McKinsey on Payments

Special Edition on Advanced Analytics in Banking

Volume 11 Number 28 August 2018

Combating payments fraud and enhancing customer experience

The fraud threat facing banks and payments firms has grown dramatically in recent years (Exhibit 1). Estimates of fraud's impact on consumers and financial institutions vary significantly but losses to banks alone are conservatively estimated to exceed $31 billion globally by 2018. Several converging trends have propelled the increasing scale, diversity, and complexity of fraud. Vulnerabilities in payments services have increased as the shift to digital and mobile customer platforms accelerates. New solutions have also led to payments transactions being executed more quickly, leaving banks and processors with less time to identify, counteract, and recover the underlying funds when necessary. Finally, the sophistication of fraud has increased, in part through greater collaboration among bad actors, including the exchange of stolen data, new techniques, and expertise on the dark web.

Salim Hasham
Rob Hayden
Rob Wavra

Increasingly agile fraud perpetrators have benefited from banks' and payments firms' limited ability to adapt. While most institutions have well-funded anti-fraud groups, key resources are often fragmented across the organization. Essential data, investigative and forensics expertise, and analytics talent are typically distributed across cyber, compliance, legal, IT, and fraud teams, with little to no coordination or data sharing.

Effectively combating fraud through analytics requires a mindset shift from a narrow focus on false positives and loss prevention to an appreciation that the same technological advancements making fraud more pervasive also enable the tools and environment to address it. With their shift to digital services, banks have access to exponentially more customer and transaction data than in the past. New technologies create the means to more accurately segment customers by risk, enabling lower-friction digital experiences—and higher satisfaction levels—for low-risk customers. And the explosion of industry verticals in cyber and data analytics has created a ready supply of talented, cross-disciplinary resources unencumbered by legacy organizational structures. Today's challenge is harnessing these components to reduce current losses, detect and prevent emerging fraud, and enhance customer experience.

The shifting fraud landscape

Fraud is not only growing but evolving (Exhibit 2, page 22), forcing countermeasures to shift from the transaction-centric assessment of fraudulent charges on a card or doctored checks deposited at an ATM, to preventing, detecting, and remediating increasingly sophisticated, long-term sleeper frauds and exotic concerns like manipulated synthetic identities. Some tactics have worked, with Visa estimating that chip technology reduced counterfeit card fraud in the US by 66 percent for EMV-enabled merchants in June 2017 compared to June 2015. Other typologies ("abuse cases") of fraud remain without effective countermeasures, straining traditional

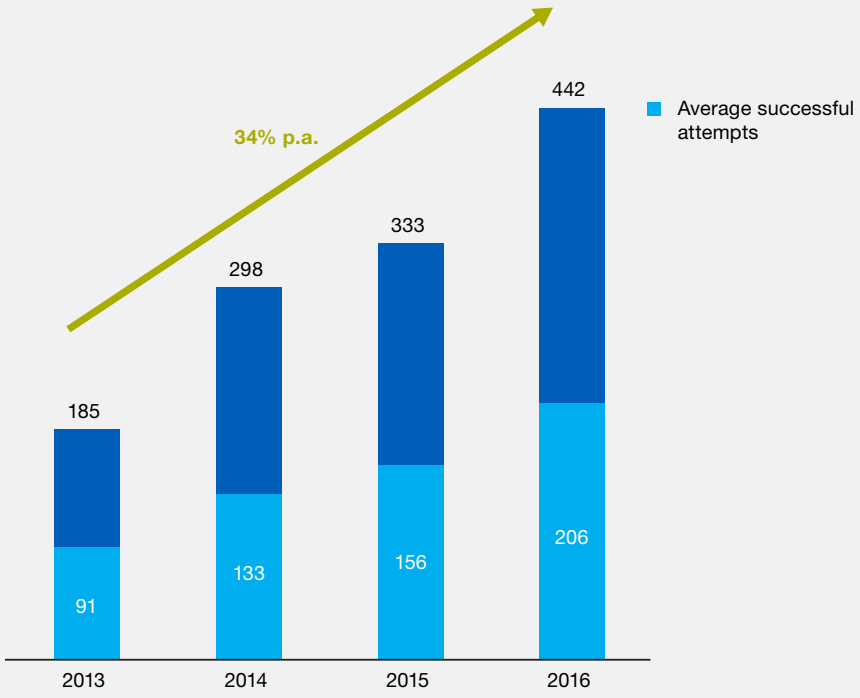
anti-fraud efforts, generating increasing losses, false positives, and negative customer experiences:

- **Account takeover** (ATO) is the theft or misuse of credentials to fraudulently gain access to an existing customer account. This can be a one-time funds transfer event or an ongoing access exploitation (e.g., adding a registered user, changing the contact email or mailing address) for criminal purposes. Successfully combatting ATO requires a mix of nontraditional data sources that expand customer identification beyond knowledge-based authentication (KBA), analytics to detect emerging trends and high-risk access events, and customer experience-sensitive authentication journeys, limiting customer challenges based on risk segmentation and other triggers.
- **Synthetic identity,** a scenario in which fraud perpetrators combine fragments of stolen or fake information to create a new identity and apply for financial products, is

Exhibit 1

Fraud is on the increase in the US.

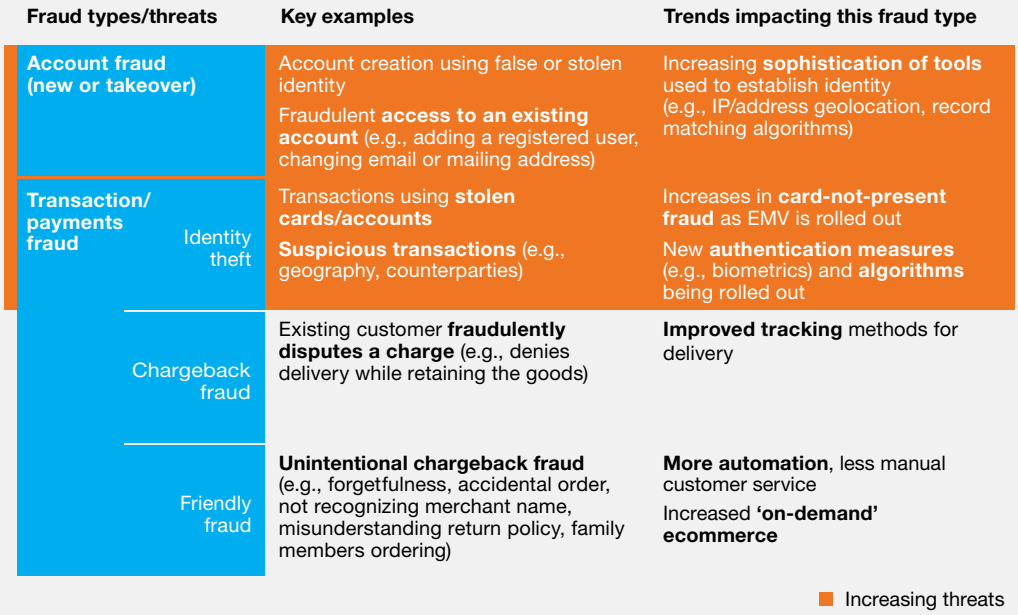
Average number of fraudulent transactions attempted per merchant per month[1]



[1] Weighted merchant responses to LexisNexis survey question: In a typical month, approximately how many fraudulent transactions are prevented by your company / successfully completed by fraudsters? What is the average value of successful fraud transactions?
Source: US Department of Commerce; LexisNexis The True Cost of Fraud study, 2016

Exhibit 2

Payments transaction fraud takes many forms.



Source: McKinsey analysis

of growing concern in light of data exposed through the 2017 Equifax breach. All of synthetic identity fraud's forms—traditional (a fusion of valid information from multiple real people), manipulated (all real information about a single person with a fake national ID/SSN), and manufactured (wholly fake information, including national ID/SSN)—can exist only because of inadequate onboarding and customer due diligence. Filling these gaps will require cross-functional collaboration across lines of business and functional silos, expanded external data for validating multiple elements of customer applications and scoring their likelihood of authenticity, and the fusion of these external sources and existing internal customer data.

