Aite PARTNER. ADVISOR. CATALYST.

Using Fraud Management to Grow Your E-Commerce Business

APRIL 2021

Prepared for:

cybersource
A Visa Solution

TABLE OF CONTENTS

LIST OF FIGURES

EXECUTIVE SUMMARY

Using Fraud Management to Grow Your E-Commerce Business, commissioned by Cybersource, a Visa Solution, and produced by Aite Group, explores how attitudes toward fraud management are changing. Rather than focusing solely on minimizing fraud losses, progressive companies are leveraging it to expand their business and maximize sales.

Key takeaways from the study include the following:

- Card-not-present (CNP) fraud continues to pose a business and financial risk to merchants.
- Weak passwords and password reuse across multiple sites provide fraudsters with easy access to online accounts.
- An emerging method to address CNP fraud is via orchestration hubs that bring together both account-level and transaction-level solutions into one cohesive system.
- Managing fraud is no longer a choice between either lower fraud or higher approval rates. Merchants are working toward balancing both.
- Fraud departments are being reinvented. Rather than a function within operations, they are increasingly working alongside finance, sales, and marketing to lower cart abandonment and drive revenue growth.

INTRODUCTION

There has been a worldwide explosion in e-commerce as companies of all sizes sell physical and digital goods online. The COVID-19 pandemic greatly accelerated the rise of digital commerce, and fraudsters have quickly followed by exploiting existing weaknesses and finding new, creative methods of committing their crimes. Merchants are constantly challenged to strike the right balance between a great customer experience and minimizing fraud losses. Traditionally, there are two points in the customer journey when risk is assessed: at the time of login and at the time of purchase. Fraud departments, usually residing in operations, are commonly focused on stopping fraudsters. They have earned a reputation as the "sales prevention" group. However, forward-thinking companies have elevated fraud management as a critical business function and leveraged it to increase revenue by approving more good orders and continuous risk management along the entire customer journey. This paper explores this new way of viewing fraud management and how merchants of all sizes can position themselves for future e-commerce growth.

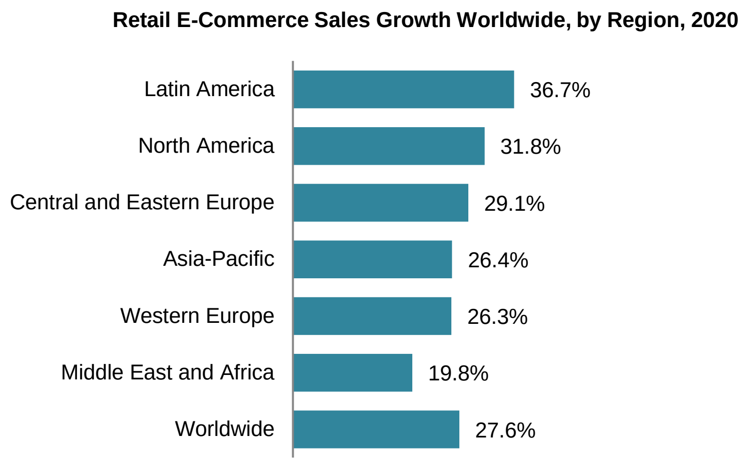
METHODOLOGY

This paper is based on primary and secondary research conducted by Aite Group as well as informational briefings with a number of solution providers and merchants.

THE E-COMMERCE EXPLOSION

While e-commerce has been steadily growing for several years, the pandemic has kicked it into overdrive as the world transformed seemingly overnight into a digital-first economy. Online sales growth percentages have been in the mid-teens throughout most of the past decade versus in-store sales growth in the low single digits. In 2020, global e-commerce sales growth averaged an astounding 27.6% (Figure 1).

Figure 1: Regional Retail E-Commerce Sales Growth in 2020



Note: Includes products or services ordered using the internet, regardless of the method of payment or fulfillment; excludes travel and event tickets, payments such as bill pay, taxes or money transfers, food services and drinking place sales, gambling and other vice goods sales

Source: eMarketer and InsiderIntelligence.com

Latin America, North America, and Central and Eastern Europe lead the way with e-commerce growth above the global average. In the United States, e-commerce sales leaped nearly 32%, and a supermarket cracked the ranks of the top 10 e-retailers due to its buy online, pick up in store/curbside service. In a three-month span, the pandemic drove growth in U.S. online sales that would have traditionally taken 10 years.

