PYMNTS.com

# SECURING B2B PAYMENTS REPORT

SEPTEMBER 2019

PYMNTS.com

# SECURING B2B PAYMENTS REPORT

## Acknowledgment

The Securing B2B Payments Report is done in collaboration with American Express, 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

**No business can go it alone in today's interconnected environment. From large software firms to small-scale mom-and-pop operations, companies rely on timely product and payment deliveries from other businesses to keep their doors open.**

These transfers are made to inventory providers, utility operations like electricity and gas, full- and part-time employees or contractors and delivery services suppliers, to name just a few. Such partnerships are essential to ensuring store shelves are stocked, the lights stay on and that employees are paid for their shifts.

Relying on a system of partnerships comes with challenges, however. It is vital that business-to-business (B2B) payments are made in a quick and friction-free manner, especially for those that depend on other firms for supplies and resources. The fallout from a missing or delayed B2B payment can be severe for both parties, resulting in fines, harmed supplier relationships and supply chain issues. Left unaddressed, these problems can cause significant harm to a company's reputation.

Delayed B2B payments also tend to have a ripple effect on cash flows. A recent study of 3,000 small business owners around the world found 61 percent of small and medium-sized businesses (SMBs) face cash flow issues. The result is that these companies often struggle to pay their bills.

Fortunately, modern payment innovations like portals, same-day ACH, automated accounts receivable (AR) and credit cards are being developed to help firms more easily complete B2B transactions. Many are enabled by FinTech providers that can quickly develop solutions and bring new offerings to market, and their rise could cause paper checks and other legacy offerings to lose their appeal.

The **Securing B2B Payments Report, a PYMNTS and American Express collaboration**, follows the latest developments in the B2B payments space. The report highlights the latest innovations and new solutions that could disrupt long-established B2B payment practices, reduce payment fraud and enhance data security.

The report includes a breakdown of the developments and solutions designed to help businesses quickly and securely make payments to their partners and protect against fraud.

## AROUND THE B2B PAYMENTS SPACE

Consulting firm CGI and invoice payment solutions provider Ordo recently announced a collaboration to make invoice processing more efficient and secure for both sides of a transaction. The tool will integrate end-to-end encryption to protect sensitive information, prevent push payment fraud and enable billers to accept partial payments or defer payments, thus avoiding being charged late fees or incurring other penalties.

Another partnership looks to help corporates fight fraud. Identity verification solutions provider GIACT Systems has announced it will collaborate with data analytics firm Equifax to launch its EPIC Platform from GIACT. The product uses Equifax's technology to analyze customer identity and behavioral data to better assess fraud risks.

# Executive INSIGHT

**What are some of the emerging types of B2B payments fraud? How can businesses better protect themselves?**

"We see fraudsters attempting to exploit many aspects of the B2B payments ecosystem, ranging from account takeover fraud to creating entirely fake businesses. Businesses need multifaceted fraud prevention strategies to combat the ever-evolving threats that can allow bad actors to trigger and route fraudulent payments.

To help combat fraud in the B2B space, we advise businesses to incorporate a combination of intelligent, nimble controls across all payment touchpoints to help provide robust fraud protection and educating employees to better identify attempted fraudulent activities. American Express continuously invests in B2B fraud prevention solutions, which leverage the most advanced machine learning models, enhanced merchant data gathering, bank account intelligence and sophisticated customer authentication strategies. [The goal] is to minimize fraud across B2B channels and products, while [also] minimizing disruption to customers' experiences."

**PAUL FERTIG,**

director of fraud risk management at
American Express

The real estate market also recently saw innovations, with property management platform InventoryBase adding a Workstreams feature for B2B clients that enables managers to submit inspection jobs, select vendors and pay suppliers through the platform. Suppliers can integrate with the platform using an application programming interface (API) that connects to their back-office solutions.

Learn more about the latest efforts to keep B2B payments secure in the Report's News and Trends section (p. 12).

