White Paper

Fraud Strategy Has a New Role: Enabler of Innovation

Sponsored by: CyberSource

Jerry Silva
March 2020

IDC OPINION

Fraud solutions traditionally focus on stemming losses, but that's not enough in the age of digital transformation where online merchants are expanding customer channels; adopting continuous, automated commerce models; and employing a multitude of new payment types. Digital commerce sellers find that they need a fraud strategy that opens the door for *secure* innovation and expansion, stemming fraud losses and optimizing transaction acceptance rates. An intersection of agile rules and advanced analytics lies at the heart of the strategy. How are digital commerce players in the age of digital transformation putting advanced fraud management strategies to work?

IN THIS WHITE PAPER

eCommerce merchants across verticals battle a similar fraud prevention challenge: They must curb attacks and stem losses without inhibiting the customer experience through excessive transaction declines.

As if this is not enough of a challenge, a fraud strategy must be agile enough to keep pace with organizations as they grow their ecommerce presence, extend their businesses across geographic borders, and digitally transform, making customer engagement possible through a multitude of devices and new channels.

Building this kind of comprehensive and nuanced fraud management strategy is a journey that can be daunting for many organizations. As merchants invest in product design, go to market, and retail innovation, they don't necessarily want to assign resources to build a vast fraud operations team or manage complicated data integration and on-premise solutions.

As a result, many organizations are changing the way they approach fraud management. This change begins with adopting a solution that helps make real-time, highly accurate decisions using flexible, testable rules and advanced analytics. But it often includes taking a hybrid approach to solution management and operations, supporting internal experts with an external team of fraud experts and solutions that can offer 24 x 7 monitoring, automated decisions, and support. This hybrid approach allows digital commerce players to deploy, test, and adapt rules on an ongoing basis through an external team without committing massive internal resources to the effort.

This IDC Financial Insights white paper presents key findings of interviews with fraud executives, representing three highly different verticals – a global fashion retailer, a leader in outdoor sporting goods, and a major airline – that share insights into building comprehensive, adaptive fraud management programs to control losses and enhance acceptance rates even as their organizations expand into new channels across borders and into new product lines.

March 2020, IDC #US45685019

In tailoring fraud solutions, each interviewed organization has deployed CyberSource, a Visa solution, and used a unique combination of flexible rules, fraud predictive models with historical and current advanced analytics, and machine learning designed to predict or estimate the outcome of each transaction acceptance, rejection, or manual review while reducing fraud losses.

DIGITAL COMMERCE INNOVATION REQUIRES SOPHISTICATED FRAUD COVERAGE

eCommerce makes up 15% of total retail sales worldwide, with cross-border expansion forecast to drive consistent growth. Geographic expansion is becoming possible largely due to innovation among payments providers, which enable digital commerce players to more easily accept localized payment methods across markets, as well as cross-border card transactions.

Meanwhile, merchants are investing in retail digital transformation to improve the consumer shopping experience, lift conversion rates, and create a "repeat buyer" experience that aligns with the expectation of instant fulfillment. Having already extended online and mobile shopping features, merchants are now seeking to create a unified, consistent, and real-time cross-channel experience. Consumers should be able to shop for an item on their mobile device, complete the purchase online, and pickup goods in-store within a single transaction. Further, consumers will increasingly engage in connected commerce in which they subscribe to services supported by automated payments conducted from a range of IoT or connected devices. It is expected that in 2020, 32% of merchants will invest in retail innovation technologies, including connected commerce, and by 2024, 15% of all payments will be made with wearables, while 10 billion devices will be connected to financial services, according to IDC Retail Insights research.

This complicated intersection of cross-border expansion with innovation in channels and customer engagement will not only result in boundless new opportunities for merchants but also introduce new fraud risks, which require sophisticated coverage and a focus on managing an environment where the lag between purchase and fulfillment is getting smaller every day.

Fraudsters notoriously target new services and products with the assumption that merchants will experience unforeseen vulnerabilities in an untested environment. Unfortunately, history proves these vulnerabilities true. Retailers have consistently reported a rapid spike in fraud attacks at the opening of mobile channels as well as the move into new markets. In addition, as the banking industry has already experienced, the size of the retailer matters little when it comes to being targeted. As the top-tier institutions began bolstering their defenses, smaller community banks and credit unions became targets of fraudulent activities. There is no reason to believe that retailers will be immune to attacks based solely on their relatively smaller size.