Mobile devices and fulfillment services are a strong contributing factor in driving online sales, especially in areas of the world that lack traditional landline-based telecommunications. As of December 2020, 5.24 billion people own a smartphone, representing 67% of the world's population.[1] Latin America, the Middle East and Africa, and people living in remote, nonurban areas of the world gained access to markets and businesses via mobile devices and delivery

[1] "How Many Smartphones Are in the World?" BankMyCell, accessed January 12, 2021, https://www.bankmycell.com/blog/how-many-phones-are-in-the-world.

services that have been traditionally off limits in the past. By 2023, 22% of all retail sales is forecast to be conducted online.[2]

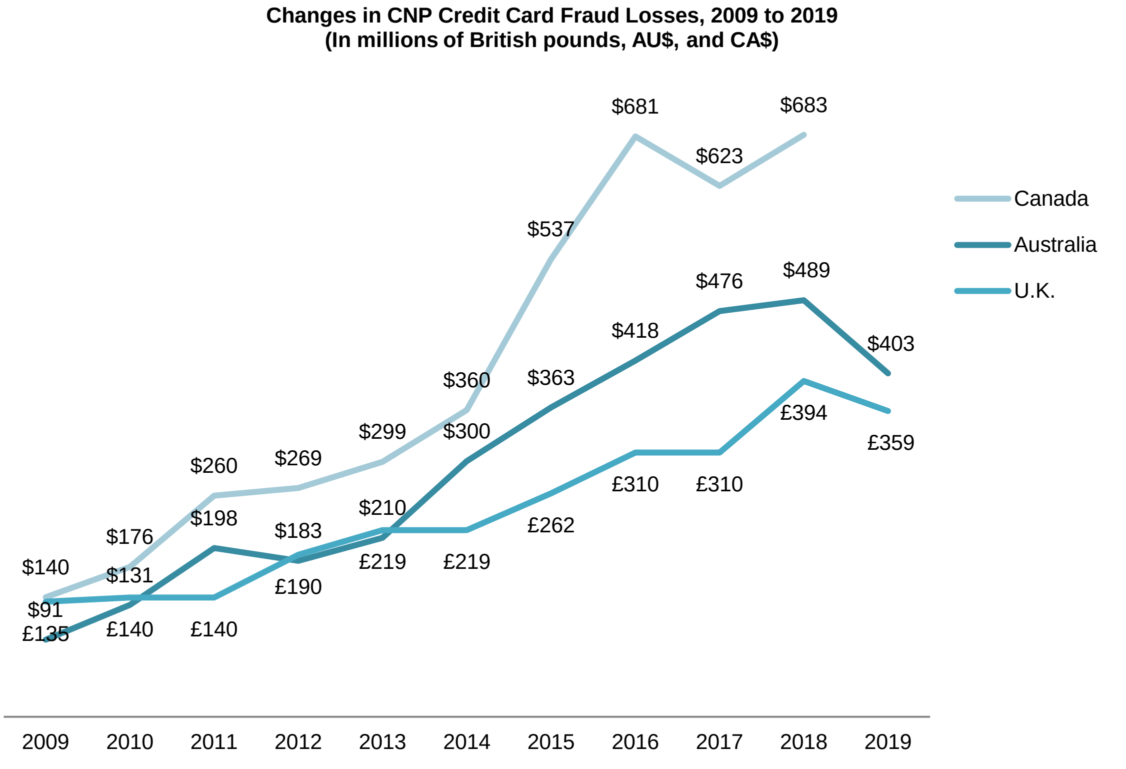
FOLLOWING THE MONEY

While businesses are keenly aware of the growth in online sales, so are the fraudsters. Card-based payments, which are the predominant method of payment for online purchases, are not protected by EMV technology and, therefore, are an easy target. The card brands protect cardholders from fraudulent transactions via a $0 liability policy. As such, the brands have defined a suite of rules to assign financial liability to either the financial institution or the merchant. Generally speaking, e-commerce fraud is a merchant liability, and with the growth in e-commerce fraud, merchants are actively seeking solutions to protect themselves. With industry estimates of global e-commerce fraud losses ranging between US$20 billion and US$30 billion annually, it is no surprise.