## ADDING VIRTUAL CARDS TO THE CONSTRUCTION TOOLKIT

The U.S. construction market is on track to reach $1.8 trillion by 2023. Construction firms looking to remain successful need to demonstrate profitability by completing projects on time, but this requires reliable cash flows that enable businesses to quickly pay suppliers and vendors. For this Tracker's Feature Story (p. 8), Karin Rush, leader of shared services for DPR Construction, and Linnet Phoenix, DPR's head of corporate accounts payable (AP), discuss how the company's use of virtual and purchasing cards is bringing greater efficiency and security to the construction market.

## DEEP DIVE: USING AI TO FIGHT FRAUD

Keeping companies safe from fraud is becoming increasingly important as bad actors grow not only more brazen in their efforts, but also more successful. The global economy incurred $4.2 trillion in fraud-related losses last year alone, but artificial intelligence (AI) is poised to play a larger role in keeping businesses' and banks' B2B payments safe. The Securing B2B Payments Report includes a Deep Dive (p. 17) highlighting AI's capabilities and what firms need to know about using the technology wisely.

# FIVE FAST FACTS

**$4.2T**

Estimated value of global financial losses reported in 2018

**$1B**

Estimated value of the global anti-money laundering software market in 2018

**55%**

Portion of corporate professionals who identified real-time payments as their top B2B payments service priority

**1,100**

Number of business email compromise fraud scams that targeted CEOs in 2018

**60%**

Share of RegTech firms that focused on solving AML and KYC issues from 2014 to 2018

# FEATURE STORY

# Building Vendor Trust With Virtual Cards

The U.S. construction market is on a roll, and recent data suggests it is unlikely to slow. The market is on track to record a compound annual growth rate (CAGR) of 4.9 percent from 2019 to 2023, reaching a value of $1.8 trillion. Construction firms looking to succeed in this growing market and turn a profit must complete their projects on time, which means access to steady cash flows is crucial. Businesses that fail to make payments to suppliers or vendors in a timely fashion risk alienating partners and stalling projects.

Having the right payment tools is therefore as important as having the right trucks, saws and jackhammers. Such solutions help construction firms resolve balances while providing their business partners with crucial access to working capital. This is why some construction firms — such as Redwood City, California-based DPR Construction, which has two dozen offices in the U.S. and divisions in the Netherlands, Singapore and South Korea — have embraced offerings like virtual and purchasing cards that expedite the payment workflow.

DPR works with a vast network of subcontractors, suppliers and vendors, and making on-time payments is essential to maintaining strong relationships with these partners and keeping projects on track. PYMNTS recently spoke with Karin Rush, DPR's leader of shared services, and Linnet Phoenix, head of corporate AP, to better understand how virtual and purchasing cards can build efficiencies in the construction market. The pair explained how these offerings keep suppliers satisfied and DPR's partners safe from fraud.

"Virtual cards move payments quickly," Phoenix said. "We can email a remittance advice to the vendor and they will have all the information to easily reconcile payments on their system."

## MAKING VIRTUAL CARDS A REALITY

DPR's vendors are presented with the option to receive payment via virtual cards once they complete the onboarding process. Approximately 30 percent to 40 percent of the company's vendors opt in, proving the feature's popularity.

"Checks take longer to reach vendors," Phoenix said. "With the virtual card, they receive an email that includes all the data they need to post the payment."

DPR has used virtual cards for five years, and their faster delivery mechanisms are likely to fuel greater uptake within the construction market.

"It's probably the direction [that] vendors are going in," she said. "Every time we have a new vendor, we send them the package and they have the option to choose … virtual cards or not. Most of them sign up."

## FIXING CASH FLOWS AND FIGHTING FRAUD

DPR works with more than 3,800 subcontractors and over 4,800 suppliers and vendors, all of which have their own payment needs and expect to get paid as quickly as possible. According to Rush, meeting these payment expectations is essential to helping them manage their cash flows.

