McKinsey&Company

McKinsey on Payments

Contents

Volume 11 Number 27 June 2018

Fraud management: Recovering value through next-generation solutions

The incidence of card fraud has rocketed in the past few years, partly as a result of the rise of e-commerce and mobile payments. Worldwide losses climbed to almost $23 billion in 2016, and could be close to $44 billion by 2025 (Exhibit 1). A recent report found that 82 percent of companies surveyed had been victims of fraud in 2016, an increase of 21 percentage points in four years. In addition to the direct cost of fraud, companies also lose sales when good transactions are denied by fraud management systems. Another report found that up to 25 percent of declined sales transactions for e-commerce merchants were false positives.

Lindsay Anan
Robert Hayden
Kaustubh Joshi
Marie-Claude Nadeau
Jonathan Steitz

As more merchants migrate to EMV, the global standard for chip-based debit and credit card transactions, fraud for card present (CP) transactions has fallen, but fraud for card not present (CNP) payments has increased. This places bigger burdens on merchants, since they bear the cost of CNP-based fraud, whereas banks do so for CP. Mobile payments face even more security risks because smartphone technology lags traditional computer systems in terms of security. For instance, operating systems are not updated as frequently, and security software is less common. As more commerce moves online and onto mobile, card and other types of fraud are draining substantial value from companies and putting the reputation of their brands at risk. Countering this threat will require companies to master state-of-the-art fraud management methods and tools.

This imperative is particularly urgent in the United States, which leads the world in losses from card fraud. In 2016, the US had a 40 percent share of global losses, worth $9 billion. Between 2013 and 2016, the cost of card fraud as a percent of revenue for US merchants rose by 42 percent, and the number of fraudulent transactions rose by 34 percent (Exhibit 2, page 32). A disproportionate share of this burden falls on larger e-commerce and mobile commerce merchants, with fraud costs as a percentage of annual revenues running 15 and 30 percent higher, respectively, than those of physical retailers.

In the near term, McKinsey expects that the main fraud challenges facing e-commerce and financial services firms will continue to be friendly fraud (disputed charges from valid cardholders) and identity theft. However, the nature of fraud is likely to evolve. For instance, identity theft is mutating from card skimming to account takeovers—a shift with major implications for most firms.

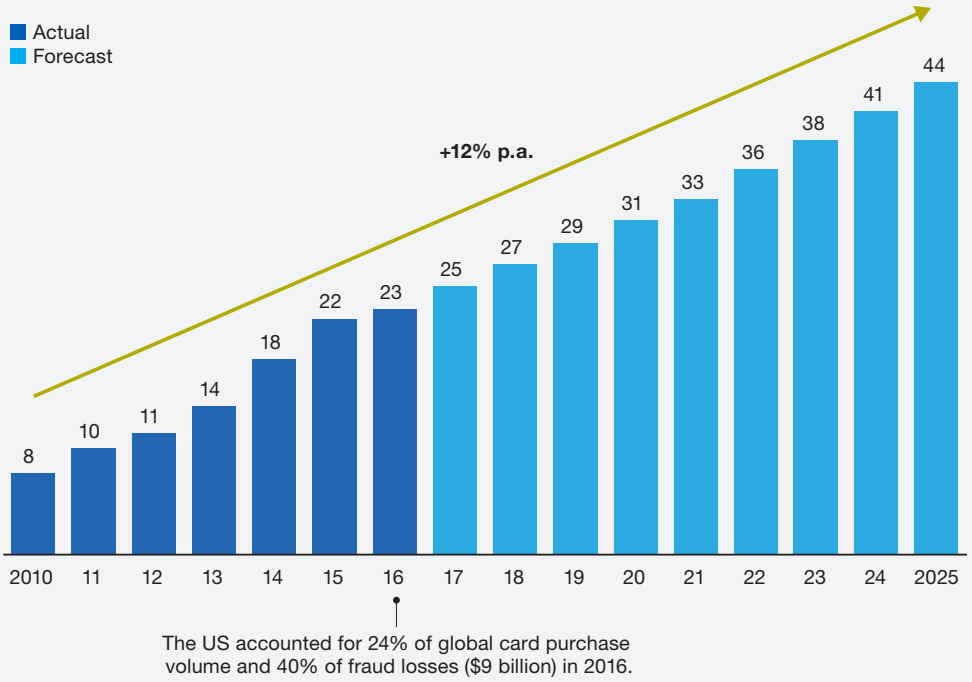
Fortunately, today's firms have the means to fight back. Next-generation fraud management solutions have the potential to dramatically improve detection rates while substantially reducing false positives. Not only that, they can improve the customer experience and build customer engagement, loyalty, and value.