Some countries are better than others at mitigating e-commerce fraud. The U.K., Australia, and Canada experienced annual increases in CNP credit card fraud from 2009 until the mid to late 2010s. Over the past few years, these losses have decreased due to industry initiatives, government mandates, or a combination of each (Figure 2).

[2] Daniela Coppola, "E-Commerce Share of Total Retail Sales Worldwide From 2015 to 2023," Statista, November 26, 2020, accessed January 12, 2021, https://www.statista.com/statistics/534123/eCommerce-share-of-retail-sales-worldwide/.

Figure 2: Changes in CNP Credit Card Fraud Losses

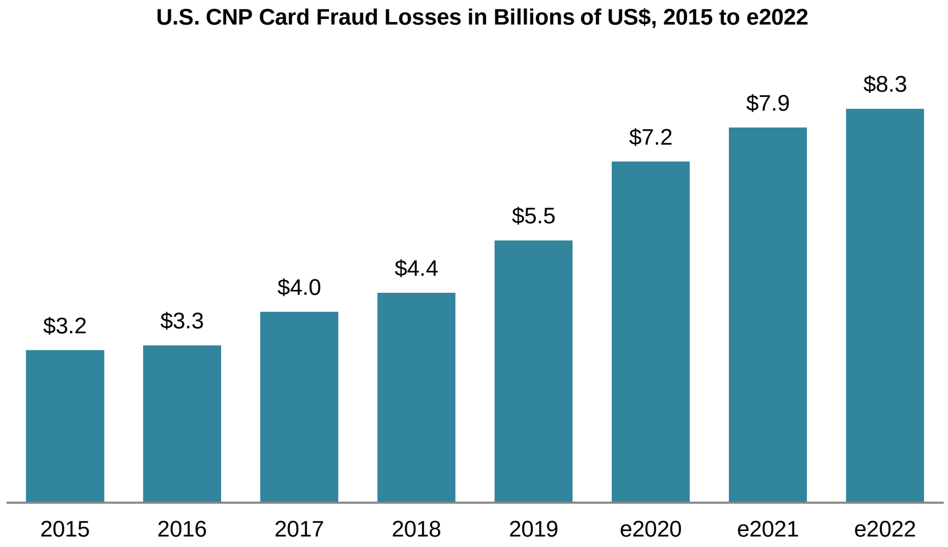


Changes in CNP Credit Card Fraud Losses, 2009 to 2019
(In millions of British pounds, AU$, and CA$)

Source: UK Finance, AusPay, Canadian Banking Association

In the United States, CNP card fraud losses have increased annually for a number of years and are projected to continue climbing through 2022. Part of this is due to merchant concerns about negatively impacting the consumer experience by adding friction in the shopping and checkout process (Figure 3).

