The Payments 2022 Playbook: Building A High-Performing Payments Team For Fraud Detection edition, a PYMNTS and Stripe collaboration, aims to better understand digital platforms' strategic roadmaps for the next three years and the role payments will play in driving their agendas. To this end, PYMNTS surveyed 250 heads of payments representing various sizes and types of business-to-business (B2B) and business-to-consumer (B2C) digital platforms: B2C services marketplaces, B2B SaaS firms, B2C merchant marketplaces, B2C retailers and B2B platforms/utilities. This Playbook examines how platforms can optimize their teams to improve fraud detection.

stripe | PYMNTS.com

PAYMENTS 2022 PLAYBOOK

BUILDING A HIGH-PERFORMING PAYMENTS TEAM FOR FRAUD DETECTION

June 2019

TABLE OF CONTENTS

PAYMENTS 2022

BUILDING A HIGH-PERFORMING PAYMENTS TEAM FOR FRAUD DETECTION

stripe | PYMNTS.com

The Payments 2022 Playbook was done in collaboration with Stripe, 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.

INTRODUCTION

A customer hands his credit card to a cashier to pay for groceries at a local supermarket only to have it declined for unknown reasons. **The experience will likely pack a psychological sting, suggesting he doesn't have the funds needed to make the purchase.**

Having a credit card declined is a common experience, and an unjustified one in most cases. Research has shown that at least five legitimate purchases are prevented for every fraudulent charge that is blocked.[1] These false positives collectively cost companies billions in lost sales, and an incalculable amount in prospective customers' goodwill.[2]

Fraud and false positives represent particularly vexing challenges for digital platforms, however. Firms like homesharing marketplace Airbnb, eCommerce giant eBay and ridesharing behemoth Uber live and die by the seamless experiences they provide their users, and a wrongly declined credit card is all fickle consumers might need to look for alternative providers. These companies also rely on card-not-present transactions to a much greater extent than brick-and-mortar businesses, meaning they are also more vulnerable to real fraud and on the hook to refund fraud victims with chargebacks for disputed purchases.

PYMNTS has undertaken an intensive study examining both digital platforms' strategic roadmaps for the next three years and the role payments will play in driving those plans. Our research has shown these marketplaces have their sights set on growth, with 94 percent of them expecting to improve their market share in that timeframe.

In the Payments 2022 Playbook series, a Stripe collaboration, PYMNTS surveyed 250 heads of payments representing various sizes and types of digital platforms. These included business-to-business (B2B) platforms, software-as-a-service (SaaS) firms and utilities providers as well as business-to-consumer (B2C) merchant, retailer and service marketplaces. This edition will explore digital platforms' ambitions, the major roadblocks presented by poor fraud detection capabilities and how companies can build high-performing teams to tackle such challenges.

Dealing with fraud is not the sole province of digital platforms, of course, as banks and card issuers have their own protocols for accepting and rejecting purchases. Our research shows these marketplaces are deeply dissatisfied with their own internal fraud detection systems, though, with just 1.2 percent saying theirs are "extremely" effective. At the root of this dissatisfaction is the sense that current solutions are inept at assessing risks, and that payment systems do not appear to be doing well at separating legitimate customers from false positives.

It is no wonder that 32 percent of platforms consider false positives, sometimes referred to as "false declines," to be their top pain point, exceeding all others in the payment process. Sixty-one percent of them consider false positives to be key inhibitors to conversions, according to our research, and the average digital platform estimates that fraud-related costs amount to 2.2 percent of its annual revenues.

It may not be surprising that fraud detection already consumes a considerable portion of digital platforms' resources and will likely continue to do so based on their current plans. Payments teams average six to 10 members, and half of the firms that employ 11 to 25 expect to increase their teams' sizes over the next three years. Our study found 68.6 percent of all surveyed companies will task their expanded teams with improving fraud detection, and that more than half plan to outsource some of this work to third-party vendors. The latter will make digital platforms' fraud detection efforts only more taxing.

For all the resources platforms are mustering to better deal with fraud, our research finds that these efforts do not necessarily translate to better performance. Just 19.6 percent of the firms that spend 3 percent to 5 percent of their revenues on payment processing consider their fraud detection systems to be "very" effective. On the other hand, 40 percent of those that devote 1 percent to 2 percent of their revenues to payment processing feel their fraud systems are "very" effective.

Our research suggests digital platforms may be overlooking the essential value their payment processors can bring to their efforts to improve fraud detection, however. As the gateways for all their payments, processors are ideally positioned to determine legitimate and fraudulent transactions. The 36 percent of platforms that do have a high degree of confi-

[1] Matheson, R. Reducing false positives in credit card fraud detection. MIT News. 2018. http://news.mit.edu/2018/machine-learning-financial-credit-card-fraud-0920. Accessed June 2019.

[2] The truth about false positives' 3X factor. PYMNTS. 2015. https://www.pymnts.com/news/2015/the-truth-about-false-positives-3x-factor/. Accessed June 2019.

dence in their fraud detection systems recognize this, and they will prioritize expanding their processor relationships — to a considerably greater extent than their peers — as a key component of their growth strategies.

