White paper

Aligning your team to fight rising fraud threats

Introduction

Fraud is constantly evolving. New technology and complex underground networks mean a rise in criminal sophistication. In response, fraud prevention has become complicated and damaging to the customer experience.

Payment trends, channel expansion, consumer confidence and regulatory compliance all continually put pressure on fraud teams—whose mandate is to mitigate risk. At the same time, product development and marketing teams are looking to drive growth—a separate mandate. These siloed goals have become a weakness that fraudsters are ready to exploit.

Though the approach of fraudsters is savvy, they are counting on such vulnerabilities and expect to be chased, not outmaneuvered. A fundamental internal shift can drive the forward-looking approach that companies need in this landscape, creating an organization that works cohesively to fight fraud—while growing revenue and attracting new customers. The reality of today's environment demands this unified approach.

How did we get here?

The evolution of fraud strategies

As technologies evolve and information security tightens, the savvy nature of fraudsters becomes more sophisticated. Fraud prevention strategies have been impacted by many trends, the most significant among them being:

The EMV shift — The combination of a "chip and pin" system in credit and debit cards in 2015 did not put an end to payment-based attacks. Fraudsters have adapted their tactics for an overall shift in fraud including card-not-present (CNP), identity takeover and synthetic-identity fraud as a result. In fact, e-commerce fraud increased to 33 percent, according to Experian data.

Online and mobile expansion — About 30 percent of all online transactions during last year's holiday peak were made using a mobile device and mobile commerce is expected to reach $284 billion, or 45 percent of the total U.S. e-commerce market by 2020.[1] Additionally, 36 percent of organizations interact with their customer in five or more channels.[2] As consumers take advantage of capabilities that drive convenience, the potential for fraud rises.

Data breach — With the increase in reported data breaches comes an increased hesitancy from consumers to share their personal information. Also, as more and more personally identifiable information (PII) is compromised, it becomes less valuable for businesses and agencies to use as a singular or isolated means of authenticating consumers. While important in compliance-oriented identity checking, elements such as name, address, phone, date of birth, and Social Security Number (SSN) alone are no longer sufficient for risk-based authentication and assessment.

Regulatory compliance — Consumers are wary of providing PII because of data-breach risk. Yet requirements must be met for a myriad of guidelines and rules including Red Flags Rule, USA PATRIOT Act checks like AML or KYC/CIP, Consumer Financial Protection Bureau (CFPB) mandates, National Institute of Standards and Technology (NIST) levels of assurance in authentication, among others.

The key to meeting these evolving needs with an effective fraud-authentication strategy is moving beyond a one-size-fits-all approach and instead, deploying right-sized solutions so there is an appropriate level of protection to every transaction—increasing confidence and driving smooth customer interactions.

> "The conversation is changing. In addition to risk tolerance, executives and fraud strategists will talk about customer disruption tolerance.
>
> —Matthew Lane, Global Fraud and Identity Service and Operations, Experian

Trends in account opening fraud

The Association of Certified Fraud Examiners (ACFE) devotes considerable time to the problem of account opening fraud in its publication, Financial Institutions Fraud. It notes that "a majority of institutions are reluctant to develop strict fraud prevention policies because determining the costs and benefits of prevention are almost impossible." It adds: "Even if an account was opened fraudulently, until money is lost due to deception, there is no way of showing that the account would have lost money." Because of its lack of reliability or transparency, business users are rightfully wary of the data on which they're basing decisions. Consequently, even when the data reveals something interesting or novel, users tend to rely on their own intuition, overriding the data, when making important decisions. To that point, our 2017 global data management benchmark report revealed that 50 percent of financial institutions say that they rely on educated guesses or gut feelings to make decisions based on their data.

Based on our experience working with large and small financial institutions and merchants globally, we have seen a much broader spectrum of responses. Companies may block or delay transactions, flag and suspend accounts after seeing a suspicious transaction, or block accounts and issue new cards before a transaction. The type of responses can vary widely and are generally based on a combination of their organization's size, tolerance for risk, available investigators, level of system automation, and access to information.

If you do not factor in the importance of the customer experience, then the more aggressive the fraud mitigation measures, the better. But that is not the direction in which the industry is heading. Draconian measures are out of step with maintaining the seamless customer experience that consumers expect. In fact, with rare exceptions, our clients view a positive customer experience as integral to business growth. That said, many organizations view a positive balance between risk mitigation and an ideal consumer experience as unattainable.

The relationship between the two mandates is so important that each team can improve and strengthen the other—an essential combination for sustainable business growth.

While organizations like the ACFE are focused only on financial cost impact, we believe the conversation is expanding. The broader discussion should encompass the impact of fraud strategies on the customer experience, which is centered on financial stability and growth for the business.

A forward-looking approach to fighting fraud

As institutions work to effectively protect against the greatest fraud risks—brand reputation, compliance, customer experience, profitability and charge-offs—it's important to take an approach that allows you to adapt to the ever-changing fraud landscape. This means eliminating what, on the surface, appears to be competing priorities between the business and your fraud teams.

Growth requires stronger internal relationships

Business growth depends on opening new channels, expanding offerings, and extending into new geographies and markets—all while maintaining a positive customer experience that is relevant and consistent. Without this, it is hard to build strong relationships with your customers and create brand loyalty.