As merchants begin to accept new payment types across geographies, they may not have rules or models designed to monitor and assess risk specific to these transaction flows. That's particularly challenging. IDC Financial Insights predicts that by 2024, 60% of merchants worldwide will accept anywhere from one to five localized payment types in markets across borders to expand their digital commerce presence. It should be assumed that the adoption of each of these payment types will require nuanced coverage. For example, it will be impossible to fit a card fraud model to a direct-from-bank or ewallet transaction, both of which are taking hold in Europe and Asia.

Finally, merchants must also be concerned about cross-channel attacks. Fraudsters are keenly aware that merchants are expanding customer engagement across channels, and they're viewing this as a weakness. Recently there is rise in cross-channel fraud in buy online, pick up in-store (BOPUS) orders, where fraudsters get an illegitimate payment accepted online and then pick up physical goods in a store, often without having to produce credentials in person.

To add to the challenge, while merchants have worked to secure mobile and online channels, they may not yet have the tools to protect the contact center where they have the added blind spot of the human element. Many attacks begin with fraudsters using social engineering agents to gain further customer credential data, which can then be used to enable an online purchase or to later impersonate a customer during a call-in transaction. In other cases, fraudsters manipulate agents into making changes to addresses and emails to begin the process of total account takeover.

FRAUD RISKS AND VECTORS CONTINUOUSLY SHIFT

As merchants strategize around fraud coverage for cross-border expansion and frictionless customer engagement, they must also keep their eye on ever-changing fraud vectors.

Card-not-present (CNP) attacks (purchases made on remote channels) now account for about 50% of total card losses worldwide and is projected to reach $35 billion by 2022, according to *The Nilson Report.* Transactions made with stolen payment cards make up about 30% of overall chargebacks, which doubles the impact on the merchant that now suffers the loss of the good and bears the requirement to refund money on the lost item. Overall, 55% of businesses report an increase in online fraud, according to Experian.

To make matters worse, merchants often have siloed chargeback and fraud management systems, creating blind spots in transaction monitoring and making it difficult to align their efforts against new and sometimes unanticipated fraud vectors.

The Ever-Present Cyberthreat in Digital Commerce

Digital commerce fraud attacks vary significantly, but many are fueled by the endless flow of breached or stolen data on the black market. A jackpot of payment card data, account number, CVV, expiration date, and address can be bought on the dark web for $1 an account. That data is now operationalized at scale by sophisticated fraud rings, which use automation and analytics to plan their attacks. One common example is fraud rings use bots to continuously test card and credential data with small transactions until they find those that work, unlocking the door for much larger purchases or to sell data on the black market.

Sophisticated Account Takeover: Social Engineering Meets Cyberattack

As fraudsters build more sophisticated organizations and technology, they meticulously compile stolen and breached data with other information amassed on social media networks, as well as through social engineering, and cyberattacks, such as phishing or pagejacking, to fully take over accounts or identities for more sustained attacks and larger returns.

With phishing, fraudsters imitate a trusted individual or source to procure sensitive data. For example, an individual may receive an email message that presents itself as coming from a financial institution, suggesting there is an account problem and requesting the individual to verify personal information through a linked form. Another related fraud strategy is pagejacking, in which fraudsters clone an

entire web page or website and then use search engine optimization strategies to elevate that fraudulent website ahead of the legitimate site in online search. Unsuspecting users very often click through to the fake site and unwittingly divulge sensitive data.

In all cases, fraudsters can use this sensitive data to first gain access to an account, often beginning by conducting nonmonetary events, such as changing addresses and emails, so that they may authenticate and receive orders. These attacks can also include device takeover where the fraudster ports a victim's phone number to his/her own device, allowing the victim to authenticate when one-time passwords are sent. This, then, can lead to further account takeover using the data and access already on the device.

Once fraudsters fully take over an account, they may start with small purchases over a long period of time, aiming to go unnoticed by the consumer. But over time, fraudsters take these complete sets of credentials and open new accounts under a victim's name, often going unseen as many consumers don't have new account alerts set up from credit bureaus or other services.

Synthetic Identity Fraud: Fueling Losses

Stolen credentials may also be used to fuel synthetic identity frauds, in which the attackers combine shreds of valid identity data with false information to make up an entirely new entity in order to open new accounts. Fraudsters may pair a valid social security number of a child – a number that has never been used – along with a true shippable address and real phone number and then add a false name and date of birth. The goal is to combine enough information to establish credentials for a new payment account. The top 5 issuing banks have seen $5+ billion in losses linked to synthetic identity fraud, according to IDC Financial Insights.