A crucial question is whether payment processors offer robust fraud detection tools powered by state-of-the-art artificial intelligence (AI) and machine learning (ML) technologies. Unsupervised learning technologies bring a real-time ability to learn and distinguish outlying patterns of suspicious user activity, and the most innovative financial institutions view AI as the optimal computational learning system in fighting fraud.[3] As such, they can not only cast much finer nets to snag fraudsters and let through valid customers, but also respond to the unique threats platforms might face and adjust risk thresholds based on companies' priorities.

It is not enough for a payment processor to pay lip service to advanced learning systems, though. These firms must offer solutions that are easily integrated into clients' enterprise resource planning systems and that can be readily adopted by internal payments teams. Platforms need high-performing teams with the right tools — and payment partners — to more effectively deal with fraud, rather than turning to ever-more complex and expanding payments operations.

KEY TAKEAWAYS FROM OUR RESEARCH INCLUDE:

MOST DIGITAL PLATFORMS PLAN TO EXPAND OVER THE NEXT THREE YEARS, **BUT THEY VIEW POOR FRAUD DETECTION AS A MAJOR GROWTH IMPEDIMENT.**

Ninety-four percent of platforms expect to grow by 2022, according to our research, and 25 percent of them expect to be much bigger than they are now. These platforms plan to branch out to new geographies and broaden their presence in digital channels like voice commerce. Most view their payment systems as vital to growth, but fraud-associated costs represent a substantial burden. They consume 2.2 percent of digital platforms' annual revenues on average, and just 1.2 percent of such companies consider their fraud systems to be "extremely" effective.

FALSE POSITIVES ARE AT THE HEART OF DIGITAL PLATFORMS' FRAUD SYSTEM CONCERNS, **WITH NEARLY ONE-THIRD OF THEM CONSIDERING SUCH ISSUES TO BE TOP OPERATIONAL PAIN POINTS.**

Our study found that 32 percent of platforms consider false positives to be major operational pain points, making them the single most-cited impediment. Moreover, 79.6 percent factor the costs of false positives into their fraud loss estimates to a far greater extent than actual fraud incidents. Just 62 percent of firms weigh cyberfraud as part of their fraud cost calculations.

LARGER TEAMS ALONE ARE **UNLIKELY TO IMPROVE FRAUD OUTCOMES.**

Digital platforms' payments teams average six to 10 members, and 40.8 percent of them plan to increase their teams' sizes. This is largely to address fraud issues, with 68.6 percent of platforms planning to assign new employees in this area. Companies with payments teams numbering 11 to 25 members are considerably more likely to consider false positives a major pain point than those with just three to five, though, at 60 percent versus 33.3 percent, respectively. This suggests that smaller, more nimble teams and effective systems to support fraud detection would be best positioned to address fraud-related issues — including false positives.

PLATFORMS THAT SUCCESSFULLY MANAGE FRAUD DETECTION WILL **PRIORITIZE BUILDING THEIR RELATIONSHIPS WITH PAYMENT PROCESSORS.**

The 36 percent that consider their fraud detection systems to be "very" or "extremely" effective will place greater emphasis on expanding their processor relationships and focus less on enlarging their teams, according to our findings. This is especially true compared to platforms that have struggled with fraud, and suggests that leveraging payment processors' capabilities may offer more productive paths toward improving fraud detection.

[3] The AI Innovation Playbook. PYMNTS.com. 2019. https://www.pymnts.com/study/ai-gap-study-june-2019/. Accessed June 2019.

CHECKLISTS

OPTIMIZING THE FRAUD FIGHT

How platforms can better manage fraud prevention and detection

- [ ] **MONITOR FALSE POSITIVES.**
  It is not enough for anti-fraud systems to block fraudulent activity. They must also be able to track cases in which users were wrongly declined.

- [ ] **STREAMLINE FRAUD DETECTION.**
  Payment processors are the gateways for all transactions, making them ideally positioned to detect fraud. Platforms must ensure that robust, sophisticated fraud detection is an integral component of their processors' services.

- [ ] **COLLECT AND SHARE FRAUD DATA WITH PAYMENT PARTNERS.**
  Each business and its vulnerabilities are unique. Platforms must review their risk rules, then collect and share relevant data with their processors to optimize anti-fraud efforts.

- [ ] **ASK MORE OF PAYMENT PROCESSORS.**
  Processors should make robust fraud detection with advanced ML technology — which is uniquely suited to respond to the dynamic nature of fraud threats — an integral part of their platforms.

- [ ] **HIRE WISELY.**
  New team members should work in concert with sophisticated fraud detection systems and focus on the vital task of tailoring fraud detection to their platforms' specific needs.

FRAUD DETECTION FOR PAYMENT PROCESSORS

A well-suited payment processor's fraud detection system should have the following features:

ADVANCED ML-CENTRIC OPERATIONS

Computer learning systems form the backbones of the most effective modern fraud detection systems.

A LARGE, GLOBAL NETWORK

Processors that handle myriad global transactions every day have vast customer data troves. As such, a new user on a platform will likely not be new to its processor.

