A Forrester Consulting
Thought Leadership Paper
Commissioned By Visa

July 2019

Understanding The Evolving Payments Landscape

Emerging Fraud Trends And Key Strategic Implications

FORRESTER®

Table Of Contents

Project Director:
Ana Brzezinska,
Market Impact Consultant

Contributing Research:
Forrester's Infrastructure & Operations research group

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

FORRESTER®

Executive Summary

Digital and mobile technology is continually evolving and advancing, creating new ways to pay; from mobile wallets to peer-to-peer to digital currency, the modern payments landscape has evolved past simply cards and cash.

Consumers, eager to adopt these new ways to pay, are changing their purchasing habits to meet these emerging methods. To meet customers' needs, banks, fintechs, and merchants must keep up with these new trends and even more innovative ways to pay for goods and experiences.

However, with these new payment methods comes a new universe of fraud that firms must manage as fraudsters increase the sophistication of their attacks by utilizing emerging technologies like artificial intelligence for criminal purposes. To tackle this new era of fraud, firms must invest in secure technologies, including authentication, identity verification, transaction monitoring, and data theft prevention technologies.

In March 2019, Visa commissioned Forrester Consulting to evaluate how banks, financial technology companies, and merchants are protecting themselves and their customers from fraud amid this rapid expansion of new payment technologies. Forrester conducted 566 online surveys across Europe, the Middle East, Africa, North America, Latin America, and Asia Pacific in retail banking, fintech, and merchant services to explore this topic. We found that while enthusiasm for new payment technologies abounds, many organizations struggle with managing fraud and are turning to trusted partners to help them navigate new waters.

KEY FINDINGS

- **Digital payment adoption (including mobile) is increasing globally.** Consumers' usage of new payment technologies is expected to increase substantially over the next five years. Banks, merchants, and fintechs are working hard to ensure they offer these capabilities to their customers. Our survey found that 58% of respondents support digital wallets, 60% support peer-to-peer payments, and 72% support mobile banking bill payments.
- **Each new payment technology brings its own host of fraud concerns.** Companies recognize that new technologies bring new fraud challenges: 68% of respondents expressed concerns about fraud in mobile banking payments; 60% for mobile wallets; and 58% for peer-to-peer payments. However, 77% are ready to invest to meet these challenges head-on.
- **Companies recognize three top fraud concerns.** They are identity verification, data privacy/data theft management, and transaction monitoring.
- **Companies with more mature security practices take a more holistic approach to fraud management.** Proper protection requires a combination of new technologies, new teams, and new skills.

FORRESTER®

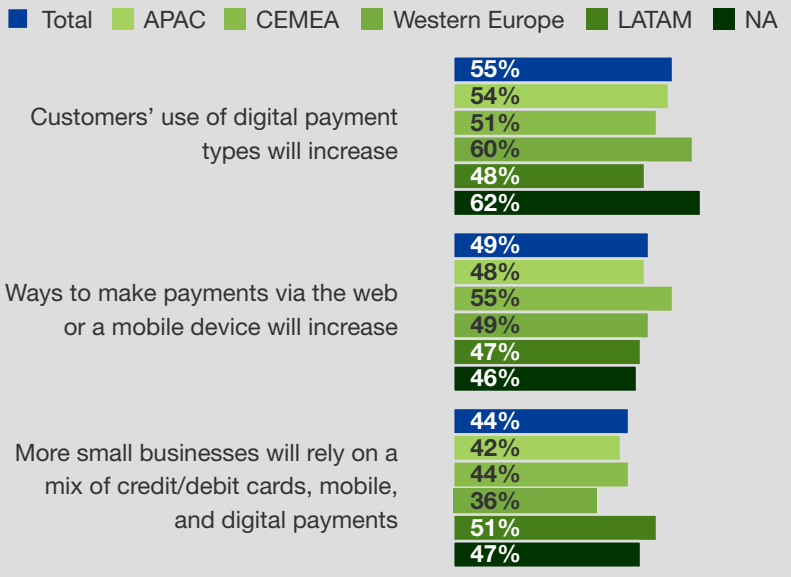
New Payment Technologies Are Emerging, And Consumers Are Utilizing These Emerging Methods

Digital and mobile technology have significantly reshaped consumers' purchasing habits. Long gone are the days when the only option for shopping was for consumers to physically enter a store to make a purchase. eCommerce has brought unrivaled convenience to shoppers around the world and has enabled purchases with a single click of a mouse or button. Simultaneously, the ways consumers pay for their purchases are also evolving. "Cash, debit, or credit" are no longer acceptable as the only options for purchases; around the globe, mobile payments are becoming increasingly more common and convenient.

