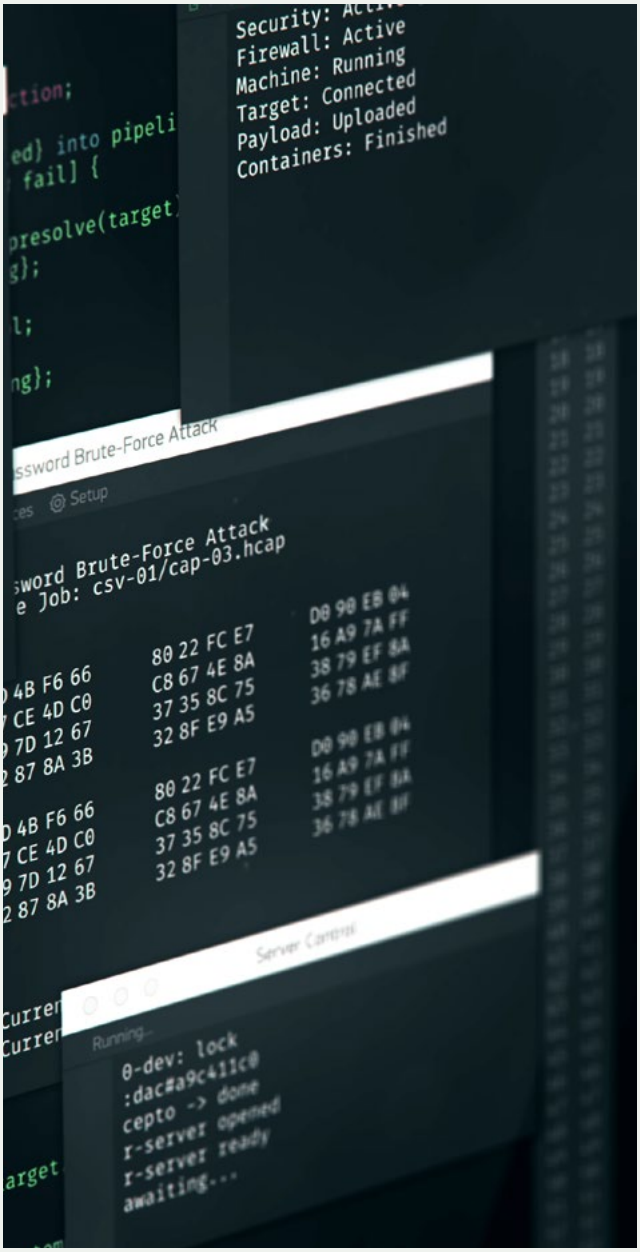
NACHA'S PHIXIUS PILOT PROGRAM GAINS NEW MEMBER

Delivering payment data quickly and easily can be important to making cash flows smoother and faster. Nacha — the organization that governs the automated clearing house (ACH) network — has been piloting a platform called Phixius that is intended to reduce such pains and streamline and secure B2B payments between multiple parties. Companies often find it difficult to exchange payments data between several entities and Nacha's solution aims to remove that friction for its participants. Organizations that connect with Phixius can access application programming interfaces (APIs) that allow them to share and manage data without storing it in a central location. The platform also offers automation supports and fraud-fighting services.

FASTER PAYMENTS COUNCIL WARNS ABOUT PREVENTING FRAUD FOLLOWING FASTER PAYMENTS

Adopting new payment methods can bring about novel concerns, however. Real-time payments' growing popularity could increase fraud risks if financial service providers are unable to act quickly, according to a new white paper from the U.S. FPC, a private sector group focused on tackling the nation's barriers to faster payments proliferation. Financial companies must be able to more quickly detect and respond to attacks in a payments environment where funds move at greater speed, Reed Luhtanen, the FPC's executive director, told PYMNTS. The FPC is reportedly working on tools to support this need.

DEEP DIVE



How CFOs Can Take Proactive Approaches To Cybersecurity

Corporations are up against steep cybersecurity challenges and CFOs have key roles to play in bringing their firms' fraud-fighting capabilities to the next level. Cyberthreats have long confronted businesses, but the pandemic-related disruptions have created even more opportunities for criminals to act.

