IDC | ANALYZE THE FUTURE

A Guide to Driving Digital Transformation with Adaptive Risk Management

WRITTEN BY:

Aaron Press
Research Director,
Worldwide Payment Strategies, IDC

Jordan Jewell
Research Manager,
Digital Commerce, IDC

Digital commerce is changing and growing rapidly, and fraud is changing and growing right along with it. Organizations need their fraud solutions to evolve along with their commerce operations and strategies.

Key Takeaways

- Traditional fraud and risk solutions are becoming less and less effective. This is not only because fraudsters are becoming more sophisticated but also because the digital economy has rapidly grown in size and complexity.
- Online merchants face a long-standing challenge: delivering frictionless commerce experiences without creating excessive risk. It is especially challenging for online merchants to strike the perfect balance between trust, risk, and simplicity.
- As the environment becomes more complex, merchants must adopt new, data-driven strategies to keep fraud at bay while continuing to create a positive customer experience and grow the business.

In this Spotlight

Click below to navigate to each section.

Introduction

From marketing, to merchandizing, to transaction, to post-transaction, data fuels today's ecommerce landscape. Powered by the ubiquity of connected devices, data has the potential to inform every decision a merchant makes at every stage of the customer journey. This creates an opportunity for merchants to deliver great, personalized commerce experiences to their customers.

All this data also creates an opportunity for fraud. Whether compromised identity data, breached financial data, social engineering-derived information, or even malware, fraudsters have access to their own large data sets and unprecedented access to sophisticated tools and forums.

To fight fraud, firms must work with a partner that can leverage the insights of a vast risk intelligence network to outmaneuver fraudsters.

Traditional fraud and risk solutions are becoming less and less effective at supporting merchants in this environment. This is not only because fraudsters are becoming more sophisticated but also because the digital economy has rapidly grown in size and complexity. Merchants need new solutions to help them stay a step ahead of fraudsters.

Digital Transformation Is Accelerating, and Consumer Expectations Are Rising

IDC has witnessed an economywide shift to digital commerce thanks to the proliferation of digital, mobile-first experiences and consumers' adoption of these experiences. This shift has been gradual but clear over the past decade, with the U.S. Census Bureau reporting that over 11% of all retail transactions occurred online in 2019. The COVID-19 crisis has significantly accelerated this trend, causing more transactions to occur online, propelling the demand for secure, seamless, cross-channel digital experiences. As a result, many merchants that had not previously invested in a digital strategy have ramped up their ecommerce operations rapidly to keep their businesses alive through the pandemic.

But COVID-19 is not the only driver here. Consumers were already expecting engaging, cross-channel, and personalized digital experiences when they interacted with brands. This is especially true in today's global economy, where merchants are no longer able to defer transformation due to the operational challenges of selling to a wide range of customers:

- Customer experiences must be high value and low friction — secure, fast, and seamless.
- There are competing priorities — enhance customer experience while reducing fraud/operational costs.
- Regulatory and compliance issues are increasing in complexity, are inconsistent around the world, and are constantly changing.
- Consumer perception of online privacy and security continues to hinder transaction completion rates.
- Fraud is a threat to every business.

In IDC's 2020 *PayPal Enterprise Payments Survey,* "preventing fraud and managing risk" tied for first place as the top challenge faced by online sellers. Savvy merchants understand that if they want to succeed, every business and technology decision they make must be centered around the customer experience. This includes fraud prevention, where merchants must prioritize a solution that addresses end-to-end fraud, provides robust data analytics, and quickly adapts as fraud evolves.

Online Merchants Struggle to Grow While Mitigating Fraud

Unfortunately, the massive growth in ecommerce has also led to rapid growth in fraud, in terms of volume and sophistication. Fraudsters have made significant investments in data, technology, and business models required to be successful at their jobs. In addition to data, fraudsters can turn to a considerable set of tools and services to streamline their operations. Crime-as-a-service (CaaS) functions even enable the

outsourcing of fraud. Attack automation tools can use identity and payment data again and again to find vulnerable sites and merchants. Remote access, location spoofing, and a range of bots let fraudsters appear to be whomever they wish to impersonate. Meanwhile, malware allows a range of theft and deception, from the stealing of data to proxy locations. In short, fraudsters have a large toolset with which to orchestrate a variety of attacks on online merchants across the globe.

