Beyond eCommerce Fraud:

How Retailers Can Prevent Customer Policy Abuse

November 2021

PYMNTS.com | FORTER

Beyond eCommerce Fraud: How Retailers Can Prevent Customer Policy Abuse a PYMNTS and Forter collaboration, is based on responses from 100 executives who have leadership responsibilities in customer service and experience and fraud prevention and come from retail organizations that had at least $100 million in revenue in 2020. The survey was conducted from Aug. 25 to Sept. 14.

TABLE OF CONTENTS

PYMNTS.com | FORTER

Beyond eCommerce Fraud: How Retailers Can Prevent Customer Policy Abuse was produced in collaboration with Forter, and PYMNTS is grateful for the company's support and insight. **PYMNTS.com** retains full editorial control over the following findings, methodology and data analysis.

Introduction

Cybercrime and fraud tend to steal the spotlight whenever they appear. Intense interest from the media and heavy scrutiny from law enforcement and regulatory agencies about fraud and security breaches virtually guarantee that eCommerce businesses are aware of the impact on businesses and on consumer trust. Less well-known and well-covered in the media is another type of fraud risk facing eCommerce businesses: known customers perpetrating policy abuse.

PYMNTS' research reveals that policy abuse costs retailers with more than $100 million in revenue in the United States as much as $89 billion per year. The most common acts of abuse, including asking for refunds for items that have been partially used and lying online that an item was never received, are often simple to execute. Because these schemes require little to no technical sophistication to accomplish, virtually anyone — bad actors or good customers — could engage in these acts, making it difficult for businesses to prepare for and react to these risks. The cost associated with not addressing policy abuse head-on is significant, yet many businesses fail to adequately identify vulnerabilities, often giving customers the benefit of the doubt or preferring to err on the side of the adage that "the customer is always right."

Beyond eCommerce Fraud: How Retailers Can Prevent Customer Policy Abuse, a collaboration with Forter, examines findings from a survey conducted between Aug. 25 and Sept. 14 of 100 executives representing businesses in the retail sector that generate at least $100 million in annual revenue and who possess intimate knowledge of — and leadership responsibilities for — customer service, the customer experience and fraud prevention. Our research reveals the surprising scale of policy abuse, the challenges eCommerce companies face in combating abuse and the pathways firms might follow to secure their organizations against policy abuse.

Understanding the most common types of policy abuse

All varieties of policy abuse are liable to impact retailers' revenues, but different types can be more or less damaging and expose merchants to different levels of risk. The odds of each approach turning into serial abuse can also vary.

- **Item not received (INR) abuse** occurs when a customer makes a purchase and then falsifies a report claiming theft or nondelivery.
- **Return abuse** occurs when a consumer returns items to a retailer when those items are not eligible for return.
- **Promotion abuse** occurs when one consumer uses multiple accounts to take undue advantage of rewards, sales or other promotions.

Promotion abuse is perhaps the easiest type of fraud for consumers to execute, as misused discount codes, free trials or scanned physical coupons can create "extreme" discounts that are used and reused well beyond their original intent. INR abuse requires a consumer to make an initial, legitimate purchase but grants either a refund or a reshipment of items. Return abuse likewise may mean the consumer uses an item but spends no money at all if they are granted a full refund after they return it. Because many eCommerce companies manage returns and complaints exclusively through customer service portals, identifying, tracking and blocking offenders, especially sophisticated serial abusers, is challenging without a comprehensive, technology-driven system that eliminates vulnerabilities.

© 2021 PYMNTS.com All Rights Reserved

The need for insight and control: Policy abuse is costing U.S. retailers more than $89 billion per year

The eCommerce surge of 2020 accelerated American consumers' transition into digital-first shoppers. PYMNTS' research found that 87 percent of companies with an eCommerce presence experienced an increase in transaction volume over the past 12 months. Merchants with an eCommerce presence have accordingly worked to make online shopping easier for consumers, providing customer experience features like instant credits for online INR claims and other liberal return policies. While brands create these policies in the hopes of boosting consumers' confidence and building loyalty, these efforts came at a price for some retailers, as some consumers took advantage and initiated fraudulent claims.

