REPORT EXCERPT

Technology & Business Insight

Thought Leadership

April 2021

Fraud Prevention

A High-Stakes Customer Experience Battleground

Jordan McKee Principal Research Analyst, Customer Experience & Commerce

As digital sales accelerate under COVID-19, the objective for fraud prevention teams must broaden from preventing losses to preserving – and ideally elevating – their business's customer experience. Enterprises must reimagine their fraud prevention strategies as a framework for removing excess friction for loyal customers with the goal of deepening relationships through personalized customer journeys. This report presents the business case for taking action. Additionally, it identifies key strategies and vendors that can help B2C enterprises address fraud in a way that complements – not hinders – their end-to-end customer experience.

The following is an excerpt from an independently published 451 Research report, "Fraud Prevention: A High-Stakes Customer Experience Battleground" released in April 2021.

To purchase the full report or to learn about additional 451 Research services, please visit https://451research.com/products or email 451sales451@spglobal.com.

451 Research

S&P Global
Market Intelligence

Table of Contents

1. E-Commerce Acceleration Puts Focus on Fraud, Customer Experience 1

Figure 1: Global E-Commerce Experiences Dramatic Growth in 2020 . . . 1

A Challenging Online Fraud Landscape . . . 2

Figure 2: Rising Fraud Volume Puts Fraud Into Focus . . . 2

Figure 3: Fraud Is a Common Occurrence for Cardholders . . . 3

Fraud's Proliferation Across the Customer Journey . . . 4

Figure 4: Promotion Abuse Is a Widespread Issue . . . 5

The Multi-Pronged Impact of Fraud on Customer Relationships . . . 6

Fraud Prevention as a Customer Trust Factor . . . 6

Figure 5: Failure To Stop Fraud Jeopardizes Trust and Relationships . . . 6

Fraud Prevention as a Customer Experience Factor . . . 7

Figure 6: False Declines Are a Frequent Occurrence for Shoppers . . . 7

Figure 7: Unoptimized Approaches to Fraud Prevention Create Friction Across the Customer Journey . . . 8

2. Benchmarking the Elusive Balance Between Fraud Prevention and Customer Experience 9

Figure 8: Most Merchants Sacrifice Their CX for Fraud Prevention. . . . 9

Figure 9: The Four Common Fraud Prevention Approaches and Outcomes . . . 10

3. Constructing an Operationally Optimized Fraud Prevention Strategy 11

Figure 10: Fraud Is About Much More Than Financial Losses . . . 11

Merchant Fraud Prevention Vendors Expand Capabilities . . . 11

Identity Focus . . . 12

End-to-End, Integrated Capabilities . . . 12

Figure 11: Merchant Fraud Prevention Vendor Capability Sets . . . 13

Large, Diverse Data Sets . . . 13

Customizable Machine Learning Models . . . 13

Multiple Revenue Optimization Levers . . . 14

The Rise of Chargeback Guarantees . . . 14

Operationally Optimized Fraud Prevention: It Takes a Village . . . 15

Figure 12: Key Outcomes of an Operationally Optimized Fraud Prevention Strategy . . . 15

4. Conclusions 17

5. Further Reading 18

6. Index of Companies 19

1. E-Commerce Acceleration Puts Focus on Fraud, Customer Experience

Fraud's Proliferation Across the Customer Journey

It's important to note that card fraud is not the only source of fraud that merchants are up against. In recent years, 451 Research has observed various forms of non-transaction fraud increasingly proliferate across the customer journey. Touchpoints from online account creation through to product returns have emerged as growing vectors for fraudulent activity and consequentially, both financial and reputational losses. Notable sources include:

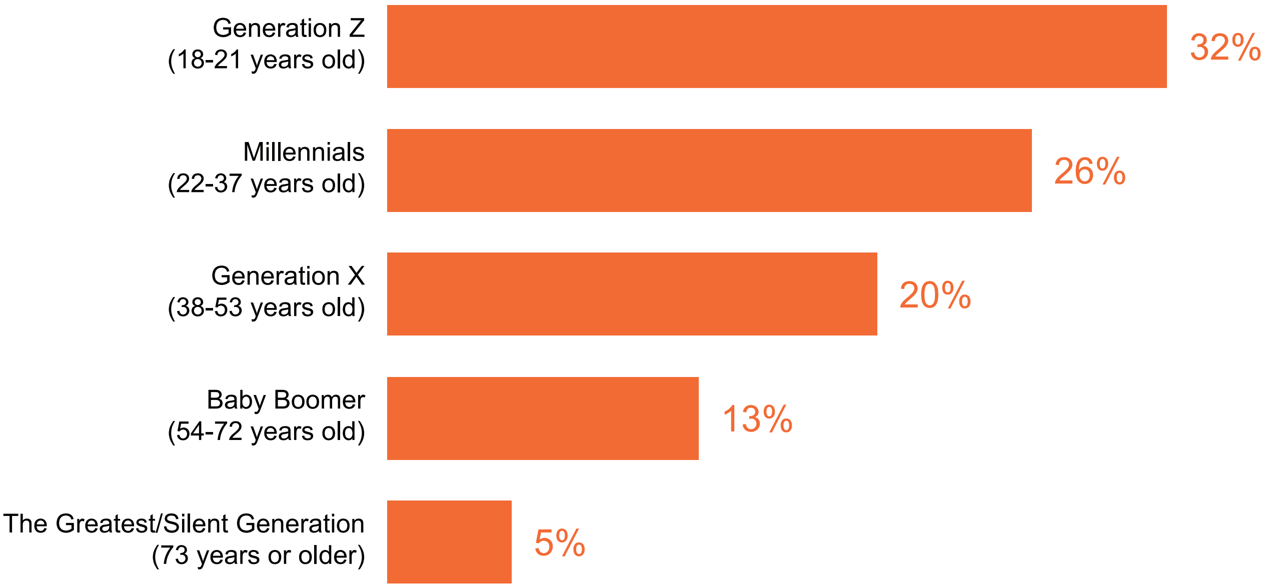
- **Account takeovers (ATO).** ATOs aren't a problem faced just by financial services organizations. Popular loyalty/rewards programs (e.g., hotels, airlines, restaurants) have become attractive targets for criminals, who either drain rewards currencies/benefits themselves, or sell the login credentials on the dark web. Bots have become an increasingly popular tool for fraudsters' ATO efforts, helping to automate and expand their attack opportunity. Reputational damage, declines in profitability and costs to replace stolen points are all common outcomes of ATOs.
- **New account fraud.** Fraudsters often create multiple fake loyalty/rewards accounts to aid in various schemes, such as transferring rewards currencies from an account they have illegitimately taken over into the new account they have created. Aside from the fraud implications, new account fraud creates increased challenges for merchants in discerning a legitimate customer interaction from a fraudulent one.
- **Buy online pick-up/return in-store (BOPIS/BORIS) fraud.** The proliferation of omnichannel commerce has created major new vectors for criminals. BOPIS shopping experiences that have been in vogue during the pandemic enable fraudsters to quickly obtain fraudulently purchased goods and circumvent traditional manual review cycles and billing/shipping address matching. BORIS provides an efficient way for fraudsters to 'cash out' goods that were fraudulently purchased online and receive a gift card, which they can then resell online through gift card marketplaces.

Concerningly, many emerging types of fraud are also committed by non-traditional fraudulent actors, including otherwise 'good' customers who are attempting to game the system by abusing both merchant and issuer business policies (e.g., policy abuse). This type of fraud can be difficult to detect, and tackling it creates a unique challenge for merchants, which must carefully and delicately address instances of abuse to minimize the impact on lifetime value, as well as on their overall customer base. Several examples include:

- **Promotion abuse.** Merchants needlessly give up margin when customers take advantage of promotions. This can take a variety of forms, including shoppers creating multiple email addresses to access multiple new customer discount codes, or oversharing 'refer a friend' discount codes outside of their network (e.g., posting to Craigslist). This is a widespread issue, with a third of Gen Z consumers and a quarter of millennials admitting to using different email addresses or other contact information to access promotions/discounts multiple times (see Figure 4).

- **Return abuse.** Merchants with lenient return policies often fall victim to abuse and can lose revenue when returned items must be discarded or resold at a discount. The tactics here are many, and include wardrobing (e.g., purchasing an item with the intent to return it), switch fraud (e.g., purchasing a new item and returning the old/defective item) and 'brick in a box' fraud (e.g., returning an item, such as an electronic, with certain parts removed). Several merchants have been forced to revise lifetime guarantees due to abusive customer behavior.
- **Item not received (INR) fraud.** INR fraud involves customers notifying a merchant that their online order was never received (when in fact it was) and demanding a refund (or new shipment) of the item. Merchants that have been overloaded with digital orders simply lack the time to investigate each INR incident and often find refunding the order is the path of least resistance.
- **Reseller abuse.** This occurs when unauthorized resellers purchase product in bulk, often employing bots, and resell it themselves. One footwear retailer we spoke with noted that reseller abuse is a significant problem for 'drops' (e.g., limited release of a particular item). Bots can wipe out all or most of the drop inventory, blocking loyal customers from making a purchase.
- **Friendly fraud.** A problem that has grown during the pandemic, this involves customers contacting their card issuers to request a refund for an item on their statement they claimed to have not authorized (when in fact, they had). Investigating and providing evidence to refute these types of disputes can quickly overwhelm fraud teams if the right processes and documentation are not in place.