At the same time, legacy fraud prevention systems have not effectively kept pace. These systems often rely on linear models that are not adept at recognizing changes in the risk environment. These legacy systems typically have limited shared intelligence, meaning merchants can learn from only their own experience rather than from the broader community.

Basic machine learning (ML) rule sets, while typically better than manually developed rule sets, tend to age poorly and are challenging to update. The result is high false positives, friction for end customers, and operational inefficiencies.

The response to the growing fraud threat has been a proliferation of new security solutions: identity, device, email, behavioral biometrics, physical biometrics, etc. These solutions add more layers of protection and are effective at improving performance. But there are also drawbacks; adding these additional security systems creates a flood of data, which must be managed and is typically viewed in isolation of other data sources. This creates complexity in understanding which elements represent risk and can obscure data relationships that would otherwise be highly predictive. The result is that such "layered methods" that combine these concepts into workflows, while better than using them in isolation, can be suboptimal in performance as merchants are challenged to pull together multiple point solutions from different providers to create the "customer experience" they are envisioning.

As merchants scale their businesses and expand their ecommerce footprint, they must address unique risk challenges head-on and at all stages of business growth.

IDC recommends that online merchants focus on the following initiatives:

- **Chargeback costs** that impact profit
- **Increases in transaction volume** that impact operations
- **Keeping up with regulations,** including know your customer (KYC)
- **Developing new offerings/programs:**
  - Account creation/management
  - In-house checkout
  - Loyalty/reward programs

Fraudsters have adapted to today's digital economy, increasing the potential risk involved in selling online. Merchants must also become smarter by adopting an adaptive risk management system that works alongside their digital commerce and payments infrastructure.

Key Trends in Fraud Management

Major trends that will shape the fraud management, digital payments, and ecommerce market over the next 36 months include the following:

- **Ability to balance convenience and risk.** Online merchants face a long-standing challenge: delivering frictionless commerce experiences without creating excessive risk. It is especially challenging for online merchants — whose goal is to win and retain new customers — to strike the perfect balance between trust, risk, and simplicity. Excessive friction can result in an abandoned cart, and a poor experience will keep customers from returning to a merchant's website.
- **Card not present (CNP)–driven omni-channel commerce.** As a larger share of merchants' sales happen online, a larger share of purchases made by merchants' net-new customers occur digitally.

This raises the risk of CNP fraud with compromised cards. New customers pose additional challenges because merchants don't know how they behave, so there is a high risk of creating unnecessary friction. When the goal of keeping customers is to maximize lifetime value, friction will keep customers from returning to merchants' websites. Worse, if fraud is committed in a customer's name, even established customers may stay away forever.

- **Artificial intelligence (AI).** There has been a significant increase in the use of AI and ML in risk management in the past five years. AI/ML has become more sophisticated in this period, and fraud management is an ideal use case for the technology. Training intelligent fraud management systems requires large data sets, driving the trend toward shared and consortium data models among multiple participants, including merchants and payment processors, where more transactions and outcomes can be included in the training data for more accurate models.
- **Regulatory shifts.** Another significant market trend in the fraud space is the regulatory shift to protect customer data, including GDPR and the mandate for Strong Customer Authentication (SCA) under PSD2. In this changing environment, protecting customer data is not just a good idea — in many cases, it's the law. Fraud prevention is not just about stopping the bad guys anymore; merchants must also protect their customers and themselves with advanced tools to prevent fraud and identity compromise.

Benefits of Using an Adaptive Risk Management Solution

Needless to say, merchants have complex business and risk challenges when selling online across geographies and customer segments. Partnering with the right fraud solution provider can help sellers solve several competing priorities.