PYMNTS' most recent survey on consumer behavior revealed the magnitude of eCommerce policy abuse. Eighty-nine percent of businesses have suffered at least one type of policy abuse in the past year. Most consumers do not abuse merchant policies by submitting fraudulent claims or attempting other schemes, yet most forms of consumer-led abuse are on the rise — businesses can lose as much as 2.2 percent of their annual revenues. PYMNTS finds that 73 percent of eCommerce companies have experienced promotion abuse over the past 12 months, making it the most common type of known customer fraud. This was followed by INR abuse (50 percent) and return abuse (44 percent).

TABLE 1:

Revenue losses to abuse over the past year
Share of revenue lost during the last 12 months, by type of abuse and firm revenue size

	All types of abuse	Promotion abuse	INR abuse	Return abuse
Total ($100M+)	2.2%	1.2%	0.6%	0.3%
More than $1B	2.4%	1.3%	0.7%	0.4%
$500M-$1B	1.9%	1.2%	0.4%	0.2%
$250M-$500M	1.6%	1.0%	0.3%	0.2%
$100M-$250M	1.9%	1.2%	0.3%	0.4%

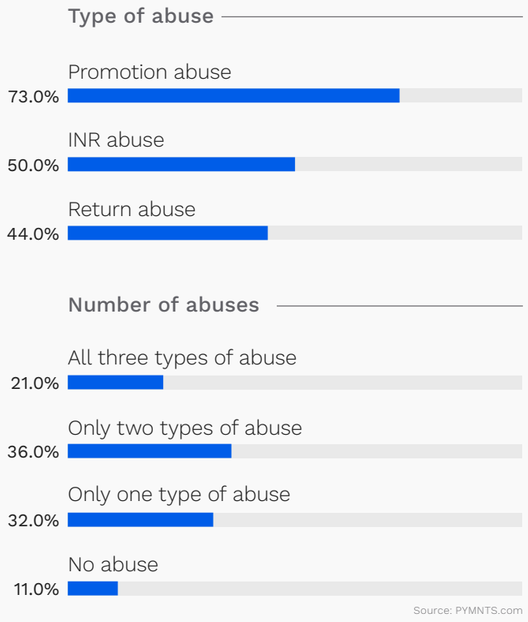
Source: PYMNTS.com

© 2021 PYMNTS.com All Rights Reserved

FIGURE 1:

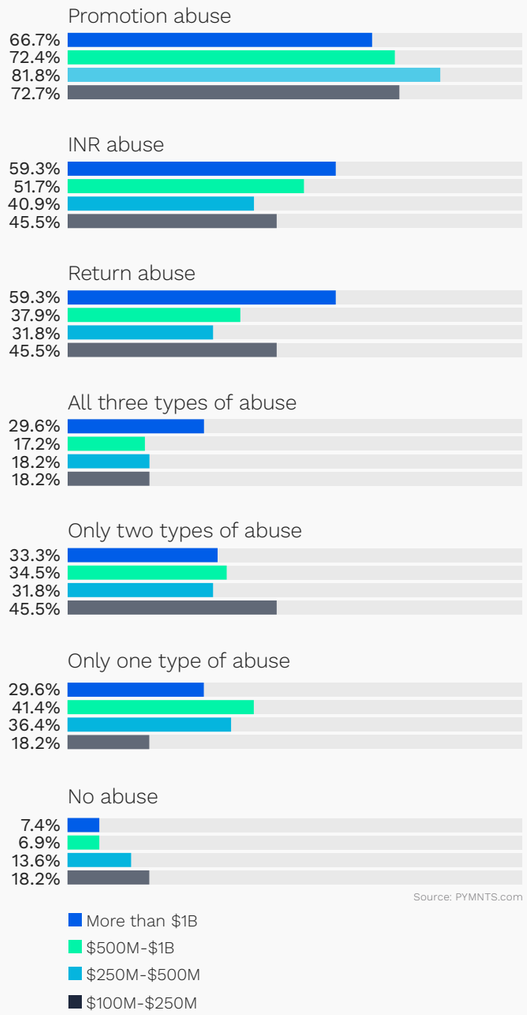
Firms that experienced policy abuse

1A: Share of firms that have observed customers commit select types of policy abuse over the past 12 months