Companies in the global payments ecosystem (merchants, banks, and fintechs) are cognizant of this shift and are transforming their operations to handle this change. Our survey of these companies found that 58% support digital wallets, 60% support peer-to-peer payments, and 72% support mobile banking bill payments. Companies expect this payments trend to continue, especially in Western Europe and North America, where over 60% of respondents noted that they expect customers' use of digital payment types to increase. Notably, in Latin America, over 50% of respondents expect small businesses to rely on a mix of credit/debit cards, mobile, and digital payments, as compared to 44% of the overall sample (see Figure 1).

Figure 1

"What changes do you expect to take place in the market over the next one to two years with respect to payments?" (Select all that apply)



Base: 566 global security, risk, and IT ops decision makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Visa, March 2019

60% of Western European and North American respondents anticipate digital payments to increase over the next one to two years.

FORRESTER®

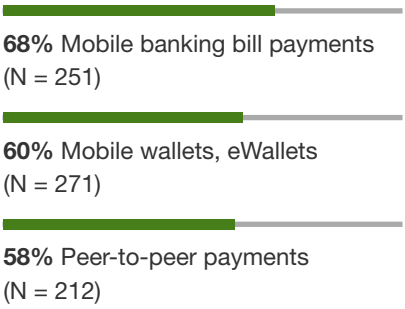
New Payment Technologies Bring New Fraud Threats

One downside of this advancement in payment technologies is that as payments get more innovative, so do fraudsters. Businesses are acutely aware of the new fraud risks that come with the adoption of new payment technologies: 61% percent of respondents at banks, fintechs, and merchants surveyed agreed that new payment technologies make them more susceptible to fraud. Specifically, 68% of respondents expressed concern regarding fraud in mobile banking payments; 60% for mobile wallets; and 58% for peer-to-peer payments (see Figure 2). A closer examination of these growing fraud concerns revealed two key observations:

- **Frequency of fraud specifically tied to digital payments is lower than other fraud types.** We asked companies what types of fraud they have experienced within the last two years and found that identity and account-related fraud were more prevalent than fraud types experienced during the purchase. Identity theft/new account fraud (i.e., using stolen identifying information to open an account in a customer's name), enumeration attacks (i.e., accessing information/functionality through automated value testing), and ATM cashout (i.e., exploiting vulnerabilities to withdraw money from cash machines fraudulently) topped the list. Fraud types that are payments-oriented, such as card-not-present fraud (for eCommerce and/or phone/mail orders) or chargeback fraud (i.e., cardholders disputing valid charges), were less common, impacting only 28% and 23% of companies surveyed. The reason for this lower number may be that companies are better prepared to defend against these threats or that the volume of those threats is lower, since many companies are still adopting these new payment types.
- **However, fraud related to digital payments has larger business impacts.** Perhaps more important than the frequency of different fraud types is the financial impact to the business of the different fraud types outlined above. When asked to approximate what percentage of fraud losses and operational costs was caused by the various fraud types, survey respondents whose companies had experienced fraud indicated that card-not-present fraud represented nearly 40% of their losses.