DATA-RICH METRICS

Processors should be able to provide rich internal fraud metrics. This can help both keep bad actors out and aid in driving conversions and loyalty.

TECHNICAL ASSISTANCE

Processors should act as partners in operating sophisticated fraud systems, also offering assistance in dealing with chargebacks and other fraud-related issues.

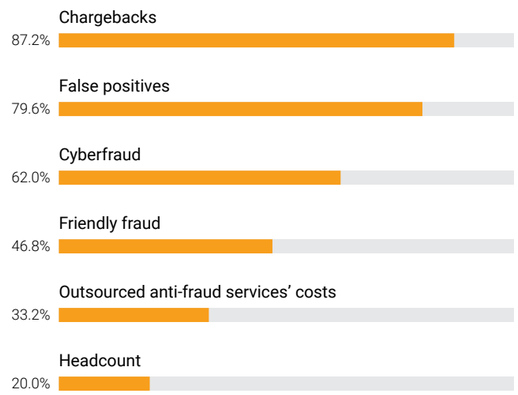
THE REAL — AND HIDDEN — COSTS OF FRAUD

Fighting fraud is a costly endeavor for digital platforms. Such online operations represent tempting targets for hackers, fraudsters and those who might unscrupulously seek refunds, sometimes referred to as "friendly fraud." Moreover, unlike brick-and-mortar retailers, online businesses are liable for the costs of chargebacks.[4]

Digital platforms therefore hold strong interest in ensuring their fraud detection systems are robust. Overzealous anti-fraud systems risk blocking too many prospective users at the door, however, and false positives are far more frequent than instances of actual fraud. As such, they may do far more damage to companies' bottom lines.

FIGURE 1:

Calculating fraud costs
Portion of firms that consider select factors when assessing overall fraud-related costs



79.6%
of digital platforms **factor in false positives** when calculating total fraud costs.

This all helps explain why fraud-related costs consume such large portions of digital platforms' budgets: an average of 2.2 percent of their annual revenues. The figure is even higher for those earning between $500 million and $1 billion annually, amounting to 2.8 percent, or $14 million to $28 million, of their annual revenues.

Our research confirms that false positives are the chief drivers of these costs. Digital platforms weigh false positives to a much greater extent than instances of actual fraud when estimating related losses, cited by 79.6 percent. Only chargebacks are factored in by more

[4] Messer, J. The economics of e-commerce chargeback fraud. eCommerceTimes. 2019. https://www.ecommercetimes.com/story/85763.html. Accessed June 2019.

firms — 87.2 percent, to be exact — to assess fraud costs. Platforms are also far more likely to weigh false positives than cyberfraud itself, which was mentioned by 62 percent.

The perceived gravity of false positives relates directly to their role in obstructing conversions. Our study found that 30.4 percent of platforms consider false positives to be top friction points in their payment processes, making them the most-cited hindrance. By comparison, fraud itself is considered a top friction point by only 16.4 percent, and 60.8 percent of all surveyed platforms consider false positives to be key conversion inhibitors.

The substantial soft costs associated with false positives help explain why platforms perceive them not just as frictions in payment processes, but also as challenges affecting them on an operational level. A surefire way to alienate prospective users is to wrongly decline their credit cards. Forty percent of platforms consider "declining legitimate customers" as a top operational pain point, according to our findings, second only to exceptions requiring manual intervention (44.4 percent). To put this in perspective, platforms consider false positives a greater operational challenge than getting new features to market on time (22.4 percent).

TABLE 1:

Top payments process friction factors

Share of firms that consider select issues to be friction points, by level of concern

	HIGH		LOW	
	1	2	3	TOTAL
Current chargeback/dispute resolution process	15.6%	22.4%	24.0%	**62.0%**
Number of false positives	30.4%	14.0%	16.4%	**60.8%**
Cost of fraud	16.4%	9.2%	13.6%	**39.2%**
Data security/tokenization	8.8%	9.2%	7.6%	**25.6%**
Customer authentication	6.4%	6.8%	7.2%	**20.4%**
Foreign exchange exposure	2.0%	8.0%	6.4%	**16.4%**
Merchant onboarding	4.8%	4.4%	5.2%	**14.4%**
Issuer declines	3.6%	4.0%	6.4%	**14.0%**
Regulatory compliance and monitoring	2.8%	7.2%	3.2%	**13.2%**
Third-party integrations	3.6%	3.2%	5.2%	**12.0%**
Too many providers	3.2%	6.4%	2.0%	**11.6%**
Unable to settle with merchants on chosen platform	2.4%	5.2%	2.8%	**10.4%**

TABLE 2:

Top payments operational pain points

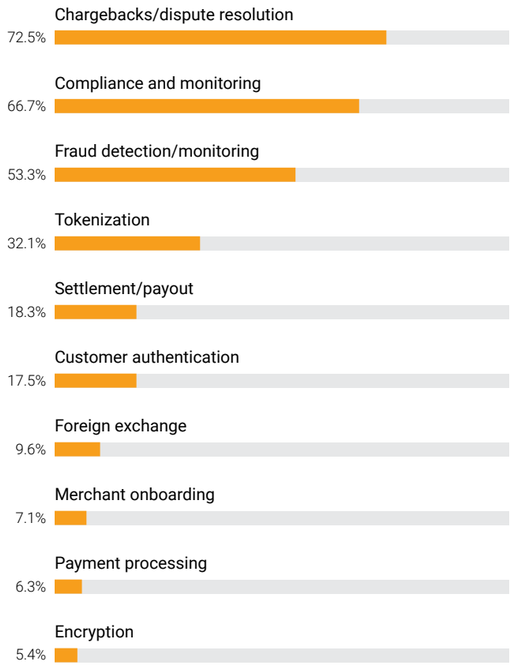
Portion of firms that consider select issues as pain points, by rank

	HIGH			LOW	
	1	2	3	4	TOTAL
Too many exceptions that require manual intervention	26.4%	14.4%	3.6%	0.0%	**44.4%**
Decline too many legitimate customers	32.0%	5.2%	1.6%	1.2%	**40.0%**
Reporting and reconciliation processes are cumbersome	14.0%	8.0%	1.2%	0.0%	**23.2%**
Takes too long to get new features into the market	9.6%	10.0%	2.0%	0.8%	**22.4%**
Checkout process is not optimized for seamlessness	8.0%	7.6%	1.2%	0.8%	**17.6%**
Can't settle transactions for merchants on our platform	3.2%	4.0%	0.4%	0.4%	**8.0%**
Too complicated to manage multiple vendor relationships	2.8%	3.2%	1.6%	0.0%	**7.6%**
Providers are unable to serve our needs	1.6%	2.0%	1.6%	0.0%	**5.2%**
Lose too much money to fraud	2.4%	1.2%	0.4%	0.0%	**4.0%**

THE MULTIFRONT FIGHT AGAINST FRAUD

FIGURE 2:

Areas in which platforms receive vendor support
Share of firms that rely on third parties for select assistance, by area



Fraud is a challenge for all modern businesses with eCommerce channels, but digital platforms are on the frontlines of this fight. The digital ecosystem's rise enabled platforms' extraordinary growth, but it has also made them uniquely vulnerable to both online fraud and detection systems that ensnare legitimate customers. Their large and growing global user bases mean digital platforms are potentially exposed to a much broader range of fraudulent schemes than traditional retail businesses. At the same time, it is incumbent upon digital platforms — more than other business types — to minimize conversion process frictions.

How have digital platforms been going about this fight? In a sense, they have been throwing everything they have at it.

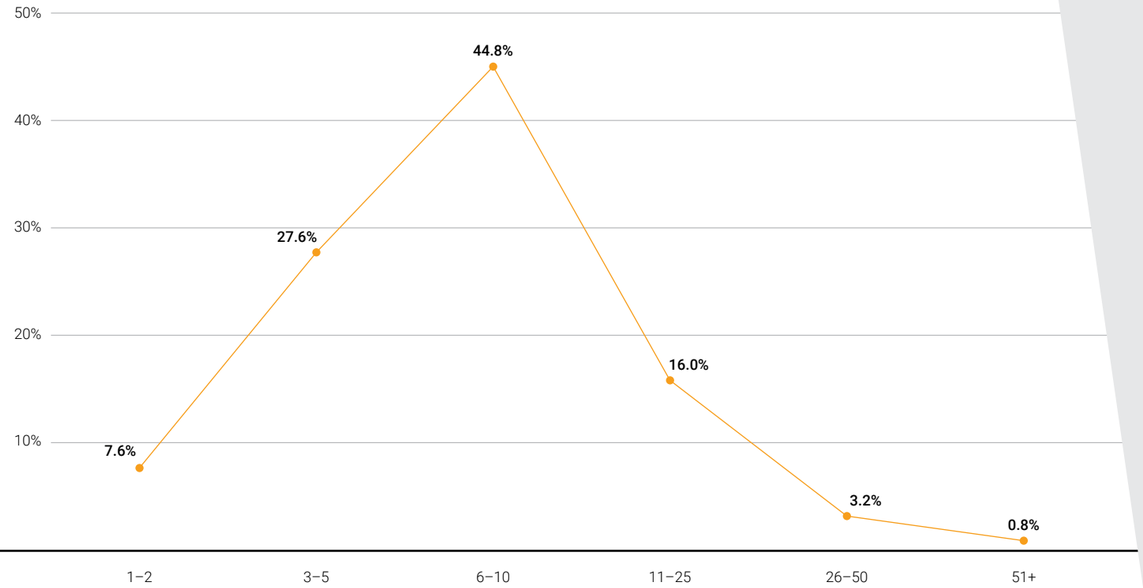
Platforms currently employ an average of six to 10 payments team members, have an average of 2.7 processing relationships that support six

53.3%
of digital platforms **rely on vendors** to provide fraud detection support.

FIGURE 3:

Size of payments teams

Portion of firms employing payments teams, by team size



payment methods and 80 percent of them have at least two vendor relationships to support the payment process. Our findings note that 53.3 percent of platforms look to third-party vendors for help with fraud detection and monitoring, far surpassing areas like foreign exchange (9.6 percent) and merchant onboarding (7.1 percent).