Figure 4: Promotion Abuse Is a Widespread Issue



Q. Which of the following actions have you taken when shopping online? (Check all that apply) - Use different email addresses or other contact information to access promotions/discounts multiple times

Base: All respondents (n=1,256)

Source: 451 Research's Voice of the Connected User Landscape: Connected Customer (Consumer Population Representative), Trust & Privacy 2020

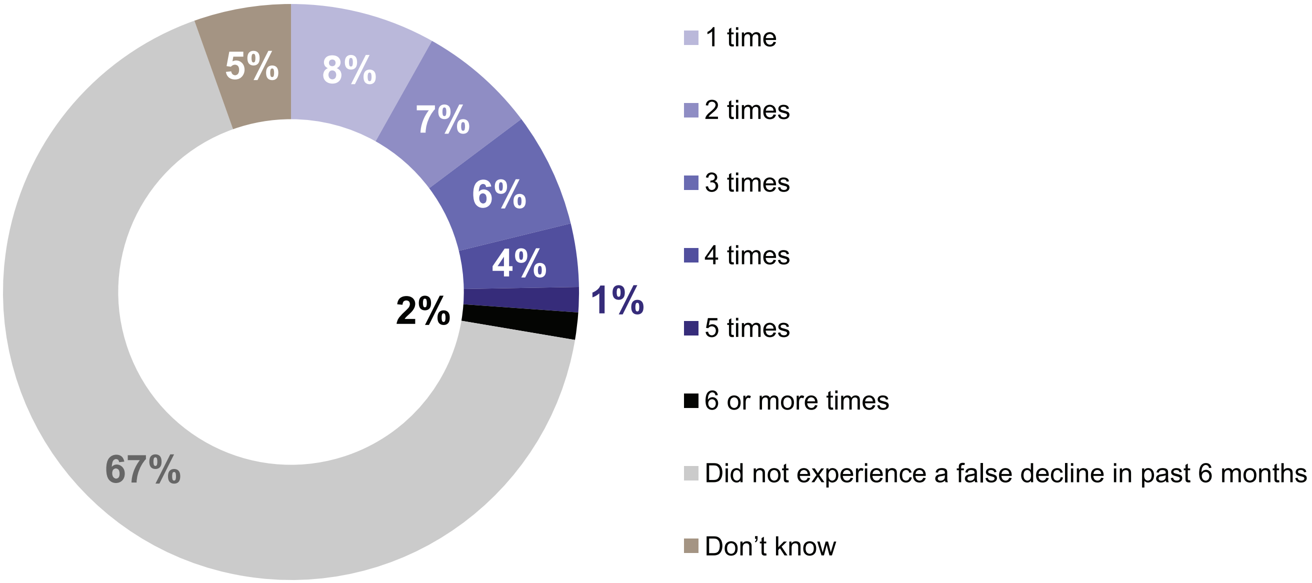
While policy abuse may seem somewhat innocuous on the surface, the impact can quickly put pressure on margins and the bottom line. In 2018, L.L. Bean revoked its lifetime product guarantee after noting that about 15% of its returns were classified as abusive, amounting to $250m in losses over a five-year span. Decisions such as this, while addressing the problem at hand, have the unfortunate consequence of compromising relationships with loyal customers who the business policies were intended for.

Fraud Prevention as a Customer Experience Factor

With more customer interactions and sales dollars moving online, the stakes for delivering a compelling digital experience are increasing. Online, a better experience is just a click or a tap away, and a single friction point can be enough to drive an abandoned cart and send shoppers looking elsewhere. In fact, of the 47% of shoppers who abandoned an online shopping cart in the last six months due to difficulties in completing the purchase, more than two-thirds ended up not purchasing the item at all, or purchased it from a different retailer, according to 451 Research's VoCUL: Connected Customer, Quantifying the Customer Experience 2020 survey. Now more than ever, fraud prevention must be thought as an essential input into the CX and revenue growth.

Among the most common byproducts of unoptimized, overly restrictive fraud controls are false declines – a jarring CX that has led more than quarter of consumers to abandon a purchase over the past six months. Concerningly, more than 1 in 10 consumers have abandoned a transaction due to a false decline more than three times in this span (see Figure 6). Our research indicates that younger shoppers are disproportionately impacted by false declines, in part due to their online shopping frequency. Consider that compared to Baby Boomers, millennials are more than six times as likely to have experienced a false decline over the past 90 days, according to our VoCUL: Connected Customer, Loyalty & Retention 2020 survey. Merchants that unintentionally turn millennials away risk damaging their relationship with this high-impact, high-growth demographic for good.