Figure 2

"How concerned is your company about payments fraud for each of your new technologies?"
(Showing percent "Concerned" or "Very concerned")



68% Mobile banking bill payments
(N = 251)

60% Mobile wallets, eWallets
(N = 271)

58% Peer-to-peer payments
(N = 212)

Base: Variable global security, risk, and IT ops decision makers at companies that use the above payment types (bases vary by payment type)
Source: A commissioned study conducted by Forrester Consulting on behalf of Visa, March 2019

BUSINESSES HAVE CONSISTENT FRAUD MANAGEMENT CONCERNS FOR ALL DIGITAL PAYMENT TYPES

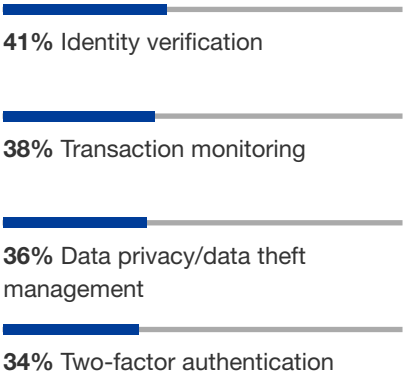
We asked respondents about where they had specific fraud prevention concerns for new digital payment technologies (e.g., mobile wallets, mobile banking bill payments, and P2P payments). Four specific authentication/fraud prevention methods consistently rose to the top (see Figure 3):

- **Identify verification (IDV).** Online and faceless customer approach with low customer friction makes IDV challenging. Firms need to use physical credit file header-based IDV methods, identity documents, device ID, and phone number reputation to provide a full gamut of IDV methods. Failure to focus on IDV will result in ID theft and fraudsters using synthetic identities.
- **Transaction monitoring.** Authenticating users is only a part of the puzzle of a holistic fraud management strategy. To protect against payment fraud, firms need to monitor transactions in context and understand any anomalies in payments compared to the user's own, earlier transactions as well as the user's peer group's transactions. Failure to monitor transactions will result in higher rates of money laundering and other increased losses due to payment fraud.
- **Data privacy/data theft management.** Fraudsters used to steal only payment card details. With the adoption of mobile and P2P payments, it's no longer the individual payment card details that are attractive but the credentials (passwords) to steal the entire contents of an application digital payment account. Failure to protect data from theft will result in higher payment fraud.
- **Two-factor authentication (2FA).** Passwords alone are no longer adequate to protect any transaction, including accessing and using P2P and mobile payment methods. While 2FA can offer an added layer of protection, there are still vulnerabilities that companies are concerned about. These concerns may be lessened as firms explore more sophisticated 2FA capabilities such as time-based, one-time passcode (TOTP) or biometrics to minimize account takeover (ATO). Failure to implement these methods can lead to increased payment fraud losses and ATO rates.

These authentication and fraud management capabilities are important for companies to acknowledge and plan for with the adoption of any new payment technology.

Figure 3

"Which of the following authentication/fraud prevention methods do you have the most concerns about implementing for mobile wallets/eWallets?"



Base: 271 global security, risk, and IT ops decision makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Visa, March 2019

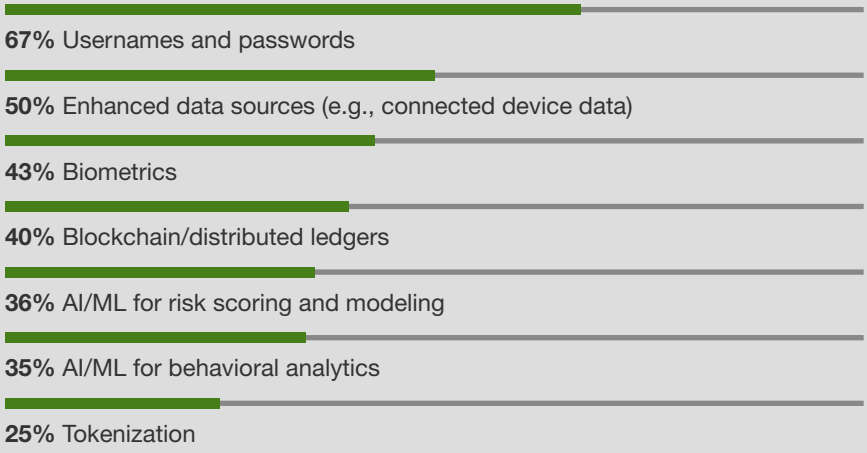
Companies Must Balance Payment Technology Investments With Security Investments