Figure 3: U.S. CNP Fraud Losses

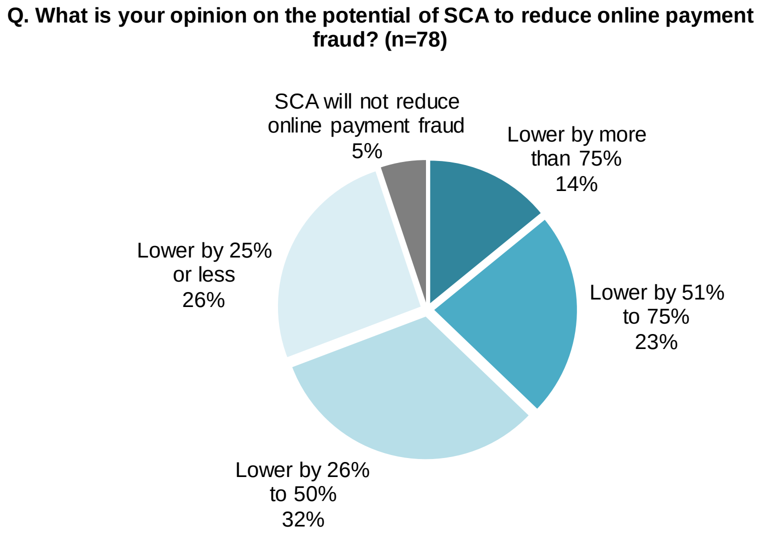


Source: Aite Group

The European Union (EU) has adopted new requirements to lower its e-commerce fraud. The strong customer authentication (SCA) component of the revised Payment Services Directive (PSD2) went into effect January 1, 2021, in most EU countries. Some notable exceptions and related compliance dates are Germany (March 15, 2021), France and Italy (April 1, 2021), and the U.K. (September 14, 2021). Companies doing business in the EU are required to deploy SCA on these dates. E-commerce transactions are further protected by this higher form of consumer authentication to lower CNP fraud losses. Based on a survey of 88 European payment executives in November 2019, Aite Group and the Merchant Payment Ecosystem (MPE) conference found a broad range of opinions as to the benefits SCA will deliver (Figure 4).[3] The rest of the world is watching closely to see how well the SCA rollout goes and its ultimate impact on fraud losses.

[3] See Aite Group's report *Strong Customer Authentication: Friend or Foe?*, January 2020.

Figure 4: Opinions on SCA's Impact on CNP Fraud



Source: Aite Group survey of 88 European payment executives in cooperation with MPE, November 2019

METHODS TO MITIGATE FRAUD

When deploying fraud mitigation solutions, merchants have two main areas of focus: either protecting the account or protecting the financial transaction.

ACCOUNT-BASED ANTI-FRAUD SOLUTIONS

Account-related fraud attacks target the customer's digital account with a merchant. Fraudsters use the wealth of personally identifiable information obtained from breaches to either create a new online account or take over a customer's existing account. Over 30 billion records have been breached since 2013 containing usernames, passwords, home addresses, phone numbers, and others, and that number continues to grow each year.

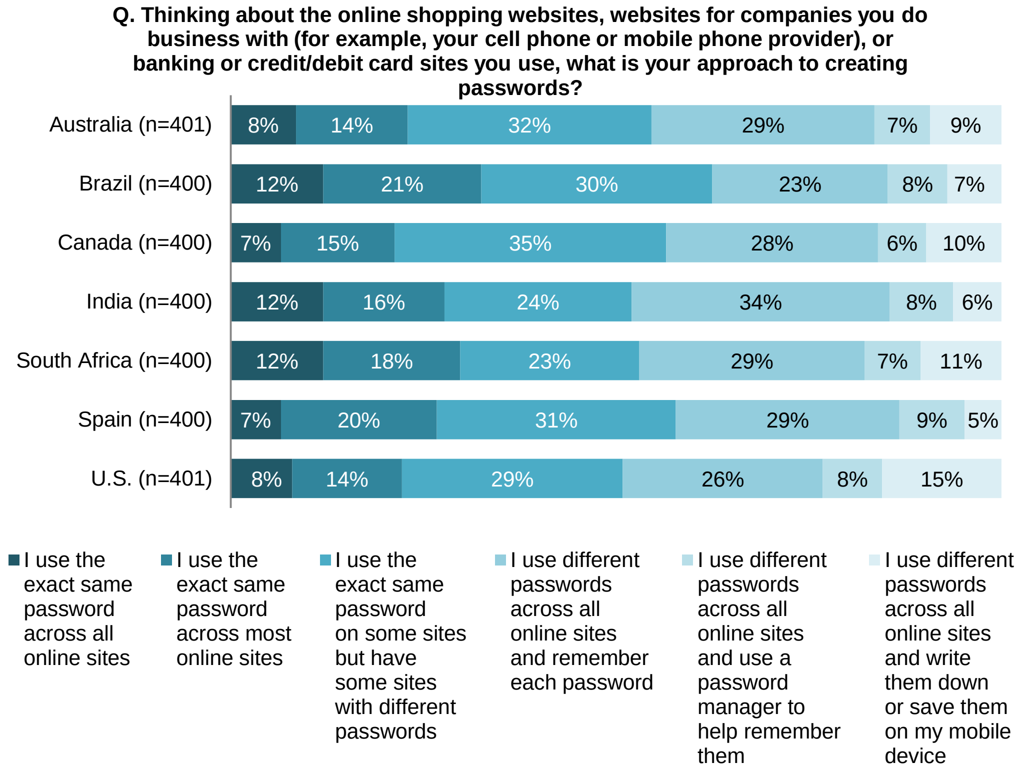
Users are notorious for reusing passwords across multiple sites as well as having weak passwords. An Aite Group survey found over half of consumers use the exact same password across some or all online sites (Figure 5).[4] Fraudsters can easily conduct large-scale testing to see which username/password combinations are valid. Once identified, chances are high that the credentials are good on other websites too. In a study of over 275 million compromised passwords by NordPass, three common passwords represented nearly 13% of the total ("123456," "123456789," and "password"). And only 44% of the passwords were unique.[5] It is no