Source: PYMNTS.com

1B: Share of firms that have observed customers commit select types of policy abuse over the past 12 months, by revenue



Source: PYMNTS.com

Our research found that the largest retailers in America were most frequently targeted and lost the highest percentages of revenue to policy abuse. Policy abuse caused retailers that earned more than $1 billion in annual revenue to lose 2.4 percent of their annual revenue. We estimated each schemes' impact on revenue losses for firms earning more than $1 billion per year

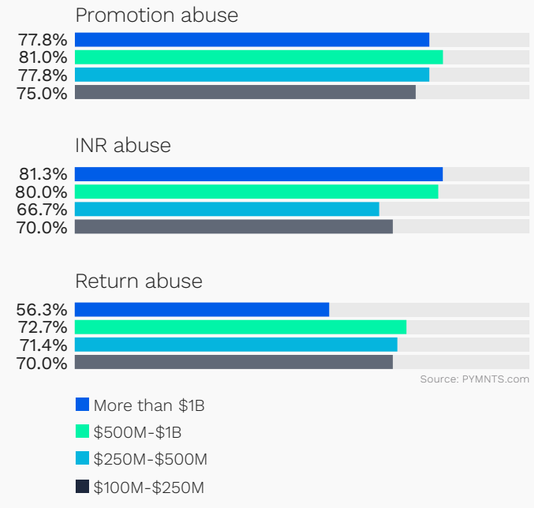
Surveyed businesses universally report that all forms of consumer abuse are rising. Seventy-eight percent of retailers that have observed promotion abuse over the past 12 months said this type of abuse increased over the same period, and this is also the case for INR abuse (76 percent) and return abuse (66 percent).

The rise in online transactions has increased the risks retailers face, yet many merchants struggle to create an effective strategy to combat these fraud types.

FIGURE 2:

Firms that experienced policy abuse

2A: Share of firms that said select types of abuse have increased over the last 12 months, by revenue



Source: PYMNTS.com

78%

Share of retailers that have observed **promotion abuse** over the past 12 months that saw it increase

© 2021 PYMNTS.com All Rights Reserved

Failure to launch: Retailers struggle to act at scale to address policy abuse

The majority of retailers are currently confronting one or more types of policy abuse, yet they face significant challenges in launching and maintaining effective operations to combat losses. PYMNTS' research reveals that 53 percent of respondents saw the inability to act at scale as the most significant barrier to enacting a comprehensive fraud-prevention policy, and this was followed by 32 percent who cited the inability to block repeat abusers as a significant challenge to their efforts to stop policy abuse.

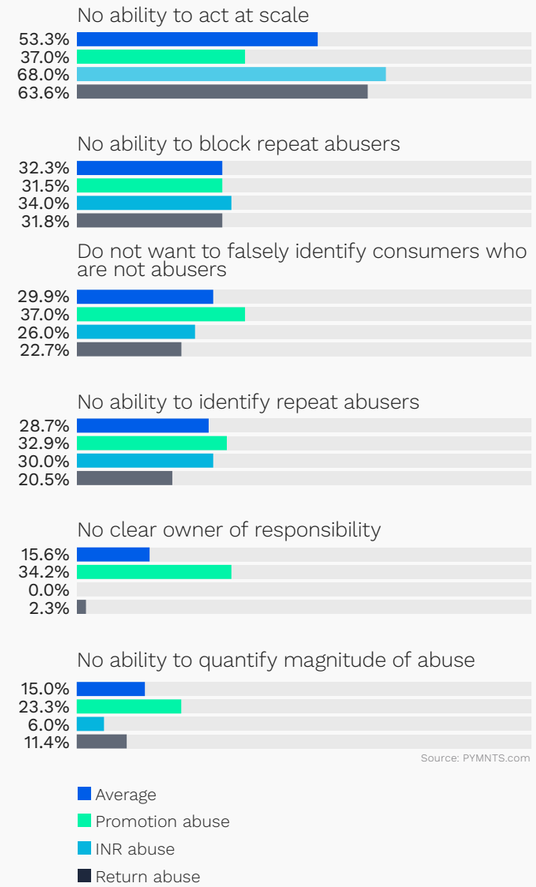
53%

Portion of survey respondents who saw the **inability to act at scale** as the most important barrier to preventing abuse