Many subcontractors hire additional laborers who need to get paid weekly, creating problems when legacy payment methods, such as paper invoices and checks sent by mail, are used to settle payments within the established terms of the invoice.

"If we're late, then they're out even more cash on the front end," Rush said. "That definitely hurts the subcontractor relationship because [it] needs that cash to keep [its] business running."

Phoenix noted that virtual cards not only improve cash flows, but also reduce fraud vulnerabilities. The cards do not require vendors to share their banking details with DPR, meaning that information is not vulnerable to compromise. In addition, virtual card numbers can be used only once before they expire.

"It's for a particular vendor for a particular invoice," Phoenix said. "Once it has been used, it cannot be used again."

Vendors that successfully process their virtual card payments are sent remittance advice notifications that include invoice details such as payment amount, purchase order and date.

These solutions have helped DPR better understand how much capital it has on hand. Having better insight into the company's cash flow presents new opportunities for savings, such as reduced spending on expedited deliveries.

"It reduced our FedEx expenses because if we needed to get an urgent payment out to a vendor, sometimes we [would] have to overnight the checks," Phoenix said.

Rush echoed the sentiment that virtual cards provide a win-win for both DPR and its network of suppliers.

"[Our cash flow] is more predictable," Rush said. "We know when payments are received because they're gone when

we send them. For suppliers, they get their money faster. It's faster than ACH."

## PUTTING CARDS TO WORK

Virtual card technology is not the only card-based solution DPR uses to streamline operations and maintain a steady cash flow. The company also issues purchasing cards that enable DPR's staff who work at different construction sites to more easily make work-related purchases.

"These are for small … purchases," Phoenix said. "If one of the job's team members has to pick up an item at Home Depot, it's easy for them to go in, pick up and pay for the item right then and there, instead of creating a charge on an account or an invoice."

These tools also help workers on the company's back end, as DPR's AP department does not have to review invoices for expenses.

"Accounts payable is able to focus on other areas and the jobs team is able to have [the items] they need immediately," Phoenix said.

Such solutions enable DPR's staff to focus on their own tasks in the field. The global nature of the company's operations requires many staff members to travel to new cities and job sites, Rush noted. Purchasing cards enable all of the company's professionals — including temporary workers or employees assigned to field-based roles — to pay for a variety of travel-related expenses.

"They can use their [purchasing] cards to pay for plane tickets or meals, incidental things of that nature," Rush said. "It makes [things] easier because they don't have to use their personal cards."

Such offerings are essential for the construction market to maintain its momentum, and the right payment solutions could prove to be as valuable as any tool in a construction worker's toolbox.

# NEWS & TRENDS

# Fighting B2B payment fraud

## HOW FALSE POSITIVES COMPLICATE THE B2B PAYMENTS FRAUD FIGHT

AP and AR departments are on the front lines when protecting companies from fraudulent activity. These divisions are charged with monitoring financial transactions and stopping any activity that is deemed suspicious. An unintended downside is an increase in false positive transactions, however. False positives occur when honest transactions are marked as suspicious, resulting in legitimate orders being declined due to fraud-related fears.

Recent research for PYMNTS' Payments 2022 Playbook found 60.8 percent of digital platforms say false positives are a major payment friction point, and more than 30 percent identified them as their top challenge. They often result in declined corporate card transactions and delayed invoice processing, which can lead to payment delays that ultimately harm buyer-supplier relationships.

## INVENTORYBASE ADDS B2B PAYMENTS TOOL FOR PROPERTY MANAGEMENT

Real estate property management platform InventoryBase has added a new Workstreams B2B payment feature for its clients. The service allows property managers to find and pay third-party property inspectors by submitting jobs to the platform and receiving bids from interested vendors. Contractors perform their duties and submit their inspection reports after being chosen and accepting the tasks, and property managers can then review the reports and pay their suppliers. Suppliers can integrate the InventoryBase platform with an API that connects to their back-office systems.