Loyalty and Rewards Fraud: Attacks Where Few Are Paying Attention

As with new account fraud, fraudsters are also focusing on the typically lightly monitored area of loyalty and reward programs. As consumers amass loyalty points through either their credit cards or digital commerce reward programs, fraudsters use account takeover tactics to utilize rewards for purchases. Though consumers consistently sign up for rewards programs, they notoriously do not redeem their points or check the status of their accounts, which means attacks go largely unnoticed for long periods of time.

Friendly Fraud

The oddly termed *friendly fraud* occurs when an established customer knowingly commits fraud on his/her own account. Scenarios vary widely, but can include customers making a purchase, receiving the goods, and then calling the card issuer to claim they didn't receive the item. Merchants have difficulty preventing this fraud since transactions are originated by known customers.

FRAUD SOLUTIONS AS THE ENABLER OF INNOVATION

Although new business processes, payment methods, and channel integrations may open new doors for enterprising fraudsters, these potential risks should not prohibit innovation. In fact, where fraud operations teams may have historically hampered the vision of product teams looking to launch new services, they can now focus on implementing robust fraud solutions that can assist to enable innovation.

Fraud solutions and strategies for digital commerce should be aimed at three core benefits: reducing losses and chargebacks, enhancing customer experience, and lifting sales conversion. The road to that trifecta is through fraud monitoring solutions that assess transactions and make real-time risk decisions based on a wide array of data. This provides a holistic view of both the exchange itself and the entity conducting that event.

In the earliest days of ecommerce expansion, merchants reviewed nearly every order to assess risk. This practice seriously slowed operations and resulted in blunt decisions of false positives and declines. This only decayed customer relationships.

The next phase of fraud monitoring used limited automation to make risk decisions on transactions. These systems were often built on similar basic rules and made risk decisions based on elements such as a mismatch of shipping address to account address. But this simple automation failed to look at these fraudulent transactions in a wider context or pattern.

Today's next-generation digital commerce fraud solutions provide nuance enabled by closely tailored rules and advanced analytics, fed by both a large volume and variety of data from a single merchant or across organizations. This provides the ability to see "normal" abnormalities in transactions as well as the very real anomalies that indicate fraud. These solutions use rules based on historical entity profiles and transactions. For example, the solutions can look at behaviors over periods of time, highlighting that a specific entity often buys airline tickets for a range of other individuals, indicating this is normal behavior that should not be flagged for review or lead to a decline. Ultimately, the goal of making better decisions leads to a reduction in declines and improved customer experience without compromising security.

To make nuanced rules work, fraud systems must ingest a wide set of data to gain a holistic view of risk. In real-time fraud monitoring, the solution should consider as much information about the transaction in context as possible. The most straightforward information surrounds the amount of a transaction, the time of day, and region. But in context, the solution would know more about the entity. How common is this transaction compared with others historically made by this account? Does this entity typically make purchases at odd times of the night? Is there a reason the device geolocation is different from the address linked to the entity's account? These kinds of profiles can be built over time, either when a consumer has an account with a merchant or by binding together historical data to a device or a card account across organizations.

It is increasingly possible — and important — to understand a user's behavior through information that reaches beyond the device. Next-generation fraud solutions evaluate device identification, IP address, screen resolution, authentication, and behavioral biometric data related to an entity to create a baseline of normal behavior and subsequently a corresponding context of anomaly.

Even with the best data and real-time decision-making tools, it should be assumed that every merchant faces unique fraud challenges and fast-changing buying patterns among its consumer base. As such, next-generation fraud tools must be finely tuned to the specific needs of each merchant, which requires a flexible policy writing system. These rules will be fine-tuned to seek patterns linked to

geography-specific frauds as merchants move into new markets. The rules will also be used to understand normal and abnormal behavior in cross-channel transactions and on new devices.

The agility to fine-tune rules also helps merchants cope with fast-changing market conditions or specific vertical industry or organizational attacks. For example, some retailers may fine-tune rules based on specific peak selling times and product buying cycles or by product type. They may adjust those rules when a season passes or a craze for the product ends.