Figure 6: False Declines Are a Frequent Occurrence for Shoppers



Q. In the past 6 months, how many times – if any – have you abandoned a purchase because one of your transactions was falsely declined?

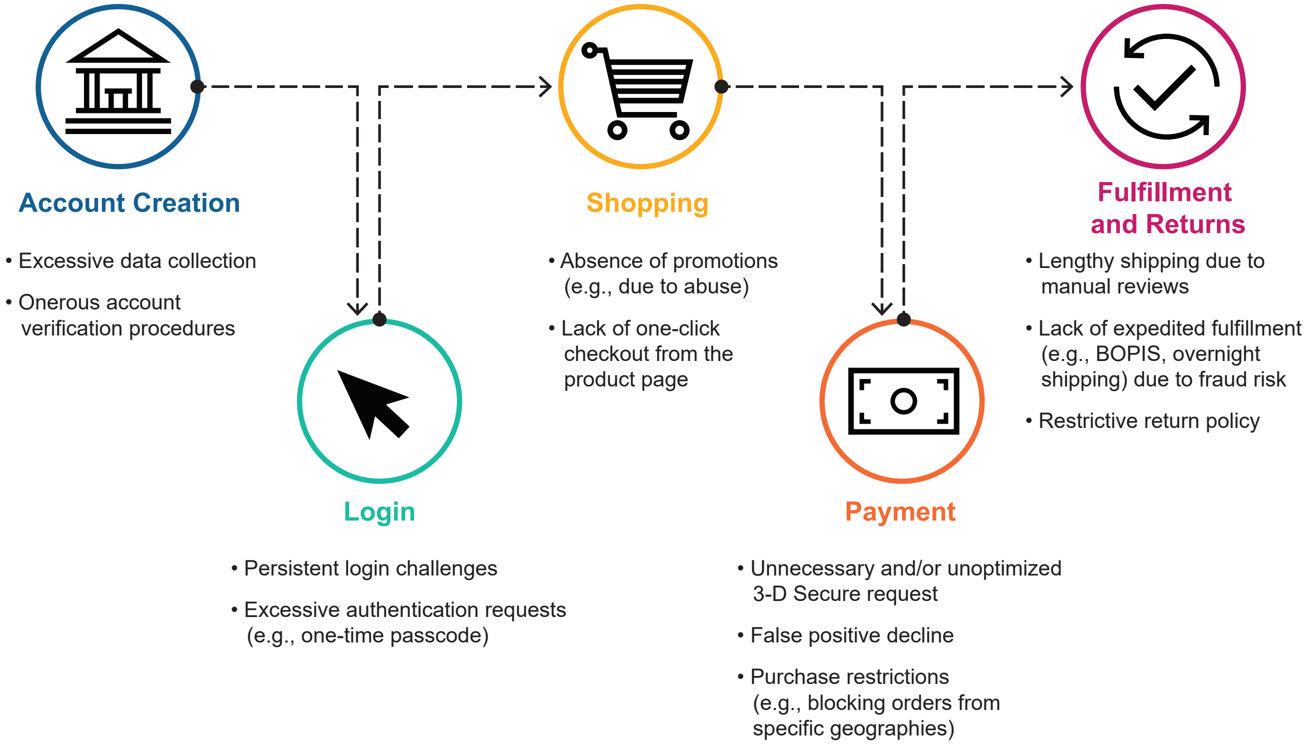
Base: All respondents (n=1,634)

Source: 451 Research's Voce of the Connected User Landscape: Connected Customer (Consumer Population Representative), Quantifying the Customer Experience 2020

Revenue turned away due to false declines often far outweighs revenue impacted by fraud losses. But the total impact of false declines goes beyond compromising upfront sales. According to our VoCUL: Connected Customer, Quantifying the Customer Experience 2020 survey, 30% of consumers say that if a transaction is mistakenly declined despite having sufficient funds in their account, it would significantly influence their likelihood to *stop shopping* with a preferred brand or retailer. Merchants must view false declines as a direct threat to customer lifetime value. This threat has only become exacerbated by the pandemic. New shoppers coming online for the first time against the backdrop of unconventional purchasing trends (e.g., high order velocity, bulk purchasing, billing/shipping address mismatches due to quarantines) have wreaked havoc on underprepared merchants' fraud rules and risk scoring systems. Valued customers will continue to be mistakenly turned away if a plan for adaptation is not in place.