## BENTO FOR BUSINESS DEBUTS NEW PAYMENT SERVICE

A new solution released by expense card solutions provider Bento for Business is helping business owners transition from making payments via paper checks. Its Bento Pay solution became available this month, enabling them to both make and receive payments using personal identifiers such as email addresses. Vendors can select how they prefer to be reimbursed, choosing ACH payments delivered to their checking accounts or having payments loaded onto virtual cards, for example.

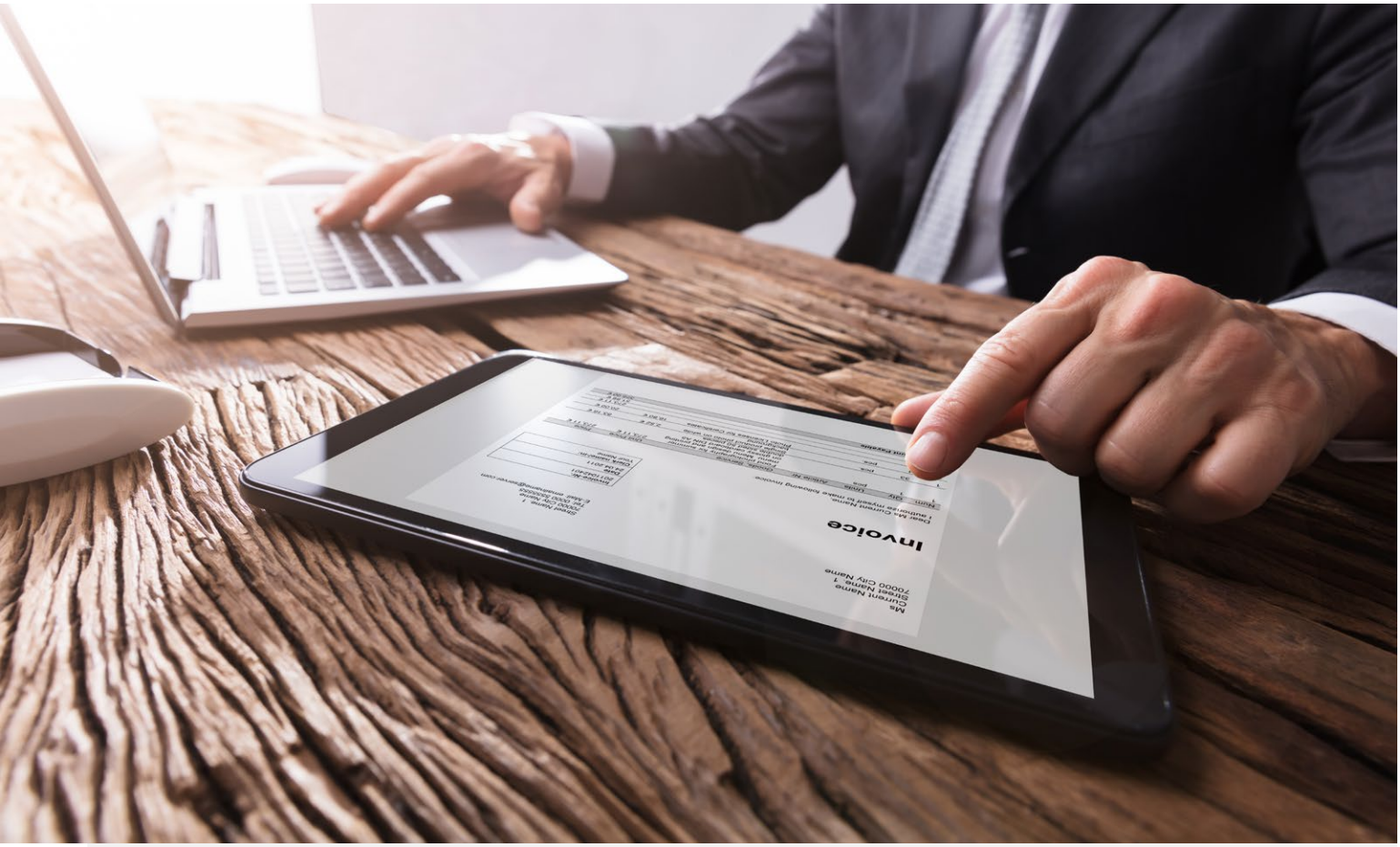
Bento for Business anticipates the U.S. small business market will reach $9 trillion by 2020, but notes that 80 percent of SMBs still use paper checks to make payments. The company has said new payment solutions could improve B2B payments' speeds. This would fit with the goals of many corporate professionals, 55 percent of whom identified real-time payments as their top B2B payment service priority.