[4] See Aite Group's report *Second Annual Global Security Engagement Scorecard™*, October 2017.

[5] "Top 200 Most Common Passwords of the Year 2020," NordPass, accessed January 12, 2021, https://nordpass.com/most-common-passwords-list/.

surprise that the account is under attack by fraudsters when such simple and repetitive passwords are used by online shoppers.

Figure 5: Global Consumers' Approach to Creating Passwords



Source: Aite Group's survey of 2,802 consumers, September 2016

Account-level fraud is hard to detect for myriad reasons. If a fraudster has access to a customer's username and password and uses it to log into their online account, it can be difficult to know whether it is the legitimate customer or a fraudster. This can be problematic in a couple of ways. One, if the online merchant stores the customer's credit or debit card data for future purchases, the fraudster can easily make a purchase and provide a ship-to address they control. Two, fraudsters can access the customer's loyalty program at an airline, hotel, or other favorite business and steal the loyalty points. Protecting both types of online accounts is growing more imperative.

Account-based fraud solutions come in many forms, such as verification services (identity, email address, government document), bot/credential stuffing, device fingerprinting, biometrics (physical, behavioral), mobile device authentication, and others. Some of these are passive solutions in that they are transparent to the user and provide a strong consumer experience. Other solutions are active in that some user engagement is required. Recently a combination of device fingerprinting and behavioral biometrics has proven to be effective at detecting fraud.

TRANSACTION-BASED ANTI-FRAUD SOLUTIONS

Transaction-related fraud attacks target online purchases in which stolen payment credentials (usually a credit or debit card) are used to acquire physical or digital goods that fraudsters can easily convert to cash. When a shopper clicks on the “Buy Now” button on the checkout page, the authorization is evaluated for potential fraud and an approve or decline decision is made. Merchants have the choice of invoking these tools pre-network (prior to sending the authorization to the card networks and financial institution) or post-network (after receiving a response from the card networks and financial institution). These fraud tools use a combination of machine learning (ML) and a rules engine to determine the appropriate action. In some cases, a suspicious authorization may be sent to a manual review team for human review and decisioning.

Most merchant efforts to mitigate fraud began at the transaction level. Transactional fraud tools have evolved over the years to include fraud detection at the account level. The benefit of a dual-pronged solution is that, prior to a transaction being generated, account-level data can inform a transaction-level ML model to improve fraud detection and increase approval rates. These combined solutions are sometimes referred to as orchestration hubs in which a central system acts as the symphony conductor and individual fraud solutions are musicians that make up the symphony. For merchants, hubs provide a single API that provides access to a holistic solution to protect both the account and the transaction, thus greatly simplifying implementation and ongoing operational management.