Machine Learning and Rule Agility

Enabling agility isn't just about the ability to quickly write rules but also about having the right data to set risk policy, as well as having the ability to test the efficacy of those rules. Next-generation fraud solutions should include advanced analytics and performance monitoring. With advanced analytics, solutions can crunch massive amounts of data, including known frauds, and leverage machine learning models to identify behavior patterns linked to these attacks. The performance monitoring is a feedback loop that helps target the models.

Machine learning models can be taught to seek specific patterns and set to unearth clusters of activity among live transactions that indicate potential attack. In both cases, they are automated and have the capacity to sift mountains of data for the most nuanced view. Often machine learning models can then be used to recommended rules for implementation.

In some cases, this data will be extracted from one merchant, but some fraud solution providers can analyze massive sets of multi-organizational information. With cross-organization, fraud operations teams can segment fraud patterns by vertical, geography, or organization size (among many factors). Segmentation allows for market-specific fraud patterns to emerge, enabling solution providers to proactively warn a merchant in a specific segment that an attack is imminent so that they may write policy rules and analytics in preparation.

Once rules are recommended, they should be tested in a sandbox environment on production data to assess their performance and outcomes. Finally, the merchant, in conjunction with its fraud solution provider, should run consistent reports on rule performance so that it may gauge changes in the market and potential degradation due to shifting fraud patterns. This is where the importance of agile rules and adaptable analytics truly come into play.

Fraud Solutions: Driving Customer Experience, Enhancing Conversion

Ultimately, a cross-section of data-driven analytics, agile rule writing, and machine learning is necessary for merchants to effectively stem fraud losses and also provide a delightful customer experience.

The ability to write agile rules and policy deftly balances how much fraud the organization is willing to allow in order to reduce customer friction. If rules are too blunt, order acceptance rates will drop, and customer dissatisfaction may increase. Fraud experts must take into consideration the cost of false declines and resulting customer frustration against that of successful fraud attacks. The cost of false declines can be closely measured by lost transactions, but more difficult to assess is the impact on long-term customer relationships and reduced repeat business. Often when fraud solution providers offer rule performance monitoring, one measurable key performance indicator (KPI) will be the number of declined orders as well as the cost of investigating nonfraud transactions.

Operational Optimization: Reduced Reviews and Managed Services

In addition to measuring success by controlled losses and optimized order acceptance, fraud operations teams should also measure reduction or control in the cost of operations. Running a fraud operations team can be expensive; wasting resources on unnecessary reviews and investigations resulting from false positives adds to that cost. As such, fraud experts should write rules with a clear eye toward reducing person-hours without compromising security or customer service.

In addition, those in charge of digital commerce fraud efforts may seek to optimize operations by adopting externally managed fraud services. The managed model can take many shapes. In some cases, fraud solution providers will offer real-time decisions as a service, while onsite teams at the merchant write both the policy and risk rules. In other cases, the offsite team will provide both rule writing and decisions, while an onsite team takes on manual review and investigation. Finally, it is possible for merchants to offload the entire operation. In any case, the goal would be to reduce complexity and cost in operations while extending hours and having flexibility in head count so that resources can be increased during peak fraud seasons and otherwise decreased.

SHAPING KPIS: THE KEY TO MAINTAINING BALANCE

Creating a fraud strategy is a complex endeavor that requires the careful balance between controlling fraud losses and optimizing order acceptance and customer experience.

As fraud experts seek to adopt next-generation fraud solutions, they should create a set of measurable values or key performance indicators that will demonstrate the effectiveness of their fraud strategies in relation to specific business objectives. In addition, they should consider evaluating whether their fraud strategy is the inhibitor or enabler of innovation.

Fraud experts should consider developing KPIs on:

- Fraud losses versus acceptance rates:
  - Transaction acceptance and rejection rates
  - Chargeback rates and reasons
  - False positive rates and value detection rate
  - Fraud losses
- Operational optimization:
  - Percentage of transactions sent for manual review (including frauds and nonfrauds)
  - Required person-hours for manual review and investigation
  - Time spent managing data
  - Time spent managing rules and their performance
- Customer experience and innovation:
  - Organizational ability to expand and innovate
  - Time to product release and control fraud in each new release
  - Customer friction, including time spent on authentication and transaction completion
  - Return customers
  - Customer complaints as they relate to fraud and/or declines

CYBERSOURCE IN ACTION

CyberSource, a Visa solution, provides digital commerce payment gateway and fraud management solutions that can combine agile rule writing and advanced analytics, as well as managed fraud services. In its approach, CyberSource takes on a collaborative role with its digital commerce customers to provide a comprehensive approach to fraud management. In the sections that follow, the three scenarios show how CyberSource solutions are put to work to stay ahead of fast-changing fraud while helping meet key business objectives and supporting innovation.