How fraud is evolving

To protect themselves, companies need to understand the pace, direction, and paths along which fraud is moving, and the trends shaping the future of fraud management.

Exhibit 1

Global card fraud losses totaled almost $23 billion in 2016.[1]



[1] General-purpose and private-label global and domestic credit, debit, and prepaid cards; excludes operational costs incurred by issuers, merchants, acquirers, call centers, and chargeback management.

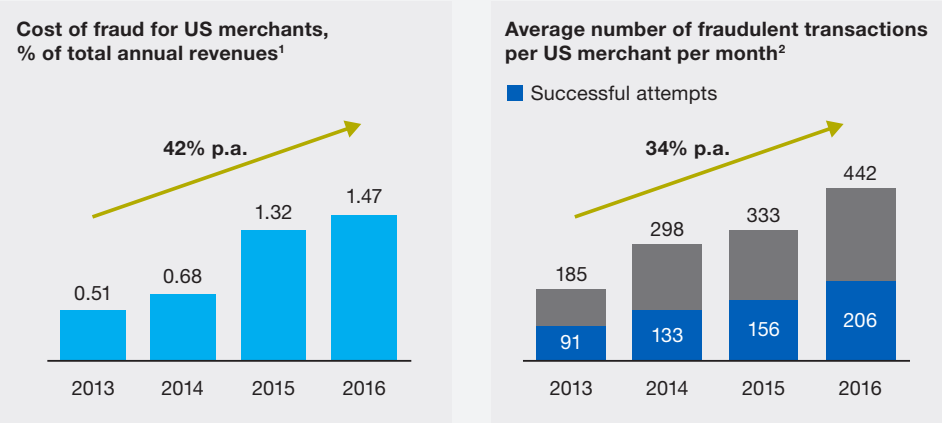
Source: The Nilson Report, 2017

As card-chip technology matures, new digital channels emerge, and fraudsters become more adept and collaborative, the nature of financial fraud is rapidly evolving. Debit cards and alternative payments channels, such as mobile payments, are experiencing higher fraud rates. Both physical and online transactions are under pressure to control fraud as incidence rates climb sharply in mobile channels. And the complexity of cyber attacks—often initiated by malware, and inert for long periods before they are activated—is growing.

At the same time, shoppers are shifting to mobile and online channels and sellers are trying to keep up by expanding their market footprints. Meanwhile, attacks and breaches are intensifying. Criminals have become more specialized and are using social networks to recruit and train others and coordinate fraud efforts. Phishing emails continue to find ways to persuade customers to click on links that then use malware to collect consumer data, including PIN numbers and other authentication information used in online shopping. As quickly as banks and companies strengthen vulnerabilities, criminals find new areas of weakness to attack. Vigilance and fraud management are neverending tasks.

Exhibit 2

US merchants' fraud costs have soared in the past few years.



[1] Weighted merchant responses to question: "What is the approximate dollar value of your company's total fraud losses over the past 12 months?"

[2] Weighted merchant responses to question: "In a typical month, approximately how many fraudulent transactions are prevented by your company/successfully completed by fraudsters?"