While false declines are a persistent headache for fraud management and CX pros alike, they are only part of the problem. Unoptimized fraud prevention strategies can create friction at multiple touchpoints across the journey as businesses take a reactive approach to new challenges. Dialed-back policies (e.g., returns, promotions), inabilities to craft VIP experiences (e.g., one-click checkout) and inefficient shopping experiences (e.g., lengthy shipping due to manual review cycles) are common outcomes of unoptimized, reactive approaches to fraud (see Figure 7). So too are roadblocks to innovation. We have spoken with numerous enterprises that have avoided entry to international markets or pulled back on the launch of new initiatives (e.g., a subscription offering) due to fraud concerns. Without an ability to effectively discern good customers from criminals, the end-to-end CX, and the business, inevitably suffer.

Figure 7: Unoptimized Approaches to Fraud Prevention Create Friction Across the Customer Journey


Account Creation
• Excessive data collection
• Onerous account verification procedures
Shopping
• Absence of promotions (e.g., due to abuse)
• Lack of one-click checkout from the product page
Fulfillment and Returns
• Lengthy shipping due to manual reviews
• Lack of expedited fulfillment (e.g., BOPIS, overnight shipping) due to fraud risk
• Restrictive return policy
Login
• Persistent login challenges
• Excessive authentication requests (e.g., one-time passcode)
Payment
• Unnecessary and/or unoptimized 3-D Secure request
• False positive decline
• Purchase restrictions (e.g., blocking orders from specific geographies)

Source: 451 Research, 2021

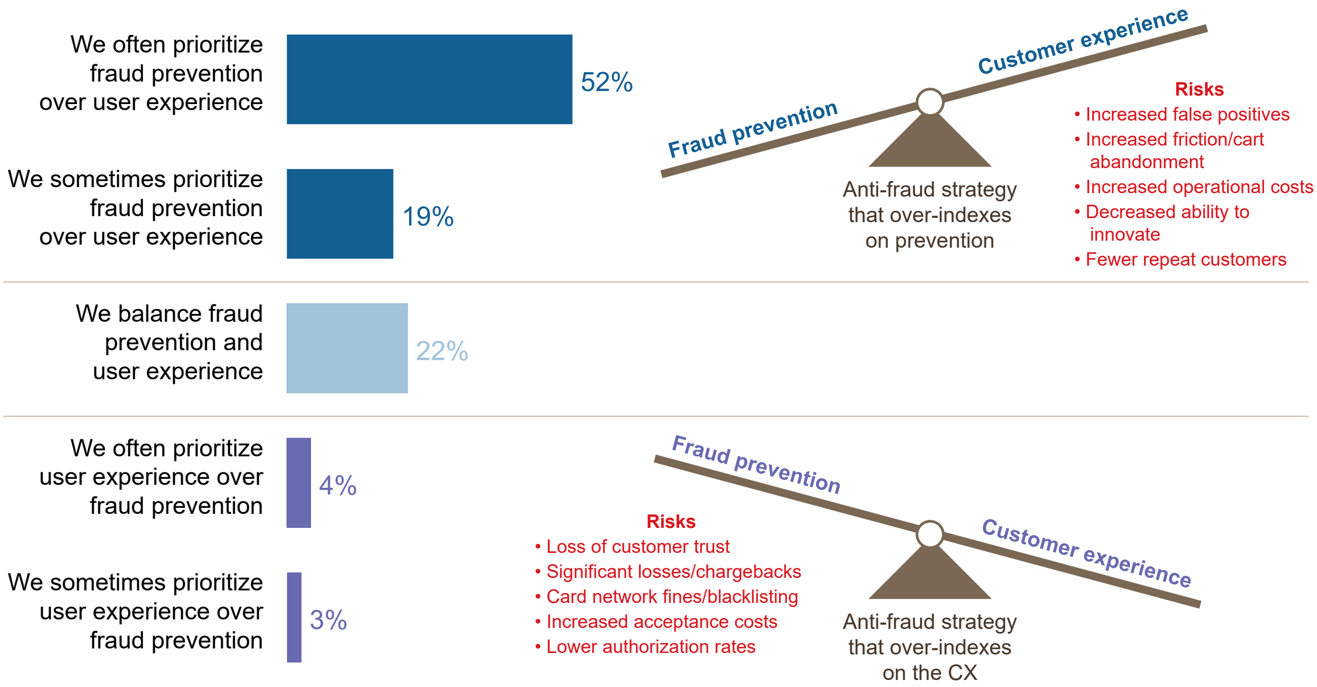
2. Benchmarking the Elusive Balance Between Fraud Prevention and Customer Experience

Striking a balance between fraud management and CX continues to be an elusive goal for many of the enterprises we speak with. Our VotE: CXC, Merchant Study 2020 indicates that 79% of merchants strongly or moderately agree that their approach to fraud prevention makes it challenging to provide a smooth CX. This rises to 87% for online-centric merchants.