This month's Deep Dive examines the state of such fraud threats and explores how CFOs are taking more proactive roles in combating them.

DATA BREACH LOSSES

Hackers are launching sophisticated attacks against organizations' data stores, and the reality of staff members working from home during the COVID-19 pandemic means that more companies than ever are relying on storing their data on the cloud. Putting information on the cloud may allow employees to access it remotely, but this also means criminals could gain remote access,.

Companies that are adopting new technologies to help operations run smoothly from home are also often dependent on third-party solution providers. Such businesses must ensure they have robust methods for vetting these solution providers, however, or else they could find themselves exposed to new risks. Any mistakes could be devastating as third-party data breaches can cost companies as much as $7.5 million. Other types of data breaches result in average losses of $4 million.

Pandemic-related challenges are only part of the puzzle. Fraud attempts were already on the rise before bad actors took the global crisis as a cue to put their efforts into overdrive. A 2019 survey of banks found that 60 percent said the quantity of fraud attacks made against them had risen, for example.

INVESTING IN DATA SECURITY

Some companies struggle to combat threats because they lack clear insights into the risks they face and the best practices for mitigating them. Another 2019 report surveying board directors found that only 24 percent were "highly familiar" with their organizations' data breach response plans while 10 percent knew nothing about them. This could be shifting, however, as companies realize the importance of tight cybersecurity.

A Q2 2019 global survey of 800 finance leaders found that 84 percent of CFOs and vice presidents of finance believed data privacy and security should be top priority. CFOs can play primary roles in helping their organizations budget and invest in tools, strategies and staff to help fend off cybercrime.

Companies are actively trying to get ahead of threats by spending more on cybersecurity, according to a recent survey of companies across corporate and retail banking, consumer and financial services, financial utility, insurance and service provider sectors. The study reported that those companies had invested 0.3 percent of their annual revenues, on average, into cybersecurity in 2019 — reflecting 10.1 percent of their total IT spending. These figures were upped to 0.5 percent of overall revenue and 10.9 percent of their IT expenses in 2020.

RISK ASSESSMENT AND FRAUD DETECTION

Boosting defenses will often require investing more staff time on these initiatives. Companies that aim to collaborate safely with third-party providers can direct employees to develop strategies for carefully vetting vendors prior to onboarding them, for example, and can hire more personnel with the expertise for conducting these provider reviews. This approach could lead to businesses implementing new, more robust procedures for assessing the extent to which prospective new partners may introduce risks and evaluating whether the benefits those providers pose are worth it.

Old-school, reactionary approaches to security hamper many organizations, which need new strategies. Companies have historically taken narrow, inflexible approaches to reducing risks in which they analyzed attacks to determine how they were conducted and then created new rules and approaches to block those specific kinds of attacks from happening again. This post-event analysis remains useful, but it can only go so far.

Firms that do not supplement this practice with other strategies can encounter threats from criminals who learn how to adjust their attacks just enough to avoid discovery. Businesses therefore should also set up methods to proactively detect ongoing attacks and thwart new attempts that may not match up exactly with known fraud threats.

ML AND AP PLATFORMS

Proactive approaches to recognize and foil threats could entail investing in machine learning (ML) tools. These intelligent technologies can help firms monitor their payment flows and pinpoint any that seem unusual and could indicate fraud. These tools can then send alerts to AP staff, prompting the investigation of suspicious activities.

AP management platforms can also provide businesses with clear oversight into the statuses of invoices and payments, granting workers the most up-to-date data. The platforms can also be programmed to send alerts should certain behaviors occur, such as changes to suppliers' payment details or receipt of unusually high-value invoices. Managers can then evaluate the situations to determine if fraud is at play.

Businesses need to investigate whether certain payments updates are legitimate requests from vendors or if fraudsters have sent them. Criminals can pretend to be existing vendors and send messages to trick AP staff into changing details on file so that money will be sent into fraudulent accounts. Managers can also check whether unscrupulous employees have tweaked especially high invoices. Such bad actors may try to inflate the value of payment requests so that they can skim extra off the top, meaning firms must confirm that pricey invoices are genuine.