Source: "LexisNexis 2016 True Cost of Fraud," LexisNexis

In e-commerce, where the customer's online experience is critical, providers face tough choices when seeking to improve their fraud management. Tools and processes such as authentication can be detrimental to the customer experience and to a seller's net promoter score (NPS), a key success indicator for many. Not only can fraud-prevention measures prove frustrating for customers, they can be expensive for companies: at some call centers, as many as 10 to 15 percent of calls are prompted by authentication issues or password resets.

In addition, as authentication becomes more sophisticated and transaction fraud becomes more difficult, the account-opening part of the value chain becomes more critical, creating a need for more robust customer onboarding processes. Most large e-commerce providers have reinforced their defensive capabilities and are better able to repel large-ticket attacks. However, the volume of small-ticket attacks, which often fall below automatic thresholds for detection, continues to rise sharply, especially for small and medium-sized merchants. As chip cards become ubiquitous, financial institutions will continue to push chargeback rates that shift more liability to e-commerce merchants, forcing them to enhance their fraud detection and recovery capabilities.

Building value with leading-edge fraud management

A few companies that have adopted state-of-the art fraud management tools and techniques have been able to improve their fraud detection rates by 15 to 20 percent and reduce false positives by 20 to 50 percent—while typically improving their customer satisfaction scores by 1 to 2 points at the same time.

Companies can enhance their fraud management efforts by taking three steps: employing advanced analytics, re-engineering fraud case management, and improving the customer experience.

1. Employ advanced analytics

Some leading providers are already taking advantage of advanced analytics to enhance their fraud detection toolkit. That might involve drawing on alternative data sources—such as social media, phone usage data, and purchasing history—or using information about a customer's location and device type to help validate the authenticity of a transaction. But across the payments sector as a whole, the use of advanced analytics is still in its infancy.

Advanced analytics techniques can dramatically improve the effectiveness and efficiency of fraud management. The integration of high-quality data sources (such as digital communications, geospatial data, and satellite imagery), the use of more sophisticated modeling techniques (such as machine learning, deep learning, and natural-language processing), and the introduction of automation technologies (such as natural-language generation and cognitive-computing algorithms) are transforming the way companies approach risk management. Where once fraud was detected by risk functions flagging suspect transactions for manual review, firms can now use neural networks based on unsupervised and supervised architectures (such as pattern analysis and classification, respectively) to monitor dubious activities.

The enormous potential of advanced analytics to improve fraud management is best illustrated through examples. While shifting to a no-branches model, one large retail bank discovered that half its account applications were being rejected, and many more prospects were dropping out of the application process. In fact, only 16 percent of prospects got as far as opening new accounts.

Seeking to resolve the problem, the bank engaged a fintech to design a system that draws on data from a range of external sources such as eBureau, FIS, Junio, and Emailage to perform live customer-risk assessments. These assessments dynamically trigger questions that customers answer as part of their online application. In its first three months of use, the new system increased acceptances by 60 percent and reduced manual verification by 10 percent, while incurring no increase in fraud losses.

In another example, a leading UK bank was able to recover 95 percent of estimated value loss from fraud after introducing machine-learning platforms with the support of QuantumBlack, an advanced analytics specialist. Having partnered with a top payments-infrastructure provider to access all payments associated with the bank's customers, QuantumBlack combined this data with data on fraudulent transactions previously identified by the bank, and analyzed the results using proprietary algorithms. This allowed it to create a fraud-risk score for each transaction. Fraud cases identified by the model represented 86 percent of incidences and 95 percent of fraud-related losses. The bank now has a live tool to identify and prioritize cases for further investigation.

2. Re-engineer fraud case management

The growing sophistication of fraudsters means that focusing prevention efforts disproportionately on one channel can lead to vulnerabilities elsewhere—the "squeezing a

balloon" effect. A better way to prevent losses is to adopt an integrated fraud strategy across all lines of business and transaction types, with a consistent set of fraud-prevention policies, limits, and thresholds across all channels.