When it comes to picking a side, online merchants tend to sacrifice their CX for fraud prevention. Nearly three in four online merchants say they often or sometimes prioritize fraud prevention over their CX. This can result in a host of consequences that negatively impact sales, costs and customer loyalty (see Figure 8).

On the other end of the spectrum, a much smaller but still notable percentage of merchants have put their CX ahead of their fraud prevention strategy. The consequences of this approach can be especially dire. Aside from jeopardizing customer trust and seeing losses mount, enterprises that let fraud prevention take a backseat may see their decline rates spike as card issuers raise their guard and become increasingly conservative about the transactions they approve. They may also face increased acceptance costs if they are deemed high-risk by their processor, experience fines from the card networks if their chargeback ratio exceeds certain thresholds, and at worst, become blacklisted from accepting card payments if they are unable to get fraud levels in check.

Figure 8: Most Merchants Sacrifice Their CX for Fraud Prevention



Q. Which of the following best describes your organization's current approach to fraud prevention?

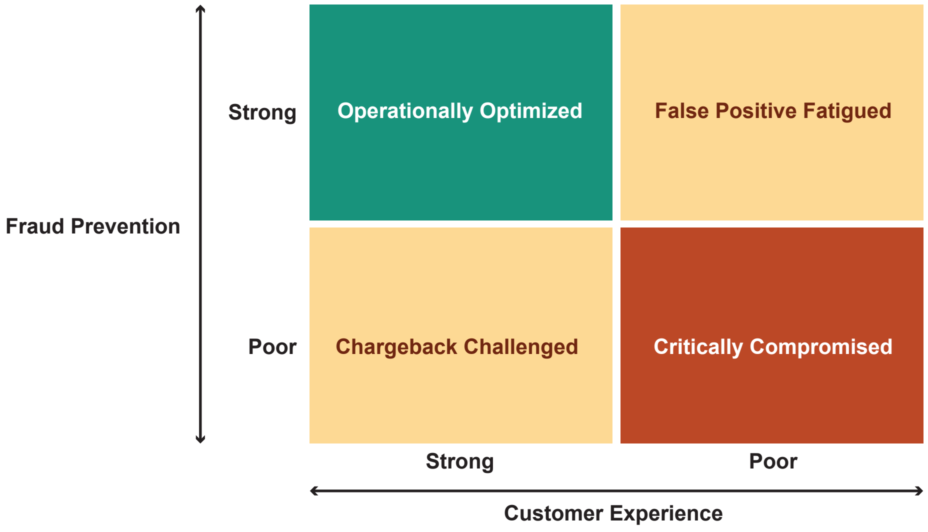
Base: Merchants with half or more of 2019 sales occurring online (n=114)

Source: 451 Research's Voice of the Enterprise: Customer Experience & Commerce, Merchant Study 2020

We typically see merchant fraud prevention strategies fall into four different buckets (see Figure 9):

- **False positive fatigued.** By putting fraud prevention ahead of their customer experience, these merchants run the risk of high rates of false positives and friction across the customer journey, resulting in lost sales. Risk-averse merchants entering new and unfamiliar markets, as well as those that are overly reliant on manual reviews and/or rules-based systems, can often fall into this category.
- **Chargeback challenged.** With a strong CX but a weak fraud prevention strategy and/or execution, dangerously high chargeback ratios are a major concern for these types of merchants. Significant losses and card network-mandated chargeback monitoring programs are common outcomes. We often see merchants experiencing hyper-growth, those new to e-commerce and those overly reliant on manual reviews and/or rules-based systems in this cohort.
- **Critically compromised.** A combination of a poor CX and fraud prevention strategy compromises both top- and bottom-line growth for these merchants. Merchants employing only static rules and/or 'hot lists' and those with a highly reactive approach to chargebacks commonly find themselves in this category. Without a near-term strategy change, critically compromised merchants face a greater risk of business-ending consequences.
- **Operationally optimized.** These merchants have struck a rare balance of both strong fraud prevention and a strong CX, creating an efficient and optimized business. Effective use of automation, intelligence and data supports top- and bottom line growth in the form of high approval rates and low chargeback rates for operationally optimized businesses. Our research shows just one in five merchants believe they have an operationally optimized fraud prevention strategy.