BALANCING THE CONSUMER EXPERIENCE

Regardless of whether a merchant uses account-based, transaction-based, or a combination of solutions, the consumer experience needs to be taken into consideration. Two terms merchants dislike are “friction” and “cart abandonment.” Friction is the number of actions a customer is required to perform in the process of making an online purchase. Those actions could be creating an online account, providing identification at the time of purchase, entering a one-time passcode (OTP) on a website, and others. Cart abandonment occurs when consumers add items to their shopping cart but do not complete the purchase of those goods or services. Friction can lead to cart abandonment and lost sales.

An Aite Group study of 1,400 consumers in the U.K., Singapore, and the U.S. on the impact friction has on cart abandonment revealed some interesting insights. Users viewed setting up an online account and providing additional proof of identity at time of payment very similarly. On average, 30% to 40% of users reported that these two types of friction would very likely lead them to abandon the e-commerce transaction. If asked to enter an OTP, 15% to 29% of users said they are very likely to abandon the transaction. The range is based on users self-identifying as a light, medium, or heavy e-commerce buyers. When examined from an age perspective, consumers 55 years old and older were slightly more willing to accept friction.[6] The best fraud solutions optimize the customer experience by applying risk-appropriate friction and only when needed to protect both the customer and the merchant.

[6] See Aite Group’s report *Global Consumers’ Authentication Preferences: Have Your Cake and Eat It Too*, September 2018.

FRAUD MANAGEMENT: LOSS PREVENTION VS. BUSINESS ASSET

Traditionally, the purpose of a fraud solution is to control and reduce fraud losses. The fraud department commonly resides in an operations group, and performance is measured by the amount of losses that are written off. In many situations, this has caused concern with internal stakeholders, such as e-commerce sales, finance, and marketing departments that are focused on maximizing sales. There is a common view that minimizing fraud requires some amount of customer impact in the form of fraud declines of good customers. It is an "either/or" scenario. A company can either limit its fraud losses or maximize its approval rates, but it cannot do both. In this conflicting environment, the fraud department sometimes has a reputation as the "sales prevention" department.

But does it have to be this way?

Instead of *either* lower fraud *or* higher approval rates, some merchants are working toward lower fraud *and* higher approval rates, striking a balance between these metrics to increase the number of good orders accepted. The fraud department is being elevated and working in partnership with other internal stakeholders to drive growth. Fraud management is viewed as a business asset and part of the planning process along with sales and marketing.

In one use case, a merchant's sales and marketing department planned a promotion in which various products were discounted to drive traffic to its website and increase sales. The fraud department was not informed about this. When the promotion launched, the fraud department noticed a substantial increase in traffic to its website and a spike in the number of purchases and average ticket amount. This caused the fraud system to generate alerts warning of abnormal behavior. Risk controls were deployed to limit activity and return to normal levels. Sales were lost, marketing dollars were wasted, and customers were upset (Figure 6).