Backcountry.com: A Comprehensive Fraud Strategy to Assess Entity and Transaction Risk

In 1997, Backcountry.com was founded as a small online business aimed at selling unique outdoor sports equipment – its first line was a collection of avalanche gear. The business rapidly expanded, with a wide array of outdoor sporting equipment, an international presence, and a market leadership position in its segment against major brands.

In Backcountry's earliest days, while orders were quickly picking up, it was still easy enough to manage through largely manual processes. As such, the company's fraud strategy was built on the use of simple rules and manual review of nearly every order. But that approach no longer sufficed with the diversification in product lines, expansion across geographic markets, and introduction of a mobile channel, which almost immediately introduced new risk and attacks.

At first, Backcountry implemented its own risk rules, which were designed to catch what appeared to be straightforward anomalies in customer transactions (e.g., mismatched billing and shipping addresses received manual review). But with higher volume and diversity in customer base, this was no longer possible. What's more, the sophisticated fraudsters could figure out the rules. Ultimately, the fraud process was getting in the way of growing the business.

By the time Backcountry set out to build a fraud strategy, it had developed a strong team of fraud experts, who knew how to crack complicated cases because of so much manual review. Backcountry wanted to optimize that team, ensuring it was only reviewing and investigating true fraud and not false positives. The organization also didn't want to grow the fraud team head count to make it a cost center.

Backcountry's Fraud Initiative: Precision in Rule Writing

Backcountry ultimately built its fraud initiative around CyberSource's Decision Manager as the center of real-time transaction risk assessment. CyberSource provides fraud monitoring as a service, receiving transaction and entity data through an API from Backcountry and making decisions to approve or reject the transaction or recommend manual review. Backcountry's expert fraud team writes the rules designed to trigger risk alerts based on its extensive history of review and investigation.

Backcountry and CyberSource worked to design the risk rules to be as specific as possible in order to make the most nuanced decisions. The teams analyzed historical transactions, including known frauds, to seek underlying risk patterns and then used these insights to design rules specific to region, channel, device, and product line, among other factors.

The granularity of rules enables the company to monitor more closely for frauds against higher-risk products. In one case, the team wrote rules specifically for what the team jokingly calls the "tent lady" – a fraudster who periodically calls the contact center to buy tents using fake credit cards. There are also seasonal trends that don't match those of other retailers. During the fall, Backcountry sees a pattern

of fraudsters seeking to buy expensive down jackets to resell on the black market for winter. With Decision Manager, the team writes stricter decision rules for winter jacket transactions, which can be loosened after the season.

On the flip side, these rules enable Backcountry to better understand legitimate traffic with seemingly anomalous behavior. For example, a close examination of trends has revealed to the team that legitimate buyers often don't provide the most accurate billing information, while fraudsters provide entirely complete sets of information. Writing rules on this knowledge means that legitimate customers are prompted to complete their details, but not declined or sent for manual review.

Understanding Entity Risk

As Backcountry's fraud strategy evolved, it became clear that the road to the best possible risk decision would require assessing more than transactional data and history — it would also include assessing the risk of the entity attached to the transaction.

For example, Backcountry's team had been hit by a series of attacks from fraud rings, which came from devices with the same screen resolution. The team learned it had to ingest screen resolution as one element or data point to assess risk. CyberSource Decision Manager enables integration with a range of entity risk solutions, which provide output data to enrich the view of entity risk.

With the ability to integrate, the Backcountry team decided it would use device identification, email history, and IP connectivity as factors alongside transactional data to make decisions. That means that for each decision, transactional history — such as unusual amounts or unusual velocity of transactions — can be paired with data about the entity's device or behavioral biometrics. These correlations highlight both normal and abnormal behavior on the device, for example, as a central part of assessing the risk of the entity conducting the transaction. In some cases, the team wrote rules for which transactions would be sent to those API plug-in solutions for further investigation of the entity. In other cases, enrichment data is used as part of the real-time transaction monitoring flow.