The cybersecurity and fraud risks facing companies during the pandemic are likely to become more sophisticated as bad actors seek to take advantage of this year's disruptions. CFOs that invest now in the right strategies, personnel, ML tools and AP technologies can best protect their organizations and prepare for future threats.

ABOUT

PYMNTS.com

PYMNTS.com is where the best minds and the best content meet on the web to learn about "What's Next" in payments and commerce. Our interactive platform is reinventing the way in which companies in payments share relevant information about the initiatives that shape the future of this dynamic sector and make news. Our data and analytics team includes economists, data scientists and industry analysts who work with companies to measure and quantify the innovation that is at the cutting edge of this new world.

COMDATA

For over 50 years, Comdata has been a leading provider of innovative B2B payment and operating technology. By combining our unique capabilities in technology development, credit card issuing, transaction processing and network ownership, we help our clients build electronic payment programs that positively impact their bottom lines and operate their businesses more efficiently. We continuously evolve our products by focusing on our customers' needs to provide security, accessibility, and profitability.

As a division of FleetCor Technologies, Comdata is part of one of the largest payment companies in the world and is the second largest commercial issuer of Mastercard in North America.

We are interested in your feedback on this report. If you have questions or comments, or if you would like to subscribe to this report, please email us at **feedback@pymnts.com**.

DISCLAIMER

The CFO's Guide To Digitizing B2B Payments may be updated periodically. While reasonable efforts are made to keep the content accurate and up-to-date, PYMNTS.COM: MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, REGARDING THE CORRECTNESS, ACCURACY, COMPLETENESS, ADEQUACY, OR RELIABILITY OF OR THE USE OF OR RESULTS THAT MAY BE GENERATED FROM THE USE OF THE INFORMATION OR THAT THE CONTENT WILL SATISFY YOUR REQUIREMENTS OR EXPECTATIONS. THE CONTENT IS PROVIDED "AS IS" AND ON AN "AS AVAILABLE" BASIS. YOU EXPRESSLY AGREE THAT YOUR USE OF THE CONTENT IS AT YOUR SOLE RISK. PYMNTS.COM SHALL HAVE NO LIABILITY FOR ANY INTERRUPTIONS IN THE CONTENT THAT IS PROVIDED AND DISCLAIMS ALL WARRANTIES WITH REGARD TO THE CONTENT, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT AND TITLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES, AND, IN SUCH CASES, THE STATED EXCLUSIONS DO NOT APPLY. PYMNTS.COM RESERVES THE RIGHT AND SHOULD NOT BE LIABLE SHOULD IT EXERCISE ITS RIGHT TO MODIFY, INTERRUPT, OR DISCONTINUE THE AVAILABILITY OF THE CONTENT OR ANY COMPONENT OF IT WITH OR WITHOUT NOTICE.

PYMNTS.COM SHALL NOT BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND, IN PARTICULAR, SHALL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE, OR LOSS OF USE, ARISING OUT OF OR RELATED TO THE CONTENT, WHETHER SUCH DAMAGES ARISE IN CONTRACT, NEGLIGENCE, TORT, UNDER STATUTE, IN EQUITY, AT LAW, OR OTHERWISE, EVEN IF PYMNTS.COM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME JURISDICTIONS DO NOT ALLOW FOR THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, AND IN SUCH CASES SOME OF THE ABOVE LIMITATIONS DO NOT APPLY. THE ABOVE DISCLAIMERS AND LIMITATIONS ARE PROVIDED BY PYMNTS.COM AND ITS PARENTS, AFFILIATED AND RELATED COMPANIES, CONTRACTORS, AND SPONSORS, AND EACH OF ITS RESPECTIVE DIRECTORS, OFFICERS, MEMBERS, EMPLOYEES, AGENTS, CONTENT COMPONENT PROVIDERS, LICENSORS, AND ADVISERS.