A robust fraud solution provides online merchants with the following key benefits:

- **Fewer transaction declines.** In the fraud management space, the main metric of success is reducing the decline rate without introducing significant additional fraud occurrences. A strong fraud management solution allows merchants to stop treating good customers like fraudsters and maximize orders/revenue.
- **Chargeback reduction.** A test of a strong fraud management solution is limiting fraudulent chargebacks. This is achieved by using extensive data intelligence and advanced machine learning to accurately identify and block fraudulent transactions and improve authorization rates.
- **A vast network of global risk intelligence.** Comprehensive fraud solutions leverage a massive data set of merchants, advanced machine learning techniques, and data science expertise to identify newly trending fraudulent activity and act accordingly across all other merchants on the network. To do so, merchants should look for fraud providers with deep experience in fintech, services compliant with regulations around the globe, and experience implementing fraud solutions for merchants of any size across a variety of verticals.
- **Superior customer experiences.** The system should enable better customer experiences by removing friction caused by unnecessary authentication and enabling seamless experiences for genuine customers.
- **Transparency.** Comprehensive fraud management solutions enable more insight and control to align merchants' unique business needs and tolerance for risk.
- **Future-proof fraud management.** The best solutions help merchants mitigate fraud today and in the future. This is achieved by enabling merchants to proactively fight evolving fraud — leveraging an advanced ML-based platform (with risk score, rule suggestions/recommendations) that adapts to evolving fraud and business needs and gets smarter with every transaction.

- **Unlocked real-time decision making.** The tools should immediately differentiate between good customers and bad actors, flagging suspicious transactions for review. This improves operational efficiency by automating the decision-making process while still providing merchants with a streamlined review process.

When properly implemented, a comprehensive fraud management solution will allow merchants to focus on what they really want to focus on—growing their business.

Integrated Risk Management on the PayPal Commerce Platform

PayPal's two-sided network provides a rich source of data that feeds its predictive models. The data comes from over 360 million active consumers and over 28 million merchants across the globe. PayPal's risk solutions are the only offerings in the industry that leverage PayPal's extensive two-sided network combined with industry-recognized machine learning and analytics, helping more accurately detect and block fraud in real time (see **Figure 1**). The results can include the following:

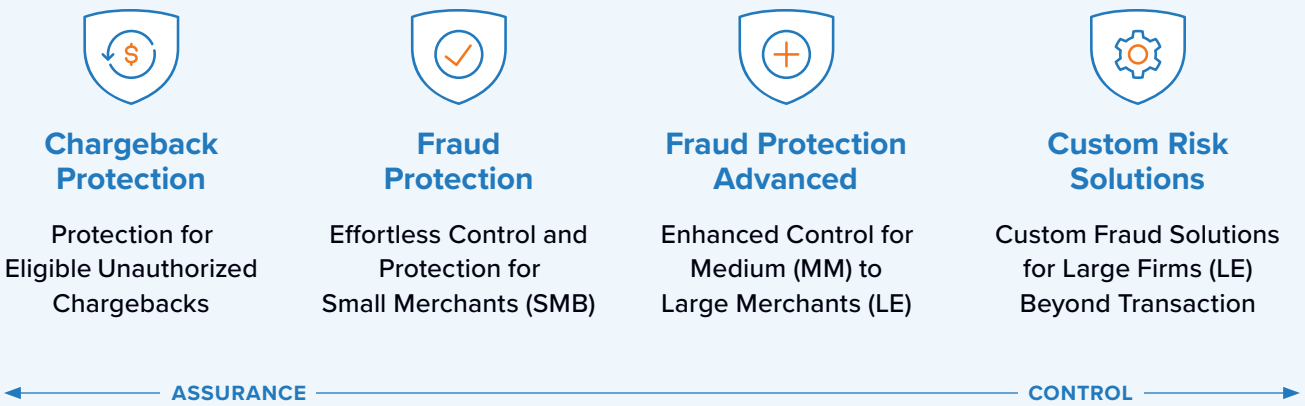
- Fewer chargebacks
- Lower false positive rates
- Less customer friction
- Lower fraud losses
- Improved operational efficiency
- Streamlined customer experiences

PayPal makes standalone and integrated solutions available to ecommerce and financial services businesses of all sizes, providing scalability as businesses grow.

The company offers the following options:

- **Chargeback Protection.** With Chargeback Protection, PayPal helps online merchants focus on growing their business rather than battling fraud and chargebacks. PayPal decisions card transactions for merchants by automatically approving or declining transactions. In the event a chargeback occurs related to a qualifying previously approved transaction, PayPal will refund the disputed amount and any associated fees, up to a predetermined limit.