Taking a Cross-Market View of Risk with Machine Learning

While Backcountry's fraud team had developed a deep expertise in studying the organization's data to determine risk rules, CyberSource was able to bring even more nuance to the rules by adding the perspective of fraud and risk patterns across many merchants.

CyberSource, which serves several hundred of the world's largest online merchants, created a fraud management solution by developing machine learning models, which analyze large sets of payments-related data from across these retail organizations. This is particularly important in identifying the fraud rings that operate by first targeting merchants that are most vulnerable until they set their controls, then moving on to the next organization.

Backcountry has seen a sharper accuracy in scores now that CyberSource's machine learning models play a role in rule suggestion and make it possible for Backcountry to maintain highly accurate watchlists for entities based on a wider array of risk variables.

Measuring Performance: Beyond Controlled Fraud Losses

Like every merchant, Backcountry measures performance by reduction in fraud losses with the ability to increase order acceptance. Backcountry specifically seeks to reduce cancellation rates — or those transactions that are sent for review and then ultimately cancelled.

Ultimately, Backcountry wants to optimize the operations of its fraud team. A central success factor for doing so is reducing the need for manual review, as well as ensuring that cases that do require investigation are more likely to be actual fraud than false positives.

But success in fraud prevention is not a point-in-time destination. Since fraud patterns continuously change and go-to-market tactics will continue to evolve, Backcountry measures success by agility. In this case, we define agility as the ability to easily write rules that can be quickly tested, implemented, and tamped back down when possible.

It is this agility that will ensure that the fraud program is a continued enabler for automation and innovation as opposed to a barrier.

Philippine Airlines: Stemming Sophisticated Fraud While Opening the Digital Gates

Seven years ago, Philippine Airlines (PAL) faced the most daunting of retail fraud dilemmas. Just as the company needed to expand in digital and contact center customer engagement, fraud attacks became more sophisticated, forcing significant losses and chargeback rates, which surpassed the card networks' thresholds and resulted in receiving bank warnings.

In an attempt to gain control, the organization used a homegrown tool to craft stringent rules using positive and negative lists, but this only forced down order acceptance rates and placed hard limits on how customers could engage in the channels. As fraudsters continued to grow more sophisticated, the homegrown tool was no longer sufficient to detect suspicious orders, which led PAL to suffer various fraud attacks.

To get this level of fraud under control, PAL restructured its fraud strategy, implementing CyberSource's real-time decisioning engine with nuanced rules and models that would help identify fraud without souring customer experience.

The goals of the implementation were to reduce fraud rates, increase order acceptance, and improve customer experience even as the organization expanded the kinds of transactions that could occur across channels, including digital and contact center. To do this, PAL specifically wanted to base its rules and models on recommendations found in a deep set of data extracted from across airlines and travel merchants in the region.

In PAL's rebuilt fraud program –– now seven years in production –– CyberSource runs Decision Manager remotely. Receiving data through an API from the airline, the solution can assess – in real time – risk-based decisions to accept, decline, or review transactions based on the customer's risk threshold rules. PAL writes its own risk detection rules in addition to the rules written by a CyberSource fraud expert assigned to the initiative.

The combined approach means most rules are built on a wide set of data, including historical transactions and CyberSource best practices, and are tailored to analyze risk associated with variables and parameters identified by PAL. Consistent assessment monitoring shows the performance of these rules and reflects degradation due to possible changes in fraud patterns or season, enabling very rapid adjustment of policy and thresholds. PAL uses CyberSource's sandbox environment to test new or adapted rules on production data to proactively assess performance and run analytics models on past frauds to find better rule outcomes.

Measuring Performance: Optimized Operations, Reduced Fraud, and Improved Customer Experience

As a first step of its comprehensive fraud initiative, PAL drastically reduced its fraud losses, and the organization has not come anywhere close to hitting the card networks' chargeback threshold. Now PAL measures its success in more sophisticated ways.

One consistently measured KPI is the organization's order acceptance rates, which directly impact customer experience. Beyond that, success continues to be measured by agility in rules. PAL's rules are a constant and purposeful work in progress. Policy is adjusted regularly to maximize revenue against rejection rates and acceptable losses, as well as to address changing market factors.

In the long run, PAL will continue to use this agility to expand product, market reach, and channel accessibility. Since its launch, the PAL initiative has added the mobile channel to its fraud program and will be able to open new channels as they emerge in a protected environment with rules that can be tailored for the use case.