Typically, product and marketing teams (who generate business demand) view fraud teams (who minimize financial loss) as a roadblock to their efforts. They see fraud teams as creating unnecessary obstacles and points of friction that can result in lost business. This is a legitimate concern given many fraud strategies in the past have been overly aggressive, or did not match the nature of the transactions. Here are a few examples of how this has happened:

- Adding more security challenges for different products or channels undermines a seamless customer experience by creating new hoops for customers to jump through and more processes for them to follow. Customers simply do not understand why security for an existing relationship with your product or service can't be automatically extended to new products and channels.
- Declining transactions in order to prevent possible fraud often results in customers using other credit cards at the point of sale; this may be a temporary inconvenience, or it may mean that you lose your coveted "top-of-wallet" position.
- Putting longer hold times on transactions in order to confirm legitimate transactions can result in financial difficulties for customers. These same customers today have a lower threshold for inconvenience and a greater willingness to change. This can lead to customer defection.

Given this context, relationships are often strained between teams on the product and marketing side and their colleagues in fraud prevention. Unfortunately, this benefits the fraudster, who counts on organizational siloes to exploit blind spots and evade detection.

Knowing your customers' behavior creates more targeted fraud strategies

In the past, marketing and sales teams were seen as the collectors and custodians of information about the customer. Fraud teams also have access to a tremendous amount of data about customers, but this information is used primarily to differentiate actual customers from fraudsters. Adding marketing insights around consumer behavior to fraud strategies will not only create more targeted, effective strategies, but will also help marketing teams plan, segment and deliver products and offers with greater success.

Best practices for aligning revenue goals and fraud mitigation

Benefits of aligning revenue goals and fraud mitigation can be self-evident. Still, many organizations must take action to implement these organizational best practices:

- Regular, proactive communication across product, marketing and fraud teams to help anticipate new points of attack. For example, including fraud teams in discussions about new product development, channels, markets and promotions can help uncover new opportunities beyond just catching fraud.
- Establish common goals for optimal customer experience across product, marketing and fraud teams. This will help to encourage a more collaborative way of creating targeted growth and fraud strategies. For example, sharing information about your customer's behavior to help improve offer redemption and fraud detection.
- Rethink how customers interact with your business, moving away from isolated interactions to a lifecycle relationship mentality. For example, shared responsibility for fraud across account opening, access and transactions will help detect fraud earlier and prevent financial loss.

The impact of these three best practices is seen in the collaborative way in which internal teams will share information to improve the customer experience while also protecting them from criminals.

Right-sized fraud solutions for increased customer confidence and smooth interactions

Most financial institutions have to cast a relatively large net to catch fraudsters. This is because fraudsters are hard to find in the crowd, so essentially the whole crowd has to be viewed with suspicion. Steps taken to block fraudsters often end up inconveniencing a disproportionate number of legitimate customers. And, customers dislike the disruption. In fact, 83 percent of respondents in a recent study reported feeling frustrated or upset about being declined, and a similar number said they felt betrayed or not trusted.

Modern fraud strategies necessitate applying the right level of confidence so that you're most likely to catch fraudsters without disrupting the business of—and relationships with—legitimate customers. We call this "right-sizing" the fraud solution. The following table illustrates how dramatically you can improve your fraud detection rate while reducing the number of false positives. Ultimately, this translates to less disruption for legitimate customers.

Key performance indicators for fraud teams	Impact of right-sized fraud solutions on account opening
Manual review rate	Reduce manual reviews by 49%
Fraud rate	Reduce missed fraud by 88%
Fraud detection rate	Increase fraud detection by 78%
Attack rate	Reduce fraudulent attempts by 48%
False positive ratio	Reduce false positives by 50%

Right-sizing fraud solutions for account opening. A right-sized approach means tackling the problem with a highly tailored solution that enables the business, rather than crippling it. Two characteristics of this approach are: 1) understanding your attack rate, or how much, and where the fraud is coming from; and 2) weighing the risk against the value of the transaction.

Conclusion

Criminals have created a business of committing fraud—a source of success, reputation, prosperity and innovation. For companies, preventing fraud loss is often viewed as a cost of doing business, and, as such, is approached defensively. In order to outpace fraudsters, organizations are modernizing their fraud mitigation strategies, making them less reactive, and more predictive and proactive. To that end, fraud teams are becoming an integral part of creating sustainable business growth by adopting several principles.

- Changing the culture of your organization so the ideal customer experience is a shared goal of fraud, product development and marketing teams and silos are removed.
  By sharing information across functions, fraud, marketing and product teams—among others—gain an expansive view of customer behavior.
- Collaborating across the customer touch points to facilitate pre-transaction fraud detection, thereby reducing capital and operational expenditures.
- Using a blended ecosystem of working with vendors, customers, partners and even competitors to increase agility.
- Applying the appropriate degree of confidence, based on the nature of the transaction, to optimize resources and streamline the customer experience.

Weaving these principles into your fraud strategies is crucial for success. Fraudsters are relentlessly fast—and getting faster. Fortunately, modern fraud mitigation approaches have shifted fraud prevention from "the cost of doing business" to an important driver on the growth agenda, with an active role in a company's success.

[1] Business Insider
[2] Experian Marketing Services study

Experian
475 Anton Blvd.
Costa Mesa, CA 92626
T: 1 888 727 8330
www.experian.com