FIGURE 1
PayPal Risk Offerings Built for eCommerce



Source: PayPal, 2021

- **Fraud Protection.**
  Built into the PayPal Commerce Platform and Braintree, Fraud Protection is a fraud toolkit that provides merchants with more insight into and control over the decisioning process of their card transactions to better balance chargebacks and declines.
- **Fraud Protection Advanced.**
  Built into Braintree, Fraud Protection Advanced arms fraud teams with robust capabilities to help identify and investigate suspicious transactions, analyze patterns, uncover key insights, and develop strategies to mitigate fraud losses and protect business growth.
- **Fraud Protection Custom.**
  This adaptive decisioning platform empowers large ecommerce firms and financial institutions with best-in-class machine learning to dynamically decision across a user's life cycle, from sign-up to log-in to checkout and beyond.
- **Risk APIs.**
  This risk mitigation service was created to help the world's largest ecommerce merchants fight transaction fraud through an easy-to-integrate API that empowers them with risk intelligence from PayPal's two-sided network, composed of over 360 million active accounts transacting more than 12 billion times a year.

PayPal is a globally recognized and trusted financial technology brand. The company also offers technical support, business consulting, and continual innovation that will drive success.

Challenges

PayPal faces the following challenges in the fraud management and digital payments space:

- **Merchant saturation.**
  In IDC's 2020 *PayPal Enterprise Payments Survey,* over 76% of respondents with a digital payments platform said that they already have a fraud management system in place.
- **Security concerns.**
  Organizations, especially large organizations with fraud management teams already in place, are often hesitant to hand over the transaction decision process to a third-party provider. Doing so requires that merchants hand over some of the revenue generation to a third party. By IDC's estimation, only a quarter of merchants completely outsource CNP fraud prevention. To overcome this resistance, PayPal will need to grant its customers some ownership of the fraud management rules and provide transparency about how decisions are being made.

Conclusion

Digital commerce is expanding rapidly, in terms of both size and complexity. Merchants must accelerate their online strategies to remain relevant but must do so without taking on unnecessary risk or sacrificing a good customer experience. At the same time, fraud is growing more sophisticated and threatens to take a larger and larger share of revenue. As the environment becomes more complex, merchants must adopt new, data-driven strategies to keep fraud at bay while continuing to create a positive customer experience and grow the business. AI and ML are critical to achieving this goal, and having a rich data source of transaction data is essential to leveraging the technology.

IDC believes that robust fraud solutions will grow in importance as the shift to digital commerce continues to drive more and more transactions online. PayPal, with its range of solutions built on its unique data assets, is well positioned to succeed in the digital commerce market.

About the Analysts

Aaron Press
Research Director,
Worldwide Payment Strategies, IDC

Aaron Press is Research Director for IDC Insights responsible for the Worldwide Payment Strategies practice. Aaron's core research coverage includes bank, corporate, and merchant challenges around the evolution of payment networks, systems, and technology, fraud and security risks, and legal and regulatory issues.

More about Aaron Press

Jordan Jewell
Research Manager,
Digital Commerce, IDC

Jordan Jewell is a Research Manager for IDC's Enterprise Applications and Digital Commerce team and leads IDC's Digital Commerce research practice. In this role, he leads research initiatives addressing both B2B and B2C digital commerce platforms, digital marketplaces, order management software, and adjacent technologies that facilitate online commerce. Jordan joined IDC in 2015.

More about Jordan Jewell

Message from the Sponsor

About PayPal

Our mission at PayPal is to democratize financial services to ensure that everyone, regardless of background or economic standing, has access to affordable, convenient, and secure products and services to take control of their financial lives.

Fueled by a fundamental belief that access to financial services creates opportunity, we work across our brands to give people the financial tools they need to connect and transact in new and powerful ways — and ultimately, to join and thrive in the global economy.

For more information, please visit us at:

paypal.com/us/enterprise/manage-risk

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

idc.com

Permissions: External Publication of IDC Information and Data

Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Doc. #US47409721