Leading businesses are pursuing digital approaches to enable next-generation fraud management, implementing visual monitoring, and using alerts from unified data flows to guide live decisions. Lean management, robotics, and other tools can be integrated into these systems to increase speed, reliability, and customer satisfaction while reducing cost and errors. For example, companies that redesign their payments-dispute process from scratch using lean principles have been able to dramatically simplify the customer experience and increase productivity at the same time. (See "Payments disputes: A pathway to deeper customer relationships," *McKinsey on Payments*, October 2017.)

One major US bank decided to re-engineer its fraud case management after suffering losses above the industry average. Part of the problem lay in its highly fragmented fraud organization, which made it difficult to measure fraud losses and attempts across the whole business. In addition, the bank's technology systems were split along business lines, meaning there was no comprehensive view of customers across all products and channels.

To tackle the fragmentation, the bank decided to develop a consistent enterprise-wide fraud-prevention strategy, consolidate fraud management into a single team, and create shared services based on skill sets. It enhanced fraud reporting by using a dashboard to track effectiveness metrics and fraud loss across all business lines, and by setting up regular summits to discuss results from the dashboard and other prevention measures. These improvements in reporting and parameter-setting gave the bank a full view of fraud losses and fraud-prevention performance across all channels and products, and helped it reduce fraud by 25 percent.

A leading global payments company that had managed to grow its digital transactions by 30 to 40 percent found that its success had put a strain on its ability to quickly identify suspect transactions and approve or decline them. Costs were being wasted and customers were annoyed when transactions were put on hold for no good reason. The company assessed customer and employee pain points, identified waste in processes, and scrutinized performance variations before revising processes to reduce handling times, eliminate handoffs, and increase responsiveness to customers. Through this comprehensive effort, the company achieved a productivity increase of 50 percent—a result that prompted it to expand the transformation to include operations, risk and compliance, and sales.

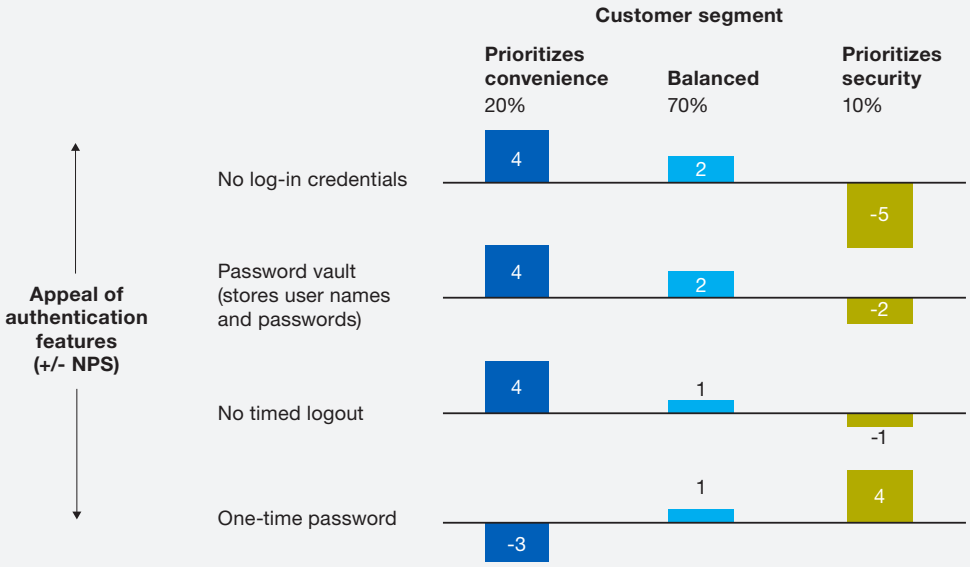
3. Improve the customer experience

As fraud prevention and detection measures grow more powerful and complex, they can also become more detrimental to the customer experience. A 2017 survey of over 4,000 banking customers carried out by McKinsey's Cyber Solutions Practice revealed that less than half were satisfied with both the security and the convenience of digital offerings.