Companies are facing pressure from both internal and external sources to implement and manage new payment risk capabilities. Forty-seven percent of respondents said that consumers are demanding new, secure payment capabilities — ready to take their dollars elsewhere if not properly protected. Additionally, 48% of executives are demanding their organizations to evolve their payment risk management capabilities, recognizing the deep and lasting impact fraud can have on their business. When looking at what companies are doing today to manage fraud and risk, we found:

› **Risk management capabilities need to be more sophisticated.** Usernames and passwords are still the most popular capability — but they have been used for years. Risk management must evolve beyond username and passwords to keep up with the new fraud management demands. However, adoption is at 50% or less for many new capabilities (e.g., connected device data, biometrics, blockchain, AI and machine learning for risk scoring, etc.). Only about a third of respondents' companies were using new sources like AI or machine learning (ML) for risk scoring or behavioral analytics; 43% were using biometrics; and only 25% were using tokenization (see Figure 4). While adoption of tokenization and blockchain is currently low, Forrester expects use of these technologies to grow as their benefits become more apparent.

Figure 4

"Which of the following capabilities, if any, does your company utilize currently to support payment risk management?" (Select all that apply)



Base: 566 global security, risk, and IT ops decision makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Visa, March 2019

FORRESTER®

- **Businesses are investing in payment security tools and talent.** Eighty-four percent of organizations are investing in hiring new talent with specialized fraud/security skills, and 77% are investing in new tools to manage their payment technologies. Organizations must create robust teams centered on managing new payment technology to keep pace with emerging new threats from fraudsters.
- **Businesses need partners to help up-level their fraud and security management capabilities and to better support new payment technologies.** Broadly speaking, organizations recognize that advanced analytics and decision-making models are crucial to success in addressing the risks of new payment technologies. Many don't have these capabilities on their own and are investing in partnerships that can provide those capabilities. Additionally, 39% of survey respondents stated that security capabilities are a critical requirement of their partners. Businesses recognize that these advanced capabilities are a key requirement to effectively roll out new payment technologies and simultaneously minimize fraud.

Mature Fraud Management Practices Lead To Greater Business Success

Through the combination of tools, talent, and partnerships, businesses can be better prepared to secure new payment technologies. However, not all companies are equally prepared with these capabilities. We asked the bank, fintech, and merchant respondents we surveyed a series of questions about how their organizations are prepared to manage payments fraud to determine their fraud management maturity. The questions focused on four primary factors regarding companies' approaches to payments fraud management: 1) the presence of clear payment security strategies, 2) the presence of strong governance practices, 3) the way in which companies are investing in the right skills and technology, and 4) the degree to which companies' risk/fraud strategies are customer focused. Based on how respondents answered these questions, we classified them as immature, transitioning, or mature regarding their fraud management practices.

When comparing responses by maturity group, we focused specifically on immature and mature organizations, rather than transitioning organizations, and observed the following key differences between those two groups (see Figure 5):

- **Confidence in fraud detection capabilities increases with maturity.** Only 54% of immature organizations are confident in their organizations' fraud detection capabilities for peer-to-peer payments — compared to 81% of mature organizations — and only 56% of immature organizations are confident in their ability to detect fraud in mobile wallet payments — compared to 88% of mature organizations.
- **Mature companies have greater adoption of advanced risk-management capabilities.** Forty-four percent of mature organizations have adopted AI and ML for risk management, compared to 24% of immature organizations. Interestingly, the findings were similar for biometrics and enhanced data sources as well (see Figure 6).