That digital platforms rely on vendors for help with elements like compliance — as 66.7 percent of them do — is understandable. They are eager to expand into new geographies, and learning the legal landscape in foreign jurisdictions may be outside their wheelhouses. In other respects, outsourcing may suggest such companies do not believe they are capable of managing complex operations in-house.

This would appear to be the case with fraud. Outside vendors will figure prominently in digital platforms' future growth plans and efforts to address it, according to our findings. Of the 25.6 percent that plan to expand their vendor relationships, 53.1 percent will do so to improve fraud detection — an area exceeded only by chargebacks and dispute resolution (62.5 percent).

Platforms appear to be making progress in chargebacks and compliance through in-house

FIGURE 4:

Areas in which platforms will seek vendor support

Share of firms that plan to seek help from third-party providers, by select firm areas

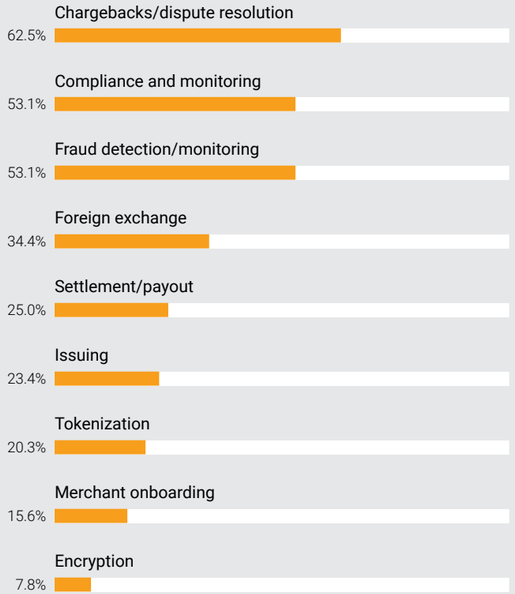
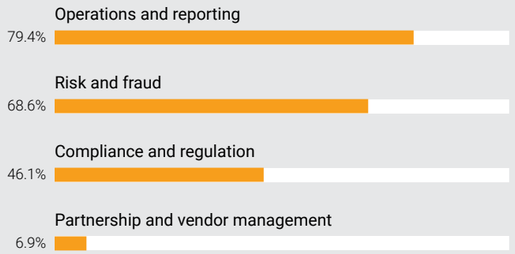


FIGURE 5:

Plans to increase team sizes

Portion of firms planning to add employees to bolster select areas, by firm area



systems, but this doesn't appear to be the case with fraud. The share that intends to outsource work in the former areas is projected to decline in the next three years, while fraud will hold steady at 53.1 percent. Outsourcing represents another substantial financial toll on platforms.

Marketplaces will also be increasing team sizes over the next three years, and new employees will be assigned to work on risk and fraud to a disproportionate degree. Our research shows that 68.6 percent of platforms intend to hire in this area, surpassed only by operations and reporting (79.4 percent).

There is no question that digital platforms view fraud detection as one of their largest challenges, and they are certainly expending considerable human and financial capital to address it. So, how are digital platforms doing? Not great, by their own estimations.

Our research suggests platforms are not making use of the most advanced tools available to detect and reduce fraud. These solutions should be at the center of their payment operations, not outsourced to a growing array of vendors. In short, strong fraud detection tools, powered by advanced ML technology, should be integral components of their processing platforms.

HOW MUCH BANG ARE DIGITAL PLATFORMS GETTING FROM THEIR FRAUD-FIGHTING BUCKS?

FIGURE 6:

Fraud systems' effectiveness
Share of firms that consider their fraud detection strategies to be effective, by level

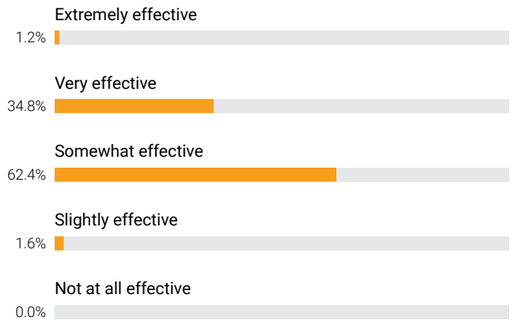
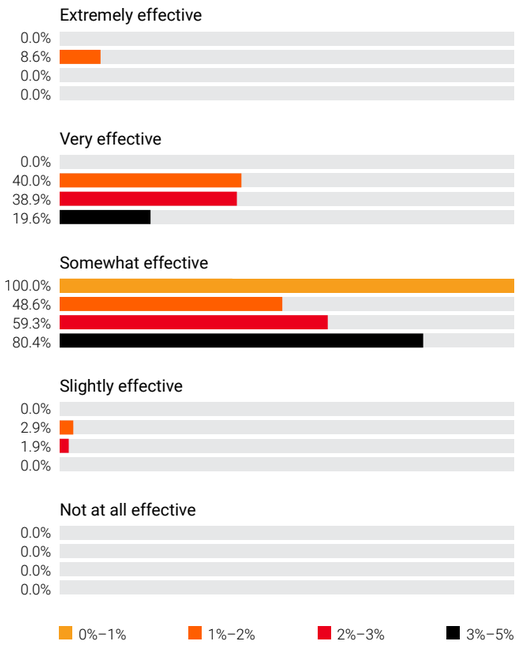


FIGURE 7:

Fraud systems' effectiveness
Portion of firms that boast "effective" fraud detection strategies, by share of revenues spent on payments



For all the resources platforms are bringing to the fraud fight, one inescapable conclusion has emerged: Very few of them believe their fraud detection systems work well.