## AMEX ACQUIRES ACOMPAY PLATFORM

A recent acquisition could add new automated solutions to American Express' portfolio. The financial services firm recently acquired automated digital payment platform acompay from ACOM Solutions Inc., which can integrate with enterprise resource planning and accounting systems to support check, ACH and card-based payments. The integration enables business clients to more easily make payments to suppliers and partners through automation, oversee spend management tasks, monitor cash flow demands and screen potentially fraudulent transactions.

In a press release, Amex said the acompay acquisition will help support several of its existing products, including EZPay Suite, EZConnect, EZ Content Manager and Document Management, among others.




### BEC SCAMS NEARLY DOUBLE OVER THREE YEARS

The U.S. federal government is warning companies to remain vigilant against a certain type of email-based fraud. Business email compromise (BEC) fraud scams — phishing attacks that target specific individuals at companies or organizations and can involve impersonating CEOs or other high-ranking company officials — are on the rise, perpetrated with the goal of tricking recipients into diverting fund transfers. In a recent report, the Financial Crimes Enforcement Network (FinCEN) noted the number of BEC incidents increased to 1,100 in 2018, more than double the 500 reported in 2016. It also reported that the cost of attempted BEC attacks jumped from $110 million per month in 2016 to $301 million per month last year, and that certain markets — like manufacturing, construction and real estate — are targeted more frequently than others.

## Improving invoice processing

### ORDO, CGI COLLABORATE TO COMBAT INVOICE PAYMENTS FRAUD

Business consulting firm CGI and invoice payment solutions provider Ordo have announced a partnership to make processing more efficient and secure. The latter's solutions enable billers to immediately receive funds when they submit electronic invoices, rather than using paper invoices. The new product will allow billers to accept partial payments or defer payments to avoid being hit by late fees or penalties.

Fraud and security are key collaboration components, the companies said, and the new platform will integrate

end-to-end encryption to protect sensitive information and prevent push payment fraud when sending or receiving funds.

### IBM LAUNCHES TRUST YOUR SUPPLIER SOLUTION

Tech giant IBM launched a new blockchain-powered solution aimed at helping businesses to keep their supply chains fraud-free. The new solution, known as Trust Your Supplier, works by automatically generating a vendor profile, a feature referred to as a passport for vendor identity by IBM. The data is stored on the blockchain platform and enables suppliers and authorized buyers to exchange data on the network. IBM said the solution, which was developed in partnership with blockchain firm Chainyard, will help prevent companies from having to invest time and resources manually aggregating vendor data and verifying their supplier bases. IBM said it plans to deploy the Trust Your Supplier solution for its own supply chain and vendor management services, and that it plans to onboard approximately 4,000 North American suppliers in the coming months.

### PROTECTING AP FROM SMARTER, FASTER FRAUDSTERS

Many corporate treasurers and executives may be interested in using faster payment systems to quickly deliver funds, but they are not the only ones looking to tap into such transactions' potential. Fraudsters and other bad actors want to exploit companies' AP process vulnerabilities to take advantage of faster payment deliveries, allowing them to more quickly make off with fraudulently obtained funds.

