Managing Fraud Risk in the Digital Age
People, processes and technologies to address the emerging risks of online and mobile payments
Contents

With convenience comes new risk................................................................. 1
Stronger authentication, not more authentication ........................................... 1
Threats along the way ...................................................................................... 2
Four steps to fighting back .............................................................................. 3
  1. Determine your organization’s fraud risk appetite ..................................... 3
  2. Put the right people and policies in place ............................................... 4
  3. Get ahead of the regulators on authentication ......................................... 4
  4. Implement strong anti-fraud tools and technology ................................... 5
Capitalizing on anti-fraud analytics ............................................................... 6
Closing thoughts ............................................................................................ 7
Learn more ..................................................................................................... 7
With convenience comes new risk

In the past, consumers used cash, checks and/or credit, debit or prepaid cards to pay for their purchases. They also used money transfer services such as ACH and wire payments, which had a delay in the settlement allowing more time for investigation. Those days are becoming a distant memory as more and more consumers embrace – and expect – the speed and convenience of digital payments, either online or from mobile devices.

New digital methods are reinventing the payments ecosystem. Payment applications such as Google Pay make it quick and easy to move money around the market and across borders. As more and more retailers are adopting various forms of digital payments, they have forced banks and financial entities to adopt alternative payment options. For example:

• By January 2017, 25 percent of all card transactions in the UK were made with debit and credit cards that use radio-frequency identification or near field communication to make fast, convenient payments.¹

• In the US, mobile wallet transaction volume is expected to grow more than five times from 2015 to 2019. More than a quarter of US consumers have used at least one mobile person-to-person payment service, with $44 billion transferred in 2015.²

• During the 2016 Christmas shopping season, consumers in the UK used digital payment methods to make 325 million purchases totaling £2.9 billion (about US$3.7 billion) in a single month – up 184 percent from a year earlier.³

• In India, 76.4 percent of consumers have used a smartphone to make a purchase, up nearly 30 percent in one year.⁴

The new ease and speed of digital payments make it more likely for a consumer to make a purchase – a win for the business and the financial institution. But this convenience brings new opportunities for fraudsters, which in turn presents new challenges for fraud mitigation.

Stronger authentication, not more authentication

Traditional card payments were vulnerable to several fraud tactics, such as counterfeit cards with magnetic strip data and BIN attacks, where an actual Bank Identification Number is used to generate many fraudulent credit card numbers.

The financial services and retail industries have made great progress in hardening the defenses against these forms of fraud. Once device manufacturers supported the integration with NFC, mobile devices provided an additional avenue for ease of payment over and above what was supported with just a plastic card.

¹ Source: UK Cards Association
² Source: Javelin 2016 Digital Channel Threat Report: Derisking Convenience
³ Source: UK Cards Association
⁴ Chanchani, Madhav, March 7, 2016, “Amazon India planning launch of digital wallet in a bid to build online payments business” - via The Economic Times
However, it becomes more necessary – and more complex – to authenticate users. How do you certify a user’s identity without causing delay in the convenience consumers are seeking?

The answer is not more authentication, but stronger authentication. For example:

- **3D Secure authentication and security protocol**, becoming more widely adopted by online merchants, helps protect online purchases made with debit and credit cards.

- **One-time passwords** generated from a standalone application, device or mobile phone strengthen the “what you know” element of authentication.

- **Biometric security measures** – which recognize something unique to the user, such as eyes, voice or fingerprint – take the “what you have” dimension of authentication to a new level and prevent unauthorized access to mobile payment devices.

- **Tokenization** substitutes a sensitive data element in the transaction with a non-sensitive equivalent, a token that has no extrinsic or exploitable meaning or value.

These authentication measures increase security without impeding the flow of the customer experience. Fraud exposure is minimal if the mobile wallet has been appropriately established. However, despite these advances in authentication, fraud continues to rise, due to vulnerabilities beyond the transaction itself.

**Threats along the way**

Looking beyond the digital payment transaction itself, financial institutions also need to recognize the ancillary risks that could invite fraud in other forms. For example:

- **Open banking**. Starting first in Europe, open banking is intended to stimulate competition and innovation in banking services, such as enabling third parties to initiate payments from customer accounts, provide financial advice or complete tax returns – with customers’ permission of course. However, questions remain about the potential for data leaks and the boundaries of responsibility if a data breach does occur.

- **Digital account opening**. Many customers want to open accounts online or on a mobile device rather than by telephone or in person in a branch. The anonymity of this channel opens the door for application fraud. Automated tools make it easy to attempt thousands of faceless applications per day. Financial institutions may find themselves processing applications for customers who don’t even exist.

  Some banks are delivering a smoother and easier application experience by using electronic know your customer (KYC) and identification and verification processes, often capturing biometric data – fingerprint, voice signature or eye map, for example – for subsequent authentication.