Most companies consider their fraud-related efforts only "somewhat" effective at best, and a sliver (1.2 percent) consider them "extremely" so. The measures platforms have been taking to bolster their fraud operations — including outsourcing to vendors — have little effect on the overwhelmingly disenchanted view they have of their anti-fraud efficacy. In fact, the more resources platforms devote to their payment systems, the less likely they are to be satisfied with their fraud detection capabilities.

Generally speaking, the more funds a digital platform allocates to payment operations, the less likely it is to regard its fraud systems as effective. Forty percent of those that spend between 1 percent and 2 percent of their annual revenues on payment processing consider their related systems to be "very" effective, according to our research, while just 19.6 percent of the platforms that spend 3 percent to 5 percent of their revenues say the same. As an absolute dollar figure, the amount larger companies devote to their payment systems is, of course, going to be larger than that for smaller firms.

A similar pattern emerges when we examine staffing levels. For platforms with payments teams of 25 or fewer members, the larger the

staff, the less confidence firms seem to have in their fraud detection systems. Our findings show that 39.1 percent of those with three to five employees on their payments teams consider their systems to be "very" effective, as do 32.5 percent of those with 11 to 25.

Firms that invest more in certain areas can typically expect better results. Why does this logic appear to be turned on its head in the case of fraud detection? One possibility is that the companies that devote more staff and funding to their payment platforms are better equipped to detect false positives, and therefore more likely to appreciate the threats they pose. This thus colors the already-dim opinions they have of their fraud detection systems.

Platforms that factor false positives into their fraud costs are more likely to spend a greater share of their revenues on their payment operations, too. Our research shows 90.2 percent of those that spend 3 percent to 5 percent of their annual revenues on payment processing do so, as do only 50 percent of those that spend less than 1 percent.

Perhaps most telling is that the platforms that spend the greatest share of revenues on their payments systems are considerably more likely than the sample to judge their fraud detection as only "somewhat" effective. In fact, 80.4 percent of these firms have this lackluster view.

This should be alarming to companies that are not prioritizing false positive detection, whether by choice or due to budgetary constraints. Our research suggests that false positives may be exacting a far greater toll than companies realize — in the form of lost sales or goodwill — as firms cannot address problems they cannot see.

This underscores the conclusion that platforms must be more strategic about how they combat fraud. Throwing additional bodies at the problem and outsourcing have not proven effective, and the answer does not appear to be in having *larger* teams, but rather in employing *higher-performing* ones. Indeed, smaller, more nimble teams armed with effective tools and guidance from their payment processing partners may be better positioned to fight both fraud and its evil false positives twin.

FIGURE 8:

Fraud systems' effectiveness

Share of firms that consider their fraud detection strategies "very" effective, by payments team size

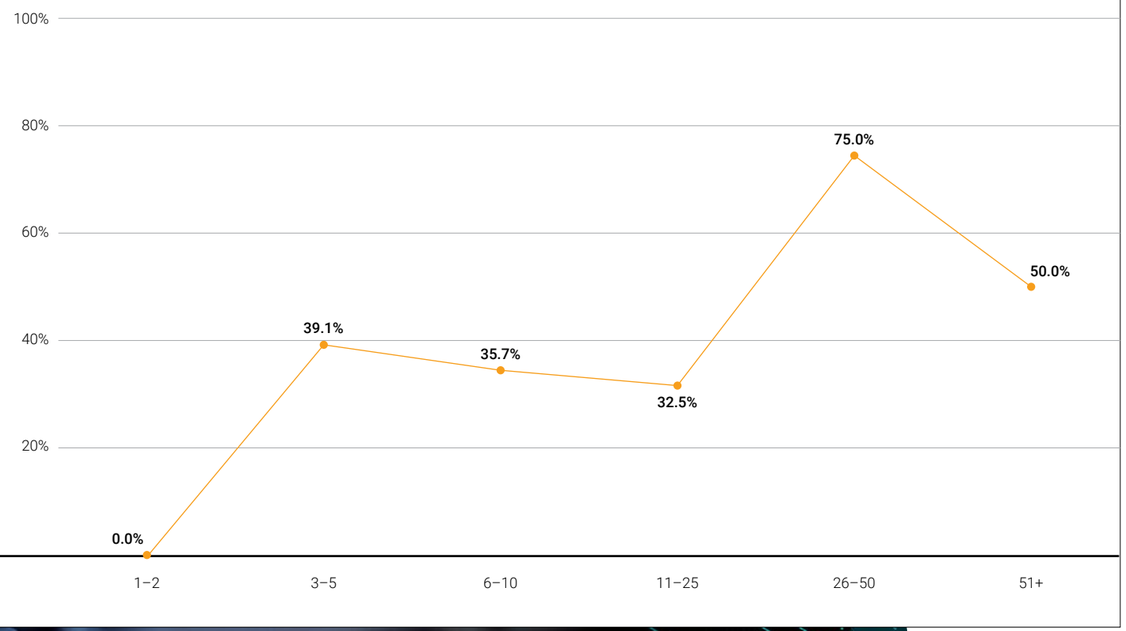
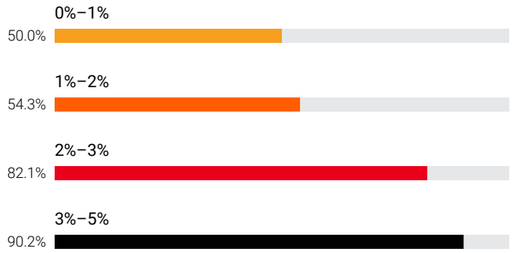