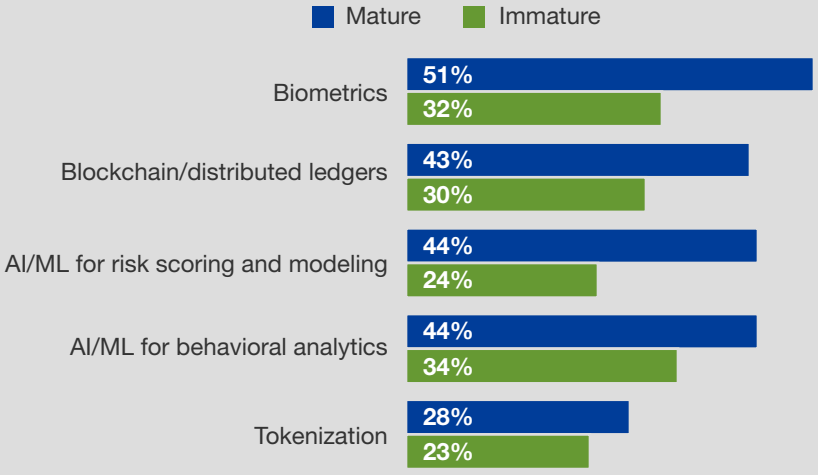
Figure 5

IMMATURE	MATURITY MEASURES	MATURE
• Lack a holistic payments fraud management strategy. • Less than half have a dedicated team to manage payment security. • Risk management priorities are most commonly driven by auditing team. • Mostly using basic security features for payments (i.e., usernames and passwords).	Level of focus in supplying customers with the right payment risk tools and features for all payment types	• Holistic approach to payment fraud (i.e., investing in tools, teams, and tech simultaneously). • Nearly all have a dedicated team to manage payment security. • Risk management priorities are driven by multiple internal teams (i.e., auditing, executives) and customers alike. • Using more advanced security techniques for payments (i.e., AI, ML, biometrics).
	Level of investment in new technology capabilities to help build next-gen fraud management solutions	
	Degree to which more sophisticated analytical techniques are used to enhance fraud detection	
	Is there a documented, repeatable process for vetting new services that could impact customer security?	
	Level of training/education for risk fraud personnel to keep up with the latest trends	
	Is there a well-defined security road map to gauge readiness against emerging risks and identify gaps?	
	Degree to which companies are making strategic investments in security innovation	
	Degree to which companies are investing in new security talent and technology	

Base: 566 global security, risk, and IT ops decision makers
*Note: Not all maturity measure shown. Maturity was calculated based on respondents' aggregate responses to all the maturity measures (see Appendix).
Source: A commissioned study conducted by Forrester Consulting on behalf of Visa, March 2019

Figure 6

"Which of the following capabilities, if any, does your company utilize currently to support payment risk management?" (Select all that apply)



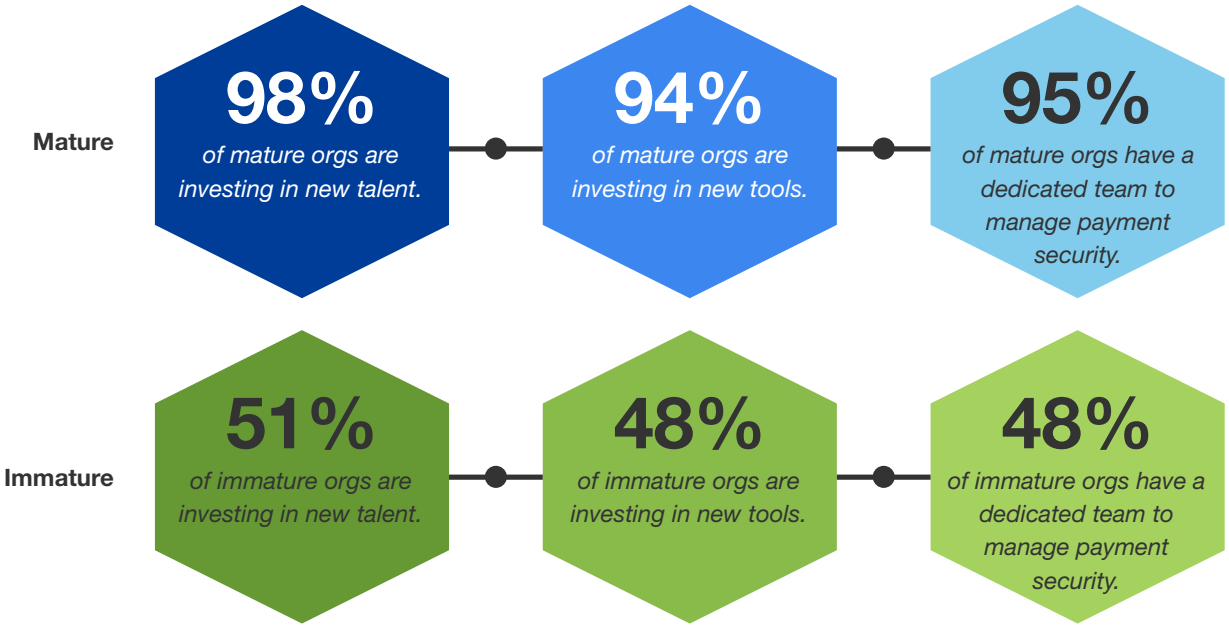
Base: 566 global security, risk, and IT ops decision makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Visa, March 2019