- **Cybersecurity**. Cyberattacks happen daily, but only a few are caught and reported in the news. We can certainly expect that attacks against banks, merchants and customers will continue to grow in volume and sophistication. Cyber criminals are
well organized and funded. Success breeds ever greater ambition and audacity. Although not directly a fraud risk, a loss of sensitive data often leads to fraud attacks and losses.

- **Internet of Things (IoT).** The IoT introduces an as-yet-unknown set of fraud risks, especially when potentially insecure devices are empowered to trigger automatic purchases or used to access or store personal or payment data that could be intercepted or hacked. The customer experience of searching, selecting and paying for daily retail purchases introduces many opportunities for fraud exposures.

### Four steps to fighting back

1. **Determine your organization’s fraud risk appetite**

   Does your organization’s leadership understand the risk environment? Have they agreed and articulated how much risk the organization is willing to take? For a typical enterprise, the goal should be threefold:

   - Low fraud losses - comparable to or better than peers.
   - High level of customer service - frictionless access, rare false alerts.
   - Optimal operational efficiency and effectiveness – effective fraud processes.

   Once objectives are articulated, you can set measurement criteria to monitor performance against them:

   - Fraud losses are likely to be based on market share data or fraud/sales ratios, benchmarked with country or regional peers.
   - Customer service metrics could include acceptance rates for account opening and transactions, low log-on failures, call center metrics, customer complaints and feedback.
   - Operational performance can be compared with industry data and benchmarking on such measures as cases worked per hour, false positives at various detection rates and fraud recovery rates.

   It is an optimization exercise, because you can’t have premium levels of all three. The ease and convenience that satisfy customers could result in higher fraud losses. Tighter application or authentication processes can end up frustrating customers with lock-outs and false fraud alerts.

   Fraud managers are very much aware of the need to balance fraud losses with customer experience and operational overhead. Business managers and marketing teams, on the other hand, often underestimate or fail to appreciate the fraud risks and become carried away with the excitement of a new product or service launch. The temptation in the rush to market is to remove or down-scope some of the fraud controls.

   It is essential to have a good working partnership with the business to secure the investment and IT resources to implement fraud controls. And it is essential to have a working partnership with IT to collaborate on technology approaches that will fit with the organization’s overall IT architecture and strategy.
2. Put the right people and policies in place

People. Since fraud management is very much a technology issue today, teams will require people who understand data and analytics but are also versed in investigative techniques and technologies. And it needs people who can scan the landscape to anticipate and understand emerging risks that accompany new initiatives.

Staffing an analytics-driven fraud task force is easier said than done. Demand for analytic talent is so great that good candidates are hard to find and harder to hire. Nearly one-third (32 percent) of respondents in an ISMG survey said their organizations still lack the in-house expertise to properly detect and respond to fraud. Looking to boost expertise from the inside, 94 percent say combating financial crime is a top training priority for their bank, according to Longitude Research.

Policy. An airtight fraud policy sets forth minimum standards regarding the end-to-end fraud prevention process, including:

- Customer authentication.
- Wallet provisioning.
- Real-time fraud protection.
- Transaction monitoring.
- Identification and verification.
- Reporting and management information.
- Fraud case review.
- Root cause analysis.
- Investigations and recovery.
- Machine learning feedback loop.

3. Get ahead of the regulators on authentication

The 3D Secure 2.0 initiative will force adoption among online merchants. This risk-based capability will help those who have struggled to balance protection with convenience. Nobody wants the liability of a fraudulent transaction, but is it worth inconveniencing customers by putting them through stringent authentication each time they visit?

However, even where 3D Secure has been adopted, fraud has continued to rise, and card-not-present fraud is now the most prevalent fraud type, representing an estimated two-thirds of account losses globally. As a result, regulators are taking a hard look at fraud risk. Mandates for authentication were first put in place in India and Singapore, and the European Central Bank (ECB) is contemplating a requirement that all e-commerce transactions be authenticated – a step that many in financial services see as unnecessary and unfortunate.

The real question is, can the industry move fast to improve the way it manages online fraud so regulators won’t impose their own requirements?

---

5 Information Security Media Group (ISMG), 2016, Faces of Fraud: The Analytics Approach to Fraud Prevention

6 Longitude Research, 2016, Combating Financial Crime: The Increasing Importance of Financial Crimes Intelligence Units in Banking
4. Implement strong anti-fraud tools and technology

Best customer service. Lowest fraud rates among peer banks. Optimal operational overhead. Balancing those three priorities requires analytics-driven tools and technologies that are:

- **Comprehensive.** The fraud technology should span account opening, transaction monitoring and network analysis, with broad data sharing and supported by analytics-driven rules and models.
- **Real-time.** Once a nice-to-have, real-time transaction monitoring is now a requirement for both traditional and new payment types. Ideally, a system will monitor all transactions, both monetary and non-monetary.
- **Cross-channel.** Now that customers have more choice in how they transact, it is more important to have a single and versatile fraud solution for all contact channels – internet, telephone, mobile, digital and in-person – to gain a holistic customer view.
- **Cross-payment.** Anti-fraud mechanisms should provide a consistent and unified view across checks, debit cards, credit cards, ACH, wire transfers, deposits, merchant transactions and digital/online payments.
- **Enterprisewide.** The 360-degree customer view created by an anti-fraud system can also add value for anti-money laundering (AML), credit risk management, marketing and sales efforts. Activities that look innocuous by themselves can appear suspicious when seen in broader context.
- **Open for integration.** Chartis Research says that “a key differentiator is the openness and flexibility of the technology architecture and a ‘tool-kit’ approach to risk analytics and reporting.”

Given the extent of legacy systems in many organizations, achieving these core capabilities could be a difficult proposition, but the benefits in fraud reduction and operational and IT cost savings will surely be worth the investment.

---

**Payments fraud, in the past simply managed as bad debt, now receives the attention it rightfully deserves.**

---

**Anti-Fraud Essentials**

In addition to the basic attributes – end-to-end, real-time, etc. – here are the top must-haves retailers and financial institutions should look for in an enterprise fraud solution:

- **Transaction monitoring with rules and optimized models** working all transactions in real time, ideally with a vision to move to a single customer view.
- **Geolocation capability and device ID analysis** for mobile and digital banking.
- **Network and link analytics** for detecting collusion and trade finance fraud and for supporting AML analysis and investigations.
- **Integrated alert management**, accessible across the enterprise to support triaged alerts and investigations for all financial crimes.
- **One-time passwords or biometrics** for strong customer authentication.
- **Data visualization** for at-a-glance identification of potentially suspicious events, activities or connections.
Capitalizing on anti-fraud analytics

Payment providers are always seeking that optimal balance between reducing the false positives that can cause unnecessary customer friction and the false negatives that can lead to financial loss. Getting it right requires analytics – the predictive ability to detect anomalies that represent potential risks, while the customer is waiting.

Here we get a little technical into concepts that must be understood to launch a strong defense against fraud. Beyond the basics, a powerful anti-fraud platform for the digital age includes the following capabilities:

• **A decision hub.** A central decision hub approach assesses activity at multiple levels, combines multiple analytical approaches and provides a unified view of an account/entity across the entire relationship.

• **Analysis of nonmonetary events.** In-session behavior can reveal a lot about a user. Most online/mobile users have regular patterns of engaging with merchants and financial portals. They use similar navigation patterns and a small number of devices. Departures from habit could signal unauthorized access. A strong authorization system can capture user behavior patterns from multiple sources and evaluate them every time a payment transaction is scored. We call this a “signatures” approach.

• **Hybrid analytics.** When you layer multiple analytics methods, you can more accurately distinguish between legitimate users and fraudsters. For example, anomaly detection and predictive analytics can uncover new forms of risk by examining what’s happening right now, not just comparing it to the past. Link analytics can establish connections that point to collusion or discrepancies that represent potential red flags or even organized crime. And self-learning techniques (see below) take fraud detection to the next level by adapting criteria as things are happening.

• **Machine learning.** Unlike rules-based systems, which are easy for fraudsters to test and circumvent, machine learning adapts to changing behaviors in a population through automated model building. With every iteration, the algorithms get smarter and deliver more accurate results. It’s easy to see the value of machine learning to keep pace with the emerging risks of new payment channels.

• **Custom data integration.** There are countless different ways to transform, enrich, validate and store the data collected from transactions – which come in many formats from different sources. The fraud platform should enable you to define your own path for how each customer transaction is transformed and enriched, validating the incoming transaction before sending it to the fraud management system. SAS calls this an “orchestration layer.”

• **Alert management.** The system should intelligently prioritize alerts for triage, investigation and disposition. Investigators need to quickly see potential areas of interest and where to focus first. Expect the capability to easily manage alerts and events with a scenario-fired event model and scenario context.

• **Integrated case management.** A common case management system will facilitate collaboration and intelligence sharing, as well as end-to-end case tracking and auditing. The right platform frees up staff by automating processes that have traditionally been manual and prioritizing the highest-value cases. Investigative staff spend less time dealing with the data and more time investigating and taking action on meaningful alerts.
Closing thoughts

Industry leaders from the banking, retail and fraud solution vendor landscape are working to streamline the customer experience with online and mobile payment options, while closing the opportunities for fraud and exposure. Balancing security and convenience requires an approach that combines consumer-facing authentication (such as passwords, PINs and biometrics) with background security measures (such as user and session-behavior analytics).

The investment is not trivial, but the returns and gained brand confidence are worth it.

Learn more

For more about SAS® Fraud Management: sas.com/en_us/software/fraud-management.html