FIGURE 9:

Assessing false positives' costs

Share of firms factoring false positives into fraud costs, by revenue share devoted to payment processing



62.4%

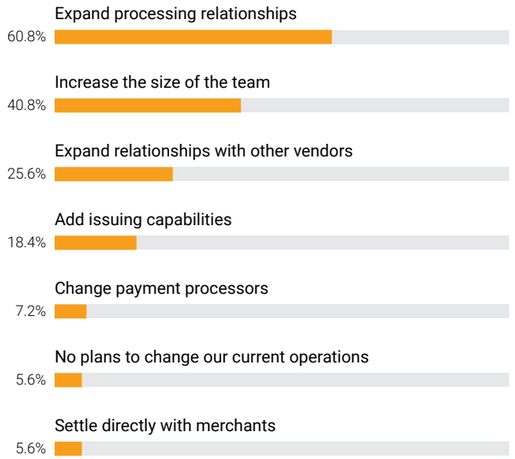
of platforms consider their fraud detection systems to be just **"somewhat" effective.**

A WAY FORWARD FOR FRAUD DETECTION

FIGURE 10:

How digital platforms plan to achieve their growth plans

Share of firms planning to invest in select areas to support their product roadmaps



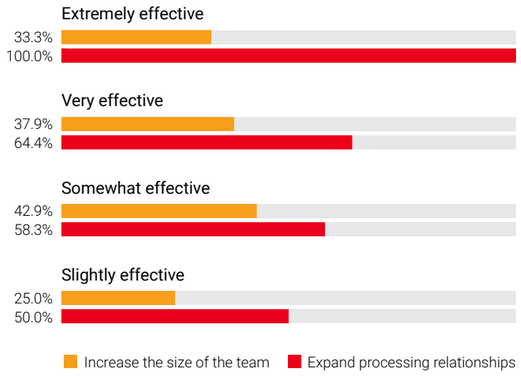
Our analysis found that fraud detection is one of the greatest barriers digital platforms face in working to gain market share and boost global presence. These firms view their performances here as mediocre at best, which is decidedly out of step with their ambitions. A few platforms consider their fraud detection systems "very" and even "extremely" effective, however, and offer insights into more effectively addressing the fraud dilemma.

Expanding processing relationships is at the center of most digital platforms' growth strategies. According to our research, 60.8 percent plan to do so, and to a greater degree than adding team members (40.8 percent) or boosting vendor relationships (25.6 percent).

60.8%
of all platforms
plan to build on their relationships
with their payment processors.

FIGURE 11:

Plans to expand processing relationships and teams
Share of firms planning to increase team sizes vs. expand processing relationships, by how they view their anti-fraud systems



100%
of platforms that consider their fraud detection efforts "extremely" effective **plan to expand their relationships** with their payment processors.

We also found that the growth strategies of the 36 percent of platforms that consider their fraud detection processes to be "very" (34.8 percent) or "extremely" effective (1.2 percent) center more on their processors and less on hiring. Our analysis noted that 64.4 percent of the platforms that are "very" satisfied with their anti-fraud systems will prioritize processing relationships, while only 37.9 percent will boost hiring. The contrast is even more dramatic among the handful of platforms that are "extremely" satisfied: 100 percent of them will expand processing relationships, and only 33.3 percent will focus on hiring.

Larger teams are not the answer for the minority of platforms that have made progress in dealing with fraud, though. They are instead prioritizing existing payment processor relationships, suggesting that leaner, nimbler teams aided by such strong relationships offer better routes for improving digital platforms' fraud detection efforts. This comes with the caveat that processors must be able to offer sophisticated fraud detection solutions that support team input and collaboration, which would likely not only be more effective in dealing with fraud, but also come at a much lower expense than hiring more employees or contractors.

CONCLUSION

Growth isn't a vague hope for many digital platforms, but rather an essential component of their business plans. These firms intend to further their ambitions by enhancing their payments teams and expanding their payment processor and outside vendor relationships over the next three years. Simply putting more employees and contractors to work is not enough to optimize conversions and address the vexing fraud detection problem, however.