Figure 9: The Four Common Fraud Prevention Approaches and Outcomes



Source: 451 Research, 2021

Although difficult to execute, the business case for an operationally optimized fraud prevention strategy is compelling. Compared to the average merchant, our VotE: CXC, Merchant Study 2020 shows that enterprises with an operationally optimized fraud prevention strategy can experience:

- **Improved conversions.** Just 13% of operationally optimized merchants are concerned about the conversion rate impact of fraud compared to the average of 20%.
- **Less fraud.** Less than one in three (31%) operationally optimized merchants have seen an increase in fraud volume over the past year compared to the average of 58%.
- **Better CX.** Little more than one in four (27%) operationally optimized merchants strongly agree their approach to fraud prevention makes it challenging to provide a smooth CX compared to the average of 42%.

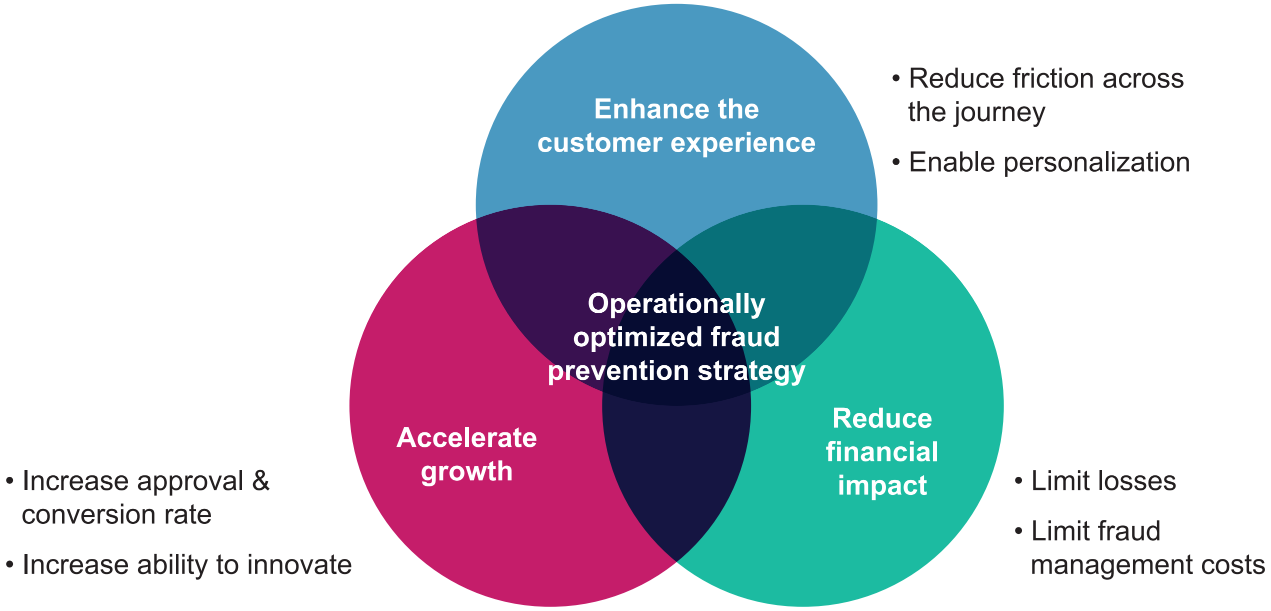
3. Constructing an Operationally Optimized Fraud Prevention Strategy

Operationally Optimized Fraud Prevention: It Takes a Village

Building out an operationally optimized fraud prevention strategy requires more than just aligning with the right partner. It requires introspection and collaboration. As a first step, enterprises should level-set the ability of their current strategy to deliver on three key outcomes (see Figure 12):

- **Enhance the CX.** How effectively does our fraud prevention strategy streamline the path to purchase for legitimate shoppers and introduce friction only when deemed absolutely necessary?
- **Accelerate growth.** Is our fraud prevention strategy architected in a way that helps the business accelerate growth, such as by minimizing false positives, decreasing cart abandonment and providing a platform for business innovation?
- **Reduce financial impact.** How well does our fraud prevention strategy mitigate losses while optimizing our use of internal resources?