An International Fashion Retailer: Fraud Coverage to Enable Rapid Geographic Expansion

Growing from a single-brand, brick-and-mortar high-fashion retail business to a multibrand, international megaretailer with a cross-channel ecommerce presence requires an entirely new fraud strategy.

When this international retailer, which requested anonymity, first began building its cross-border ecommerce presence to add to its brick-and-mortar stores, the organization had no fraud solutions in place. There was little need for transactional monitoring for in-store purchases, which were protected by credit card network coverage.

But expansion into online sales, and the acceptance of card-not-present transactions, meant this retailer was suddenly liable for losses. To add to that pressure, the retailer grew so swiftly across markets that it caught the eye of fraudsters, increasing losses and chargebacks soon followed. The first response was to begin declining orders, but the group knew immediately that wasn't the right approach. One cannot adopt fraud prevention at the cost of reduced sales.

As the organization set out to find a fraud solution, it learned quickly that a comprehensive strategy is required more than simply reducing fraud. The retailer needed a solution that would reduce customer friction, increase order acceptance, and limit time-consuming manual reviews while reducing losses. Specifically, the organization was seeking a solution that would enable the company to write flexible policy rules and, in turn, closely balance the amount of fraud losses it could sustain in relation to the optimization of order acceptance.

The retailer was especially concerned with high customer satisfaction as it pushed into each new geographic region. During the expansion, the group learned quickly that each market had unique fraud challenges and differing consumer profiles. And while the team could rely on the collective past experiences of similar CyberSource clients in those markets to help frame the appropriate initial fraud strategy, fraud solutions still have to be finely aware of nuances for each region for the team's particular products.

In seeking out a fraud strategy, the organization didn't want to build out a labyrinth crime-fighting team or spend endless IT resources managing complicated systems. The company had become known internationally for innovative retail tactics, which relied on interesting technology. It didn't want to get off course or lose focus by diverting intensive technology resources to fraud operations.

This retailer ultimately decided to employ CyberSource's Decision Manager, entering what the organization calls a true collaboration with the fraud management provider now eight years in the making. Decision Manager provides real-time monitoring and decisions on every transaction using a combination of advanced analytics models and adaptive policy rules to identify potentially fraudulent sales while increasing order acceptance. The solution ingests a wide array of data from the retailer's systems, ranging from transaction details to shipping and billing address, account numbers, device ID, IP connection, and more. The goal is to establish a baseline of normal customer behavior in order to identify anomalies that indicate fraud. The best kind of solution does this with the kind of nuance that allows for there to be "normal" abnormalities.

In addition to implementing monitoring via Decision Manager, the retailer also engaged a team of fraud experts to handle manual review and other operations. The CyberSource team functions on behalf of the retailer in a 24 x 7 fraud management operation. Meanwhile, the retailer maintains a small, focused fraud team onsite, which runs quality assurance on output from the CyberSource team, making final decisions on transaction holds. The retailer's team works with the CyberSource team to write policy and rules to balance "acceptable losses" with optimized customer experience.

Market and Brand Expansion Enabled by Advanced Analytics and Agile Rules

The combination of agile rule writing and advanced analytics is key to enabling this merchant to continue its geographic ecommerce expansion strategy. Since each new market poses unique fraud threats and introduces new consumer profiles, it is crucial to enter that geography with a fine-tuned set of models and rules. The problem is that fine-tuning can be hard in the early days of a new market entry. This is where CyberSource's past regional client experience and advanced analytics become most important.

As the company starts moving into new geographies, the CyberSource team runs a full analysis of the market by running advanced machine learning analytics to crunch massive amounts of cross-merchant data in the region. Analyzing this cross-sectional data makes it possible to identify existing fraud patterns as well as to establish consumer profiles to best understand normal and anomalous shopping behaviors.

The outcome of these models allows CyberSource to suggest fraud decisioning rules, which can be used right out of the gate in a new implementation. The CyberSource team provides insight as to whether to lower risk rates on higher-amount transactions in a wealthier market or to limit high-value transactions in an area rife with fraud, for example. Without access to Visa's wide set of data, and the use of advanced models, it could otherwise take months to train a fraud solution with the nuance necessary for new markets or product launches.