Doug Cranston, vice president of product management at payment processing solutions provider Bottomline Technologies, recently told PYMNTS in an interview that fraudsters are getting smarter at understanding and exploiting payment, AP and settlement processes. Banks and providers can aid AP, treasury and other payment professionals by educating them about fraud trends, he pointed out, and by providing expertise and using advanced tools such as machine learning to help detect and deter fraudulent acts.

### GIACT UPS FRAUD GAME WITH DATA ANALYTICS

B2B payments players are actively taking steps to crack down on fraudulent activity as bad actors become cleverer. Data analytics and technology company Equifax recently announced it will work with identity verification solutions provider GIACT Systems to help joint corporate customers mitigate fraud risks. The pair has announced the launch of the EPIC Platform from GIACT, a new B2B product enabling businesses to address customer fraud risks throughout their client relationships.

EPIC Platform from GIACT uses Equifax technology to analyze customer identity and behavioral data, as well as support real-time enrollment, payment, identity management, compliance and mobile fraud prevention. The partnership will unlock important access to some of the most complete and unique data assets available in the market, according to GIACT co-founder and CEO Melissa Townsley.

## Global AML efforts

### SMALLER FIRMS LESS RELIANT ON TECH AS THEY FACE HIGHER AML LABOR COSTS

A recent LexisNexis Risk Solutions study has found that smaller companies that do not use technology to comply with anti-money laundering (AML) regulations typically pay more in labor expenses. It polled 143 decision-makers in several industries — including banks, insurance companies, investment firms and asset managers — across the U.S. and Canada about the costs of AML compliance.

Firms with less than $10 billion USD in total assets pay $1.5 million per year on AML compliance, according to the

findings, and smaller firms that used up to one technological solution spent $8.4 million per year on compliance, with $4.9 million (58 percent) going to labor costs. Larger firms spend more overall, but used two or three technological solutions to remain AML-compliant. As a result, labor costs for these firms represented 54 percent of total AML compliance spend. These concerns are fueling the global AML software market, which reached $1 billion last year.

## US SUES TO RECOVER DARK WEB PROFITS

The U.S. Justice Department is seeking to recover a substantial sum from the now-shuttered BTC-e cryptocurrency exchange. It filed a civil lawsuit seeking $100 million, alleging that the exchange worked to help cybercriminals launder stolen money. Officials allege the funds were illegally obtained using ransomware, dark web marketplaces and hacked cryptocurrency exchanges.

The lawsuit seeks $88.5 million from BTC-e accounts and $12 million from Alexander Vinnik, the company's founder and CEO. Vinnik was arrested in Greece in 2017, and U.S. officials have since tried unsuccessfully to extradite him to face charges.

## FEDERAL AGENCIES OUTLINE RISK-BASED APPROACH TO AML COMPLIANCE

Other U.S. officials — including the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC) and the U.S. Department of the Treasury's FinCEN group — recently released a statement to clarify the agencies' risk-focused approach to studying how FIs are abiding by the Bank Secrecy Act/Anti-Money Laundering (BSA/AML) program. The statement did not include any new requirements, but instead emphasized that FI programs will be reviewed for their risk assessment capabilities that help determine individual risk profiles. Examiners may review additional information, such as testing and audits from previous analysis and measuring an FI's ability to identify, monitor and control risks. Increasing financial compliance regulation has resulted in a rise in the number of RegTech firms over the past five years. Sixty percent of them are focused on providing know your customer (KYC) and AML solutions.

# DEEP DIVE

# Using AI To Solve The $4.2T Fraud Problem

Digital payments volume is increasing as emerging technologies enable more seamless online transaction experiences for consumers and businesses. Cybercriminals are also seeing opportunities to use these offerings to their advantage, however, now employing them to exploit vulnerabilities, siphon funds and access valuable data.

Merchants and FIs have been turning to such solutions to help customers quickly and securely transact, but bad actors are doing so to rapidly commit financial crimes and get away undetected. The latter successfully made off with $4.2 trillion from the worldwide economy last year, a problem that will become only larger as transfer speeds increase.