FORRESTER®

› **Mature companies take a more holistic approach to fraud management.** Mature organizations are investing in talent, tools, and teams simultaneously while immature organizations are approaching these investments in a piecemeal fashion (see Figure 7). This also includes the way companies use partners: 64% of respondents at mature companies said that security capabilities of partners are a critical requirement in working with partners, compared to only 17% of respondents at immature companies.

Figure 7

Mature Organizations Approach Fraud Management Holistically



Base: 566 global security, risk, and IT ops decision makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Visa, March 2019

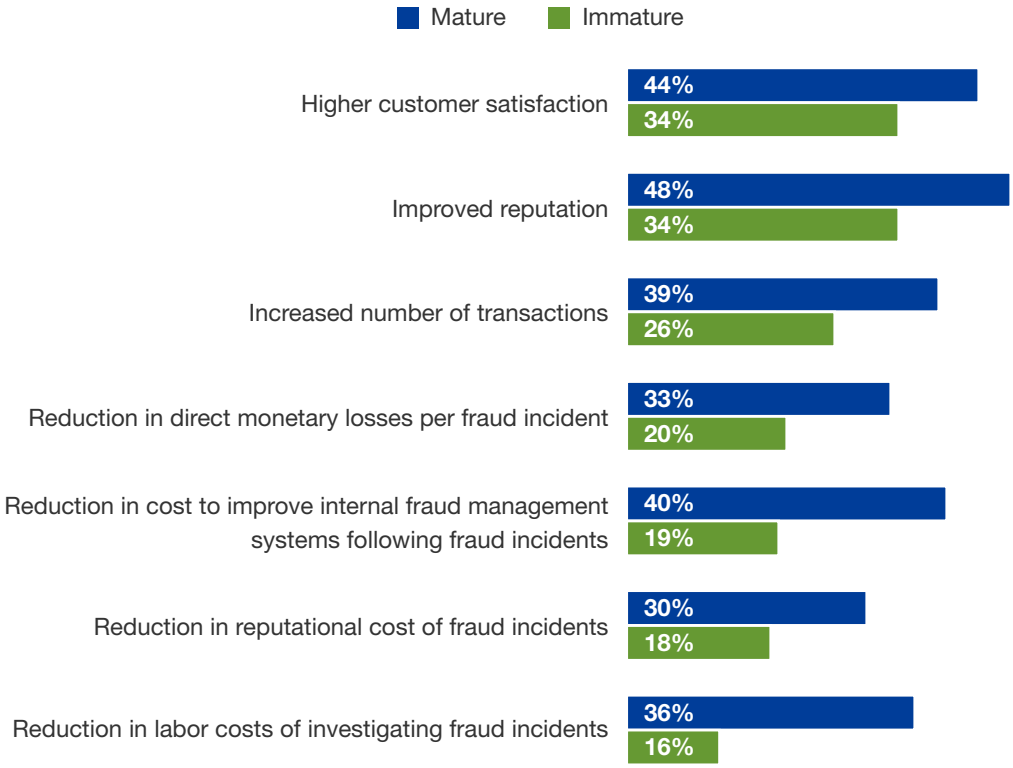
MATURE COMPANIES EXPECT A BROADER RANGE OF BUSINESS BENEFITS

As mature companies take a more holistic approach to fraud management, they see greater opportunity for those efforts to benefit the business. For example, for every benefit category we asked about in the survey, mature companies had a higher expectation for those benefits, by a margin of at least 10% or more (see Figure 8). The top expected business benefits of improving fraud management capabilities are:

- **Improved customer satisfaction.** The top benefit cited by both mature and immature organizations was higher customer satisfaction. Improved customer experience has a clear impact on bottom-line revenue for businesses; notably, Forrester found that companies with exceptional customer experiences grew revenue five times faster on average than their competitors with poorer customer experiences.[1] By investing in new fraud management tools, technology, and talent, mature organizations are more readily able to create seamless customer experiences.
- **Improved reputation.** Nearly 50% of mature organizations see higher improved reputation as a benefit of improving their payment security technologies, as compared to 34% of immature organizations. Brand reputations take years to grow, and mature organizations realize that they must fortify their payment security walls to secure their reputations.
- **Reduction in internal fraud management system costs.** Forty percent of mature organizations see reduced costs in internal fraud management systems, as compared to 19% of immature organizations. In fact, this was the third-most stated benefit for mature organizations, but the fifth-most stated benefit for immature organizations. This large delta is due largely to the fact that mature organizations are holistically approaching their fraud management tools and teams, which includes building in feedback loops so that after an incident, systems are continuously improving.

Figure 8

"What are the top benefits/advantages your company hopes to achieve through improving security of new payment technologies?" (Select up to five)



Base: 566 global security, risk, and IT ops decision makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Visa, March 2019

Key Recommendations

Managing payment fraud holistically is imperative in meeting consumers' growing demands, maintaining/improving fraud management, and keeping a business ahead of the curve and successful.

Forrester's clients report that to avoid issues reported above — especially around fraud detection capabilities — and to build a world-class fraud management strategy, they employ a combination of the following best practices:

Look at customers in context through the lens of AI — regardless of what type of payment they use. It's all about treating your customers' information on an entity basis and using artificial intelligence and machine learning technologies to 1) reduce investigation workload and 2) improve the customer experience by optimizing authorization and fraud rates. Don't just look at a single payment transaction but understand the customer's identity in its entirety (address, payment type at enrollment, etc.) and the customer's peer group's payment history for better decisions. Older, simpler risk-scoring technologies, such as pure rule-based risk scoring on its own to protect against fraud, will quickly become obsolete. This method also allows fraud management decisions to inform business intelligence and marketing decisions.

Incorporate tokenization as part of a holistic fraud management strategy for mobile and P2P payments. Generations Y and Z demand a new generation of payments. Forrester expects that mobile and P2P payments will proliferate very quickly in the next 18 to 24 months. This mandates that firms 1) use tokenization to protect cardholder data in the event of a breach, 2) ingest as much data around these payments (e.g., IP and geolocation, device attributes, etc.) as possible, and 3) look to vendors that offer out-of-the-box, productized fraud management models for mobile and new P2P payments.

Integrate fraud management systems and investigation interfaces. If your investigators and analysts must work with more than one fraud management solution to get a complete 360-degree view of a customer and their transactions, it will likely lead to lower accuracy, more rework, and thus higher investigation costs. Integrating fraud management systems to offer a single pane of view to fraud investigators helps to alleviate the problems above.

Improve the customer authentication experience. To utilize additional data elements for enhanced transaction processing and to minimize fraud losses, firms need to deploy versatile and flexible password-less, risk-based, and two-factor authentication methods (including biometrics and behavioral biometrics) to guard against ATO and other types of emerging online fraud. We recommend using push notifications, facial and fingerprint biometrics, and behavioral biometrics as the most difficult-to-tamper-with types of 2FA. Leveraging industry standards such as 3D Secure (3DS) to allow the exchange of additional customer data can enable a more secure online payment experience.