- **Business email compromise** invokes social engineering to lure an empowered employee to initiate a transfer to the fraudster's account, usually at the apparent request of an executive. A similar phenomenon, *invoice redirection*, leverages social engineering to alter payment information for legitimate payables accounts (often by claiming a new bank account has been opened), redirecting payment to a fraudster's account. These are growing fraud categories—business email compromise alone causes nearly $1.5 billion per year in losses according to the FBI—demanding institutions respond with tailored frontline training, re-architecture of existing controls (e.g., who can change payment information and based on what informa-

tion, verification of new information with a known contact), sophisticated analytics to flag risky changes before payments are made, and new data and technologies like voice analytics.

In "Fraud management: Recovering value through next-generation solutions" (*McKinsey on Payments,* June 2018), our colleagues identified three concrete steps to effectively redefine fraud operating models to fight these emerging threats: re-engineering fraud case management; redesigning journeys to improve the customer experience; and employing advanced analytics. Given the vast potential of advanced analytics in the fraud arena and the significant barriers to its effective use, we will focus on this critical dimension. When done well, analytics can consistently reduce fraud losses by 3 to 5 percent in mature environments and by over 30 percent in evolving contexts. And yet we have seen even the most advanced firms struggle to attract and maintain analytics talent, transcend organizational and disciplinary boundaries to deploy the best solutions, and transition from analytics test cases to production capabilities.

False starts

In the face of the continuous evolution and increasing pace and volume of fraud threats, fraud teams find themselves hamstrung by ineffective triage of alerts, poor data quality, and non-existent or outdated intelligence. Compounding this fragmentation, many investments in fraud-related artificial intelligence can be characterized as "science projects," lacking the scale to deliver enterprise impact. In the meantime, institutions are dedicating additional resources to manually wade through low-value alerts or building increasingly aggressive rules and models that often hurt customer experience more than they mitigate fraud.

Fraud interventions driven by advanced analytics tend to follow a few archetypes:

- *Predictive detection, encompassing user authentication* (e.g., determining whether the transacting party is in fact a customer), customer due diligence (e.g., low/high-risk fraud profiling as a factor in exception decisioning), and transaction risk (e.g., whether hallmarks of fraud are present in the context of other transactions for the account, customer, and household). This can come in the form of in-house custom analytics models, commercial off-the-shelf software-enabled detection, or public partnerships with emerging technology companies, like HSBC's relationship with Ayasdi.
- *Enhanced internal process efficiency*, such as capacity forecasting and providing analysts with context detailing the reasons a transaction failed an initial screen.
- *Automated fraud triage and other robotic process automation (RPA).* The London School of Economics examined 16 case studies of RPA, finding first-year returns on investment of 30 to 200 percent. The longer-term value—including enhanced compliance and the reallocation of employees to higher-value tasks—is likely even greater.

Many banks, however, have faced serious challenges when attempting to effectively integrate advanced analytics into their fraud defense. Common pitfalls include:

- Building models that do not take advantage of all available data, overlooking siloed risk scoring inputs residing in cyber, customer relationship and product sales groups.

Such inputs can be as simple as determining whether cross-ownership of mortgage or card products correlates to lower fraud risk or exploiting device geolocation data to inform mobile deposit fraud screening—which enabled a US bank to identify deposits typologies with higher fraud incidence of 25 to 1,000 times. More ambitious enhancements include holistic realignment of a bank's financial crime structures, people, and technology, as undertaken by HSBC in 2015 with its creation of a unified Financial Crime Threat Mitigation organization.

- Deploying "crime- and institution-ignorant" models, which are statistically compelling but hobbled by a lack of understanding of underlying fraud mechanisms, institutional controls, and intervention options. While staffing fraud analytics efforts with cross-disciplinary teams of data scientists, data engineers, translators, and financial crime and fraud subject matter experts is a powerful solution, Citigroup went one step further, empowering a permanent Global Investigations Unit to proactively analyze and combat emerging financial crimes with a full range of experts and technical staff.
- Not addressing the growing model risk management (MRM) demands in fraud mitigation. The increasingly opaque and sophisticated models used to detect fraud and the rapid pace at which fraud is evolving combine to create model risk. Some causes are easily addressable—assumptions about the markers of fraud and the scale of potential losses can become strained—but others stem from well-meaning attempts to use cutting-edge deep learning and neural network algorithms which are difficult, if not impossible, to interpret. Techniques like Locally Interpretable Model-Agnostic Explanations (LIME) provide some insights into sophisticated models, but do not mitigate the increased model risk that the push for performance and innovation has created.
- Not accounting for the increasing interest of regulators in fraud models. This scrutiny is likely to accelerate, given the opaque nature of fraud rules and concern over whether they impose disparate impact on members of a protected class. Loss ratios and raw statistical performance cannot be the only metrics by which modern fraud models are measured.
- Grafting advanced analytics tools onto existing processes and policy frameworks rather than leveraging analytics to transform the business. Analytics should not be deployed merely to dig out of a false positive hole created by bad policies and inefficient processes. While many frauds are driven by control weaknesses, fast-growing threats like synthetic identity fraud exist only because of insufficient onboarding processes and customer due diligence at the application stage. Using advanced analytics to detect these frauds or reduce false positives being generated misses the real opportunity to fix outmoded policies and underperforming processes.