Many organizations are thus tapping into advanced, unsupervised learning technologies — which provide opportunities to reduce financial fraud as detection becomes smarter and machine learning more powerful — like AI for assistance. The outlook for banks, businesses and consumers to remain protected could significantly improve with the systems' prevalence.

**The following Deep Dive examines how AI technology is being deployed on the anti-fraud front lines.**

## THE HIGH COSTS OF FRAUD

Fraud takes many shapes and forms and comes with a hefty price tag. The increasing risk of fraud is prompting many firms to implement AI-based solutions. These solutions can analyze consumers' personally identifiable information (PII) and transactional data, helping combat and identify irregular credit card activity for specific patterns — whether false positives or actual fraud. False positives occur regularly with traditional rule-based anti-fraud measures, as the systems tend to flag anything outside their given sets of parameters.

False positives are considered one of the most significant barriers to businesses' customer acquisition and retention efforts. A recent study found 60.8 percent of digital platforms consider false positives to be key conversion process friction points, a major problem for online companies. Their ranks include digital platforms such as Amazon Business and Airbnb, meaning they must deliver user experiences that are seamless, secure and allow trustworthy customers to quickly conduct transactions.

A firm attempting to make purchases from a new overseas supplier can trigger a fraud warning, for example, but AI solutions might compare it to a cluster of similar SMB accounts and further examine it before raising a flag. Digital platforms can thus create digital, data-based user profiles with AI-based systems in place, then determine if recent activity warrants cause for alarm. These solutions are likely to increase customer satisfaction and reduce the risk that banks will incorrectly flag genuine users' accounts.

## GETTING AI SECURITY RIGHT

False positives can undermine fraud detection systems' effectiveness, making it crucial that developers understand the importance of seamless, accurate data input processes. AI systems are only as effective as the input systems that support them, and should consider factors like geographic data and how it compares to traditional patterns, for example. Firms would do well to carefully analyze confirmed fraud alerts to understand how accurately their systems flag cybercrime-related events.

Banks and businesses would also be wise to take holistic approaches to fraud. Data collected by firms'

marketing divisions might include insights on the most popular channels — online, mobile or in-person — through which consumers choose to interact. This can lead to further opportunities to enhance security at these access points.

Fighting fraud requires several layers of protection to be effective in detecting bad actors while approving trustworthy partners. Merchants that deal with live customers can use chip-enabled point-of-sale (POS) terminals, an EMV-enabled technology that can keep payment card data secured at the POS and assure customers that their data will be protected.

Solutions like enhanced authorization for card-not-present transactions can share additional information like email addresses, IP addresses, shipping experiences and more to build more complete user profiles. Others, like EMV-3D Secure and tokenization services, are winning appeal by enabling merchants to shift liability and alleviate the need to store payment information. When combined with other measures, these tools have been proven to reduce fraud by approximately 60 percent.

AI will be essential in the fight against fraud, especially as bad actors become savvier in their digital crime efforts. The technology must be taught how to correctly collect and interpret data to be effective, though. Such solutions are only as effective as their users and developers teach them to be.

# ABOUT

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 companies in payments share relevant information about the initiatives that make news and shape the future of this dynamic sector. Our data and analytics team includes economists, data scientists and industry analysts who work with companies to measure and quantify the innovations at the cutting edge of this new world.

American Express is a globally integrated payments company, providing customers with access to products, insights and experiences that enrich lives and build business success. Learn more at americanexpress.com, and connect with us on Facebook, Instagram, LinkedIn, Twitter, and YouTube.

Key links to products, services and corporate responsibility information: charge and credit cards, B2B supplier center, business credit cards, travel services, gift cards, prepaid cards, merchant services, Accertify, InAuth, corporate card, business travel, and corporate responsibility.

We are interested in your feedback on this report. If you have questions, comments or would like to subscribe to this report, please email us at B2BPayments@pymnts.com.

# DISCLAIMER

The Securing B2B Payments Report 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 LIMITATION`S 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.