Our research reveals that having large payments teams and budgets does not necessarily translate into more effective fraud detection, and that firms must also make sure they have the right payment partners at their sides as they forge ahead with ambitious growth plans. Platforms need high-performing teams aided by access to effective tools to see such progress, and may thus be better served by turning to payment processors that offer advanced, ML-based anti-fraud systems.

Having payment platforms capable of both seamless processing and effective fraud detection will be key in building these high-performing teams.

METHODOLOGY

For the Payments 2022 Study, we surveyed approximately 250 payments heads from digital payments platforms located both in the U.S. and abroad. Our survey was conducted during March 2019, and respondents hailed from five, distinct platform types, including the following:

- **B2B SaaS firms:**
  SaaS companies that sell services to businesses (e.g., Slack, Tableau, Greenhouse, GoDaddy).
- **B2B platforms/utilities:**
  Companies that provide web-based business services (e.g., Shopify, DocuSign, Squarespace).
- **B2C retailers:**
  Companies that sell consumers retail products through their own websites. They may also have physical stores (e.g., Apron, Warby Parker).
- **B2C merchant marketplaces:**
  Third-party companies that allow merchants to sell products and services to end customers (e.g., Etsy, eBay, Airbnb, HotelTonight).
- **B2C services marketplaces:**
  Third-party companies that allow service providers to sell services directly to end customers (e.g., Uber, Lyft, TaskRabbit, Fiverr).

We asked respondents a variety of questions designed to help gauge the state of their current payments operations, and the role they foresee those systems playing in supporting their future growth and expansion. Our assessment considered factors on a number of different payments methods and functions, including but not limited to chargeback/dispute resolution, FX management, voice-recognition capability and real-time payments functionality. We also considered additional factors, such as overall cost of operation, the number of each respondent's payments vendor/processor relationships and payments functionality according to geographic locale.

The majority of platforms in our sample operate primarily in the United States: 61 percent of companies we surveyed earn less than 40 percent of their annual revenue from non-U.S. customers.

The distribution of platforms in our survey sample was also balanced in terms of size, with their distribution representing companies in all revenue brackets. These included firms generating annual revenues ranging from $21 million to more than $1 billion.

DEMOGRAPHIC DATA	N	Percentage	INDUSTRY SEGMENT				
			B2C services marketplaces	B2B SaaS firms	B2C merchant marketplaces	B2C retailers	B2B platforms/utilities
N			46	50	55	53	46
Percentage			**18.4%**	**20.0%**	**22.0%**	**21.2%**	**18.4%**
Share of annual revenue derived from non-U.S. customers							
0%	64	**25.6%**	28.1%	6.3%	32.8%	28.1%	4.7%
1% - 20%	38	**15.2%**	23.7%	21.1%	13.2%	18.4%	23.7%
21% - 40%	51	**20.4%**	7.8%	37.3%	11.8%	23.5%	19.6%
41% - 60%	52	**20.8%**	9.6%	26.9%	19.2%	26.9%	17.3%
61% - 80%	34	**13.6%**	23.5%	14.7%	26.5%	5.9%	29.4%
81% - 99%	3	**1.2%**	33.3%	0.0%	0.0%	0.0%	66.7%
100%	8	**3.2%**	12.5%	0.0%	50.0%	0.0%	37.5%
Annual revenue							
$21M - $50M	59	**23.6%**	16.9%	20.3%	15.3%	25.4%	22.0%
$50M - $100M	58	**23.2%**	24.1%	20.7%	13.8%	25.9%	15.5%
$100M - $500M	62	**24.8%**	16.1%	29.0%	22.6%	14.5%	17.7%
$500M - $1B	28	**11.2%**	28.6%	14.3%	7.1%	21.4%	28.6%
$1B +	43	**17.2%**	9.3%	9.3%	51.2%	18.6%	11.6%
Number of people in payment processing operations							
1 - 2	19	**7.6%**	10.5%	26.3%	15.8%	26.3%	21.1%
3 - 5	69	**27.6%**	18.8%	11.6%	29.0%	27.5%	13.0%
6 - 10	112	**44.8%**	21.4%	25.0%	11.6%	17.9%	24.1%
11 - 25	40	**16.0%**	17.5%	20.0%	40.0%	12.5%	10.0%
26 - 50	8	**3.2%**	0.0%	12.5%	25.0%	37.5%	25.0%
51+	2	**0.8%**	0.0%	0.0%	50.0%	50.0%	0.0%

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.

stripe

Stripe is a set of tools for building and running an internet business. We help businesses accept payments from anyone, anywhere, and build new kinds of companies like Lyft or Kickstarter. Internally, we say our goal is to increase the GDP of the internet — we want to bring more businesses online worldwide.

In everything we do, we put our users first. We work hard to build the cleanest, most robust APIs possible so that our users can focus on building great products. There's always something more we can do — we're constantly seeking out areas of our product we can improve.

We are interested in your feedback on this report.
Please send thoughts, comments, suggestions or questions to payments2022@pymnts.com.

PAYMENTS 2022 STUDY:
How plateforms will use payments to transform global economics