Figure 12: Key Outcomes of an Operationally Optimized Fraud Prevention Strategy


Enhance the customer experience
• Reduce friction across the journey
• Enable personalization
Operationally optimized fraud prevention strategy
Accelerate growth
• Increase approval & conversion rate
• Increase ability to innovate
Reduce financial impact
• Limit losses
• Limit fraud management costs

Source: 451 Research, 2021

Ultimately, delivering on these outcomes is a task bigger than fraud and risk management teams alone. An operationally optimized approach to fraud demands that enterprises break down the organizational, experiential and technology silos that exist at touchpoints across the customer journey. This requires collaboration between a variety of teams, including fraud/risk, CX, information security, payments, e-commerce, operations and marketing. While challenging, 451 Research believes this is an essential step to establish a unified vision and strategy for improving the CX and fraud rates across the end-to-end customer journey. One large enterprise we spoke with accomplished this with the creation of a digital experience center of excellence, of which fraud management is a key focus of. The group brings together cross-functional viewpoints, strategies, data sharing and technology buying to better secure and optimize their end-to-end digital customer journey.

Above all else, it’s important to view fraud prevention as an ongoing exercise in optimization. Static rules and policies foster a reactive approach to fraud, which will prove detrimental in more ways than one. One merchant we spoke with noted that while it collected the CVV2 on nearly 95% of its transactions, it never investigated the fraud rates for those transactions where the CVV2 was not collected. Upon deeper analysis, the company discovered more than 90% of fraud stemmed from transactions where a CVV2 was not present. Another, after conducting a much-overdue inventory of its fraud rules, uncovered several, years-old undocumented rules that no longer made sense for the business. Reviewing fraud rules and policies on at least a monthly basis is a sound practice to adopt.

Tracking a broad range of KPIs beyond traditional metrics such as chargeback ratios and approval rates is another optimization best practice. Several examples include the incident rate of specific chargebacks (e.g., item-not-received, significant not-as-described), chargeback ‘win rates,’ authorization rates, checkout abandonment rates, manual review rates and false decline rates. Diverse KPIs help to tell a more granular and accurate story on the overall effectiveness – and impact – of a fraud prevention strategy.

For fraud prevention to be truly effective, constant honing, evolution and input from across the organization is required to accommodate shifting business and customer priorities. Keeping pace with changing business needs ensures fraud prevention supports, not hinders, innovation and growth.

CONTACTS

The Americas
+1 877 863 1306
market.intelligence@spglobal.com

Europe, Middle East & Africa
+44 20 7176 1234
market.intelligence@spglobal.com

Asia-Pacific
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence

These materials have been prepared solely for information purposes based upon information generally available to the public and from sources believed to be reliable. No content (including index data, ratings, credit-related analyses and data, research, model, software or other application or output therefrom) or any part thereof (Content) may be modified, reverse engineered, reproduced or distributed in any form by any means, or stored in a database or retrieval system, without the prior written permission of S&P Global Market Intelligence or its affiliates (collectively, S&P Global). The Content shall not be used for any unlawful or unauthorized purposes. S&P Global and any third-party providers, (collectively S&P Global Parties) do not guarantee the accuracy, completeness, timeliness or availability of the Content. S&P Global Parties are not responsible for any errors or omissions, regardless of the cause, for the results obtained from the use of the Content. THE CONTENT IS PROVIDED ON "AS IS" BASIS. S&P GLOBAL PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS, THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED OR THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION. In no event shall S&P Global Parties be liable to any party for any direct, indirect, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees, or losses (including, without limitation, lost income or lost profits and opportunity costs or losses caused by negligence) in connection with any use of the Content even if advised of the possibility of such damages.

S&P Global Market Intelligence's opinions, quotes and credit-related and other analyses are statements of opinion as of the date they are expressed and not statements of fact or recommendations to purchase, hold, or sell any securities or to make any investment decisions, and do not address the suitability of any security. S&P Global Market Intelligence may provide index data. Direct investment in an index is not possible. Exposure to an asset class represented by an index is available through investable instruments based on that index. S&P Global Market Intelligence assumes no obligation to update the Content following publication in any form or format. The Content should not be relied on and is not a substitute for the skill, judgment and experience of the user, its management, employees, advisors and/or clients when making investment and other business decisions. S&P Global Market Intelligence does not endorse companies, technologies, products, services, or solutions.

S&P Global keeps certain activities of its divisions separate from each other in order to preserve the independence and objectivity of their respective activities. As a result, certain divisions of S&P Global may have information that is not available to other S&P Global divisions. S&P Global has established policies and procedures to maintain the confidentiality of certain non-public information received in connection with each analytical process.

S&P Global may receive compensation for its ratings and certain analyses, normally from issuers or underwriters of securities or from obligors. S&P Global reserves the right to disseminate its opinions and analyses. S&P Global's public ratings and analyses are made available on its Web sites, www.standardandpoors.com (free of charge) and www.ratingsdirect.com (subscription), and may be distributed through other means, including via S&P Global publications and third-party redistributors. Additional information about our ratings fees is available at www.standardandpoors.com/usratingsfees.