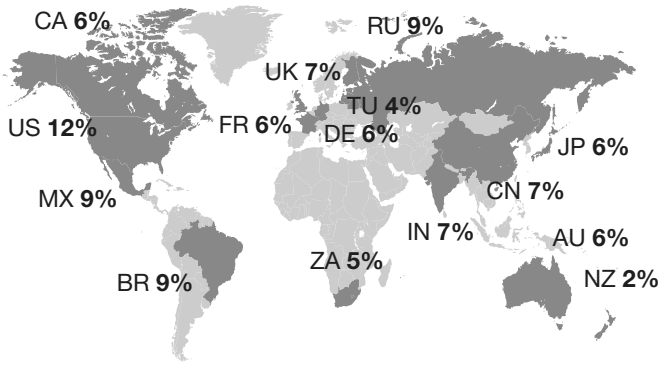
Treat fraud management as a process and program, not as a single project. Treat payment fraud management as a cycle and continuing improvement process and not as a single, standalone project. This requires continuous model monitoring and improvement, including velocity monitoring. Firms should also focus on what threats are prevalent and stay current on the tools and practices to mitigate those risks that are common or unique to their business to stay on top of evolving fraud patterns.

Appendix A: Methodology

In this study, Forrester surveyed 566 professionals across North America, Latin America, Western Europe, Central Europe/Middle East/Africa (CEMEA), and Asia Pacific. Survey participants included decision makers in fintech, retail banking, and merchants. Respondents were offered a small incentive as a thank you for time spent on the survey. The study was completed in March 2019.

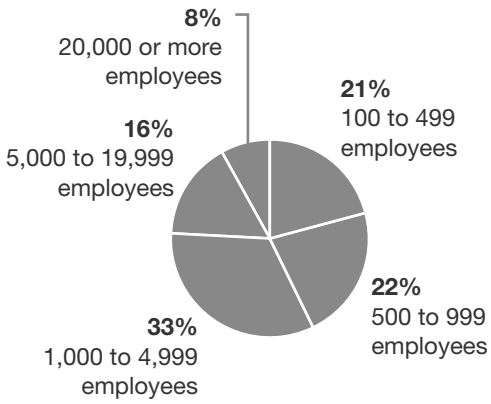
Appendix B: Demographics

COUNTRY

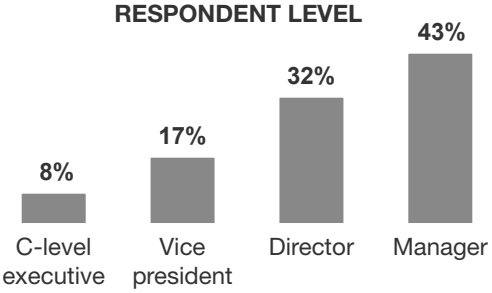


- North America **18%**
- Latin America **18%**
- CEMEA **19%**
- Western Europe **18%**
- APAC **28%**

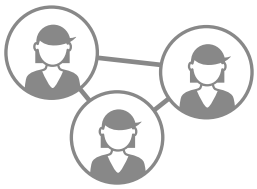
COMPANY SIZE



RESPONDENT LEVEL



DEPARTMENT



38%	Finance accounting
26%	IT security and operations
17%	eCommerce
17%	Compliance/risk management
2%	Operations-fraud/ authorization strategy

RESPONSIBILITY

100% of respondents are involved in:

- Digital payment technology planning and investments.
- Identity and access management.
- Risk management.
- Fraud prevention.

INDUSTRY GROUPINGS

Fintech **33%**	Financial technology	**33%**
Retail banking **33%**	Issuer and acquirer	**17%**
	Issuer only	**13%**
	Acquirer only	**3%**
Merchants **34%**	Consumer services	**13%**
	Entertainment	**10%**
	Retail and restaurants	**7%**
	Telecommunications	**2%**
	Travel and hospitality	**2%**

Base: 566 global security, risk, and IT ops decision makers
Note: Percentages may not total 100 because of rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of Visa, March 2019

Appendix C: Endnotes

[1] Source: "Improving CX Through Business Discipline Drives Growth," Forrester Research, Inc., June 19, 2017.

FORRESTER®