In addition, rules can be fine-tuned for payment types that are specific to each of these markets. While most markets depend on card transactions, many also have alternative retail payments that are unique to local systems. For example, many markets still allow for cash-on-delivery orders, which require specific fraud monitoring rules based. These rules can be based on amount or historical transactions linked to an entity or address, for example.

Creating fraud monitoring rules with early-day accuracy based on rich data means that this retailer can live up to its objective to never enter a market with unnecessarily high restrictions. From a policy point of view, the company tends toward entering a new market to establish new relationships with the least possible friction.

Beyond market expansion, the retailer has also been able to write rules that are specific to the fraud trends in each of its brands. Varying brands have fraud patterns that may be specific to the kinds of items those brands sell or the consumer base those brands serve.

Reporting and Business Intelligence

This collaboration between the retailer and CyberSource is supported through a series of reports, which represent solution performance. Varying views can represent specific rule performance, overall losses, chargeback rates, and changes in conversion rates. In addition, the merchant's internal QA team pulls specific reports from the CyberSource system showing performance by region, agent, and time. The constant monitoring enables the joint organizations to keep a pulse on the models and rules as expansion continues and fraud trends change.

Ultimately, the measurement of success in a Decision Manager deployment for this merchant relies on a number of rich and interconnected factors. Like most merchants, the true sign of success is improved customer satisfaction and conversion rates with the lowest possible fraud losses and chargebacks. Beyond that, though, the organization is consistently measuring operational efficiency, specifically through the required time spent among its internal reviewers based on the accuracy of CyberSource's output. Finally, a true barometer of success is the ability to freely continue to expand and innovate without fraud as a barrier.

ESSENTIAL GUIDANCE

As ecommerce evolves to be a key driver of the global economy, nearly every business will adopt a digital commerce role — and they will all need a fraud strategy that is smarter than the fraudsters who will attack. Digital commerce players have a lot to consider in building next-generation fraud strategies that balance the need to protect the business from existing and emerging fraud attacks while delighting customers, supporting key business growth strategies, and enabling innovation. To help achieve these goals, the following guidance should be considered:

- **Choose a robust and agile fraud solution.** Embrace a fraud solution designed to effectively confront today's sophisticated fraud challenges including account takeover, new account fraud, loyalty and rewards, and friendly fraud. Ensure that your fraud solution includes adaptive rules, advanced analytics, machine learning that leverages continuous revalidation, and performance monitoring to ensure business objectives are consistently met. Choose a solution that is robust enough to support innovation and grow with your business.
- **Build fraud strategies with innovation as a central goal.** A fraud strategy should be about enabling rapid innovation. Good fraud solutions should be at the heart of digital transformation — certainly not a barrier. Work with a fraud solution that enables analytics models, which can be adapted to cover the continued expansion of devices, channels, payment types, and geographies without limits. In taking this approach, it is key to involve innovation teams in the overall fraud strategy planning.
- **Choose an implementation and strategy style.** Adopt a fraud strategy that matches your organizational needs. That could mean an on-premise, an externally managed, or a hybrid model. This choice may depend on the size of the organization and the willingness (including budget) to build a full fraud operations team with 24 x 7 coverage. In cases of hybrid implementation, it is important to choose a solution provider that acts as a true partner to the merchant fraud team, with the two acting as extensions of each other.

- **Set operational goals.** Choosing a fraud strategy enables the optimization of fraud operational resources by reducing wasted time on investigating false positives and/or by reducing the necessary person-hours to maintain the goals of the initiative. This should be a key objective of the fraud strategy.
- **Identify business and fraud prevention KPIs in the same context.** Tailoring a solution should be just as much about enhancing innovation and customer experience as it is about reducing losses. Since business and security objectives are interconnected, KPIs should be set with both in mind as they relate to each other.
- **Think agile.** The ecommerce market is fast changing and so is fraud. Fraud strategies must enable users to engage in rule writing, model adaptation, and production-level testing quickly enough to address these rapid changes.

Sources and Methodologies

This IDC Financial Insights white paper is based on a number of sources and methodologies typically used by IDC analysts, including:

- One-on-one interviews with industry executives
- Collaboration with IDC analysts covering other industry and technology areas
- Comprehensive knowledge of vendor products and services
- Best practice and behavioral data accumulated through IDC surveys
- Individual experience and tenure of IDC analysts with years in the industry

IDC uses standardized approaches to the development of content to ensure adherence to IDC research policy and consistency with the advice given to its clients.

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.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com