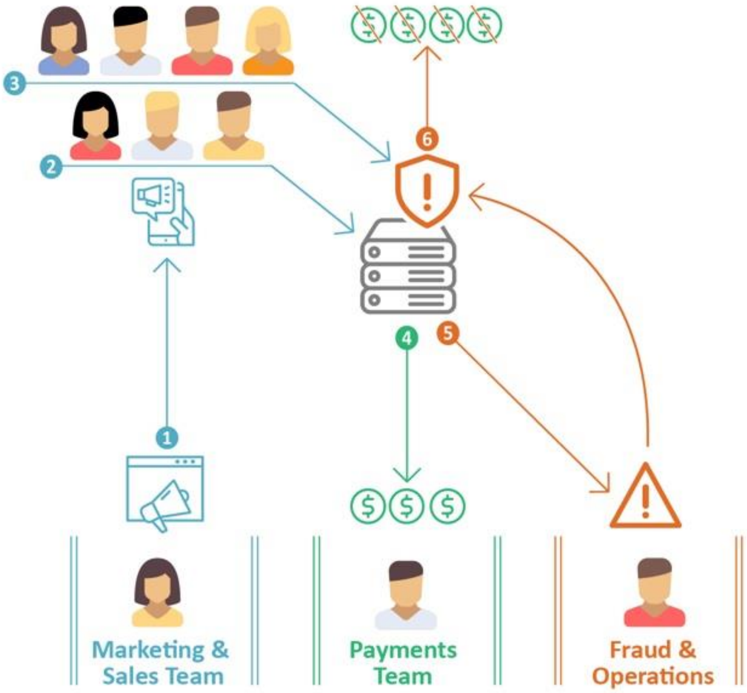
Figure 6: Siloed Business Environment

1. Sales and marketing team create and launch promotion

2 & 3. Customers receive promotion and go to website to make purchases

4 & 5. Some purchases are approved, but spike in traffic and orders alerts the Fraud department

6. Fraud department blocks orders to return to pre-spike levels



Source: Aite Group

Proactive merchants are breaking down organizational walls and bringing together sales, marketing, payments, fraud, and operations to communicate plans and share data to optimize fraud and risk strategies. For example, fraud tools can be modified to anticipate increased order activity and risk levels related to promotions. The payments team can share information on approval rates and work with the fraud team on plans to increase them. Operations can provide access to the order management system to give insights into loyal customers for whitelisting in the fraud system. The fraud department can leverage incoming chargebacks to educate the sales/marketing departments on consumer disputes to improve clarity on websites and/or increase the prominence of terms and conditions in the checkout flow. Working collectively, the fraud team can become a strategic asset to grow a merchant’s business (Figure 7).

Figure 7: Collaborative Business Environment

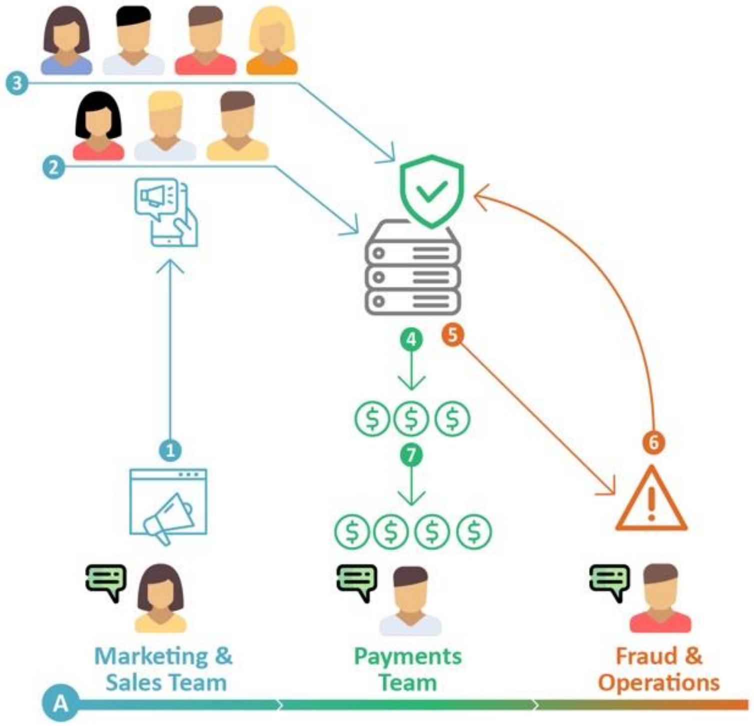
A. Sales, marketing, payments, fraud, and operations communicate plans and share data

1. Sales and marketing team create and send promotion

2 & 3. Customers receive promotion and make purchases on website

4 ,5, 6. Spike in web traffic and sales are approved by Fraud

7. Higher sales are realized



Source: Aite Group

MOVING TO PERFECTION

In a perfect world, a fraud tool identifies and approves all good transactions and declines all fraudulent transactions. A fraud system has two operating metrics that are within a merchant's control: false positives and false negatives. Effectively managing them can lead to higher sales and customer satisfaction.

False positives are when a good transaction is declined, causing customer dissatisfaction and internal inefficiencies. False negatives are when a fraudulent transaction is approved, resulting in a chargeback and financial loss to the merchant. Mitigating false positives maximizes a merchant's revenue, and optimizing false negatives minimizes a merchant's costs—a double business benefit.