The best analytics interventions leverage cross-disciplinary expertise, fusing analytics with deep industry and client organization context. At a regional bank in the United States, the breakthrough came from shifting its focus from identifying fraudulent transactions to minimizing dollar losses from a specific fraud typology. Pairing this approach with risk-

Accelerating analytics-driven fraud defenses

"Money mule" accounts are often recruited via unwitting accomplices (e.g., through work-from-home schemes) and exploited to launder illicit funds, rapidly moving sums through multiple accounts to obfuscate sources and frustrate identification and repatriation efforts. Advanced network analytics and machine-learning techniques can discern patterns in the noise, exposing suspicious accounts with impressive efficacy. For instance, QuantumBlack, a McKinsey company focused on advanced analytics, analyzed over 18 billion transactions across multiple banks, creating a "mule-inesque" score integrating indicators of mule activity (e.g., account age, economic relationships, direct debit frequency). QuantumBlack analyzed over 10,000 suspected criminal account networks through an investigator analytics support tool, visually tracing dispersion networks to allow for real-time detection and timely repatriation. The exercise ultimately identified 15,000 mule accounts across multiple banks.

Although signature fraud has been a common tactic for generations, it has taken on new dimensions in certain markets. A bank in Latin America was overwhelmed by both traditional loan application fraud (e.g., for recently deceased relatives) and "auto-fraud," where an applicant intentionally modifies their own signature with the intention of later claiming not to have initiated the loan. Using deep learning-based image analytics techniques, McKinsey identified the subtle indicators of both types of fraudulent signatures. The new model improved fraud detection by over 31 percent when compared to the bank's existing model.

driven policy changes and data science-driven enhancements to tune their detection model, the bank was able to create a combination of model enhancements and policy change efforts projected to reduce annual losses in the target category by over 32 percent.

Succeeding in fraud analytics

Effectively deploying analytics to combat fraud requires a shift in thinking from a narrow focus on false positives and losses to an appreciation that the same trends making fraud more pervasive also enable the tools and environment necessary to combat it. With their shift to digital services, banks have exponentially more customer and transaction data than in the past. New technologies also create the means to more accurately segment customers by risk, enabling lower-friction digital experiences—and higher satisfaction levels—for low-risk customers. Many of the technological advances that have sped the pace of payments can also be leveraged to increase the speed and efficiency of anti-fraud processes. And the explosion of the cyber and data analytics verticals has created a ready supply of talented, cross-disciplinary resources unencumbered by legacy organizational structures.

Analytics provide a unique and powerful means to transform fraud operations. The most successful fraud analytics programs are designed to be:

- **Business-back:** Anti-fraud analytics efforts must be built on a unified, cross enterprise foundation, breaking down silos between channels, products, and fraud types. This is usually best accomplished with an overarching fraud operations transformation mandate from senior management, transcending analytics. Given the increasing impact of fraud on bottom lines and reputations, the business case to secure such a broad mandate should be fairly straightforward. The goal should be

a process seamlessly integrated across the fraud lifecycle, incorporating data spanning business units and functional silos to create a holistic view.