E-commerce players need to think about authentication, fraud management, and customer experience simultaneously, not individually, as they are often treated today. Poorly designed authentication experiences have a disproportionate impact on

Exhibit 3

Different customer segments place different values on account authentication features.



Source: McKinsey Payments Practice

customer engagement, fraud mitigation, and operational efficiency. The same McKinsey research shows that among the customers who register for online accounts, around 20 percent never manage to log in, citing "password" and "authentication" as the main reasons.

Authentication and the decline of a transaction can be moments of truth for customers, and companies' need to adopt more robust customer onboarding processes puts account opening under particular pressure. That means companies need to address not only how effective they are at preventing disruptive events such as nonfraud card declines and locked accounts, but also how they can turn a fraud-related interaction into a better experience for the customer.

Making this happen will require the careful crafting of follow-up communication and a well-designed value proposition for monitoring and identity protection.

Our research shows that customers do not value security and convenience equally, and that different types of customer have different expectations of control, transparency, security, and convenience in their e-commerce journeys. We identified three main customer segments: those who value security over other factors, those who value convenience, and those who value a balance between the two. Having an automatic timed log-out increased satisfaction for customers who value security, but reduced it for those who value convenience, for instance (Exhibit 3). The key to success is to deploy flexible,

tailored authentication experiences to meet the specific needs of each customer segment.

By redesigning customer journeys, a company can rapidly uncover short-term opportunities to deliver impact as well as draw up a long-term roadmap to differentiate experiences, reduce fraud, and lower costs. One bank studied how different segments of customers feel when faced with a transaction denial. Building on its findings, it introduced new ways of handling transactions flagged as potentially fraudulent. Some customer segments were sent a mobile alert and could simply swipe to confirm the transaction as authentic; in other cases, small transactions that would previously have been denied were approved with a follow-up email confirming the transaction with the customer. This solution not only reduced lost sales and cut the cost of fraud management, but also increased overall customer satisfaction.

By redesigning fraud management using similar approaches, some businesses have increased digital usage by 10 to 20 percent, largely by making authentication painless for the customer. Other benefits include halving fraud incidents and increasing the value recovered from them by 95 percent.

Implementing an integrated approach

These three initiatives are essential to next-generation fraud management, but not sufficient. A comprehensive approach requires multiple interdependent steps to be implemented together. These include:

- Defining target data models that include internal sources (combining data across product silos) and external sources (using data beyond the bureau, such as device, biometric, and social data)
- Redesigning process controls for account opening, transaction initiation, and other customer journeys
- Developing an advanced vendor approach by creating a "fraud lab" for testing new technologies and data sources as fraud continues to evolve, and correlating fraud-prevention technologies to optimize coverage
- Refining the risk-management framework and policy for fraud, including defining fraud-loss tolerance at a granular level to align with business strategy and overall risk appetite.

* * *

Better management of card fraud not only reduces losses and processing costs for payments providers, but offers opportunities to improve the customer experience through a deeper understanding of how different segments value security and convenience. Businesses that adopt the leading-edge practices outlined above can protect themselves against increasingly sophisticated forms of attack and boost customer loyalty, engagement, and value at the same time.

The next issue of *McKinsey on Payments*—a special issue on advanced analytics—returns to the subject of payments fraud with an article on new technological tools and approaches for fraud prevention.

Robert Hayden, a senior expert in McKinsey's Cleveland office, passed away last month. Please see page 4 for a remembrance of Rob. **Lindsay Anan** is a consultant and **Marie-Claude Nadeau** and **Jonathan Steitz** are partners in McKinsey's San Francisco office; and **Kaustubh Joshi** is an associate partner in the New York office.