False positives and negatives are measures of the effectiveness of a merchant's fraud strategies deployed within the fraud tool/system. Of the two, false negatives are easier to manage. Visa and Mastercard provide regular feedback to merchants on false negatives in the form of chargebacks marked with a fraud reason code. Visa provides this data in its TC40 file, and Mastercard provides it in its SAFE file. They can be mitigated by carefully analyzing chargebacks and making the appropriate adjustments to the fraud system. It is also a best practice to create a feedback loop into the fraud system's ML model by inputting known fraudulent transactions for the ML model to learn.

False positives are more difficult to manage because there is no definitive source of this information. In an ideal world, a merchant would call the cardholder of every declined transaction and ask if they performed that transaction. That is not realistic due to resource constraints and a lack of certainty about the phone number, which could be the cardholder's or the fraudster's. One source of this information is the call center. Good customers who are inadvertently declined may call to ask why they were denied. The fraud department should partner with the operations group to establish a mechanism to capture this valuable information. Another option is to adopt a common practice in the issuing world. Financial institutions commonly contact their cardholders about suspicious transactions via a text message, email, or interactive voice response (IVR) call to determine if they recognize them. Studies have shown that cardholders appreciate and value this practice, as it demonstrates that the financial institution is watching out for them. Merchants can do the same, creating goodwill with their customers and collecting valuable data on false positives for refining the fraud system performance. This would require use of an identity verification tool to ensure the phone number and email address belong to the cardholder and not the fraudster. A global e-commerce fraud report by Cybersource found that e-commerce merchants decline 2.5% of all orders due to a fraud concern.[7] Any reduction in this number is an immediate increase in sales without adding costs—a very attractive proposition for any e-commerce merchant.

[7] "2019 Global eCommerce Fraud Management Report," Cybersource, 2019, accessed March 3, 2021, https://www.cybersource.com/content/dam/cybs2019/documents/en/global-fraud-report-2019.pdf.

CONCLUSION

Fraudsters continue to evolve their attack vectors and increase the sophistication of their attacks. It requires constant diligence to ensure the appropriate defenses are in place. Yet fraud is not only about stopping the bad. Fraud can also be a strategic advantage to grow your online business. Effective companies treat fraud with the same level of importance as marketing, product, and sales. When the cogs of the machine are well oiled and work collaboratively, overall performance increases. It is no different in a business setting with the fraud department.

Specific takeaways for merchants follow:

- Online commerce is here to stay. Future busines winners are those who embrace it and optimize the experience for customers.
- Fraudsters are keenly aware of the shift in consumer preferences for and adoption of online shopping. This poses a business and financial risk to merchants that needs to be carefully managed.
- There is a plethora of commercial fraud mitigation solutions at the account level and the transaction level. Newer solutions offer orchestration hub capabilities that combine both types of solutions into one.
- Regardless of which fraud mitigation solutions are deployed, merchants need to carefully monitor the consumer experience to avoid adding too much friction, which can lead to cart abandonment.
- Managing fraud is no longer an operational function focused solely on minimizing losses. As online selling becomes more competitive, proactive merchants are elevating fraud management to drive growth.

ABOUT AITE GROUP

Aite Group is a global research and advisory firm delivering comprehensive, actionable advice on business, technology, and regulatory issues and their impact on the financial services industry. With expertise in banking, payments, insurance, wealth management, and the capital markets, we guide financial institutions, technology providers, and consulting firms worldwide. We partner with our clients, revealing their blind spots and delivering insights to make their businesses smarter and stronger. Visit us on the web and connect with us on Twitter and LinkedIn.

AUTHOR INFORMATION

David Mattei
+1.617.398.0908
dmattei@aitegroup.com

CONTACT

For more information on research and consulting services, please contact:

Aite Group Sales
+1.617.338.6050
sales@aitegroup.com

For all press and conference inquiries, please contact:

Aite Group PR
+1.617.398.5048
pr@aitegroup.com

For all other inquiries, please contact:

info@aitegroup.com