- **Criminal-forward:** Applying a criminal mindset to fraud analytics—a common tactic used by law enforcement agencies—can provide inputs to better understand the motivations and methods of perpetrators of fraud. From this starting point, models can be designed to predict, prevent, and detect crime based on powerful data-driven insights and expert-created indicators created from more nuanced and comprehensive understanding of the criminal. By mapping typologies to indicators of fraud, analytics can be better targeted and prioritized. Such a focus requires more than just fraud experts and data scientists; it demands a rigorous, evidence-based method to testing expert hypotheses with large data sets on past fraud and a culture that embraces the power of such a hybrid approach.
- **Intelligence-driven:** Rather than building models that chase historical fraud threats after the fact, banks must continuously evolve their analytics-centered defenses based on detailed up-to-the-minute understanding of the criminal environment. Such knowledge is best developed through intelligence operations and sharing, including monitoring of the dark web. Rather than interrogating fraud incidents in isolation, institutions must take a broader look at the patterns of crime. Industry-wide objectives such as FS-ISAC in the United States provide a more robust data set from which to identify such patterns. The goal should be to shift risk identification from regulatory rules-based detection and predictive models built on past frauds to forward-looking analytics built on well-founded indicators of crime. This creates the means to spot broader patterns of suspicious behavior—such as campaigns by criminal networks as opposed to lone fraudsters—and to look for emerging fraud typologies before significant losses result.
- **Customer-focused:** While constantly evolving to counter the fraud threat, countermeasures should be designed in ways that create a distinctive customer experience balancing trust and convenience to accelerate insight into fraud. Analytics should play as critical a role in facilitating low-risk customers and transactions as they do in thwarting potential fraud, enabling institutions to create customized, analytics-informed journeys balancing security and convenience. Models must be built on the proper foundation, integrating customer behaviors across accounts and transactions into a single view that enhances the power of prediction and detection.

Cutting-edge efforts integrate these themes, pairing a mandate to improve customer experience with improvements in fraud identification. One global bank undertook such a hybrid effort, redesigning customer authentication journeys in its digital channel to simultaneously improve its confidence in customer identification while dramatically improving experience. Beyond achieving its security-related goals, this effort reduced costs related to customer lock-out by $5 million and improved Net Promoter Scores in the online channel by 29 points.

Getting started

To get the most from advanced analytics, organizations should begin by clearly articulating their operational objectives. This crit-

ical foundation provides the proper screens against which to evaluate analytics efforts and investments. It also aligns analytics interventions with business unit goals, identifying the core decisions requiring analytics support, prioritizing those decisions best informed by advanced analytics, mapping data to inform those decisions, designing models leveraging that data, and establishing the metrics against which to evaluate analytics success.

Building from this base, firms should approach advanced analytics as a transformation rather than a one-off event. In the near term, this involves a focus on:

- Identifying the universe of possible interventions, connecting the business with analytics and compliance to prioritize based on potential impact and technical feasibility.
- Articulating clear operational goals, understanding where internal analytics capabilities stand today, where they should be, the investments required, and developing plan to transition from outside support to a reliance on internal resources.
- Cataloguing current capabilities and ensuring they are being leveraged to their maximum potential. Banks often have many of the tools required for an effective initial defense but have not yet aligned them properly.

Individual use cases, pilots, and other traditional means of intervening through analytics should be used to enhance these base capabilities and push the institution's capacity, rather than simply as a means to deliver point solutions. In the medium to long term, organizations must build organic capabilities to constantly reassess evolving fraud threats, revisit and improve the operating model, and design fit-for-purpose advanced analytics and fused data sets.

* * *

The perpetrators of fraud are highly adept at exploiting advances in technology, collaboration, and specialization. Legacy approaches to fraud prevention have not kept pace, with financial institutions stubbornly dependent on siloed data and manual processes. Banks and payments firms looking to establish a competitive edge—and avoid increasing loss exposure and mitigation expense—must harness these same trends. Advanced analytics provide a tangible reason to integrate data across siloes, a means to automate and enhance expert knowledge, and the right tools to prevent, predict, detect, and remediate fraud. Analytics is not an overnight fix, but it can pay immediate benefits while creating the foundation for anti-fraud operating models of the future.

Salim Hasham is a partner in McKinsey's New York office, and **Rob Wavra** is an expert associate partner with McKinsey's QuantumBlack in Boston. **Rob Hayden** was a senior expert in McKinsey's Cleveland office. Rob passed away suddenly and unexpectedly earlier this year, and is deeply missed by all whose lives he touched. Please see McKinsey on Payments, Issue 27 for a remembrance of Rob.