FIGURE 3:

Merchants facing significant challenges in combating policy abuse

Challenges faced by retailers in managing select types of abuse



Source: PYMNTS.com

© 2021 PYMNTS.com All Rights Reserved

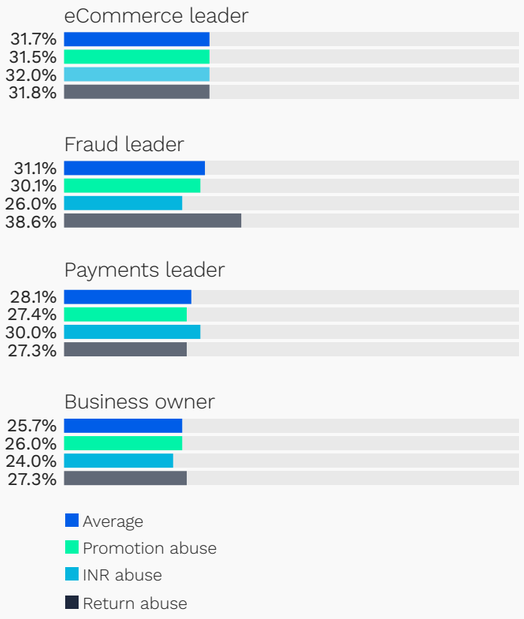
Many firms also struggle with the ownership of policy abuse in their organizations, making it harder for firms to create cohesive, organization-wide strategies. On average, only 31 percent of firms that have observed abuse over the past 12 months say that the designated leaders of their anti-fraud efforts were actually responsible for the day-to-day reduction of abuse-related loss. Similar percentages of firms delegate this responsibility to other managers, such as eCommerce leaders (32 percent), payments leaders (28 percent) and business owners (26 percent). The generally dispersed nature of responsibility for policy abuse can lead to poor management of the day-to-day challenges of assessing and addressing abuse, which can include tracking and blocking serial abusers. Firms that have witnessed promotion abuse in the past year are more likely to cite the desire to avoid false positives as a significant challenge to policy abuse prevention at 37 percent.

PYMNTS found that four out of 10 firms that have faced abuse in the past year do not automatically track the losses. Larger firms are most consistent in tracking customer abuse loss: 88 percent of large firms that have faced abuses over the past 12 months automatically track abuse-related losses. By comparison, 56 percent of small firms report using manual tracking to monitor policy abuse. Consequently, many businesses may not have full visibility to the types and magnitude of policy abuse they face.

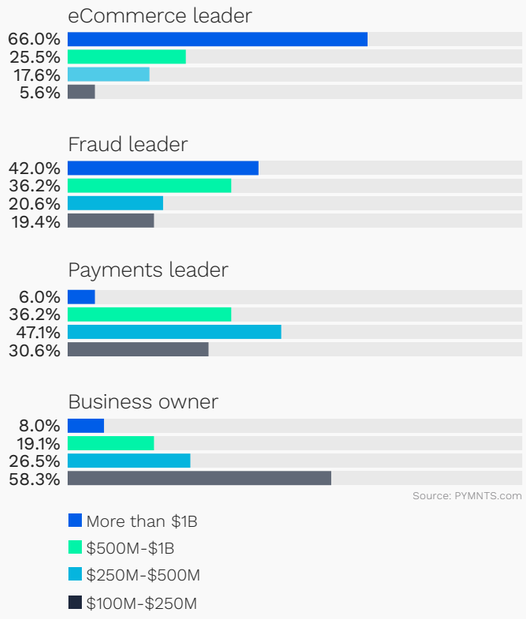
A significant percentage of retailers want to develop new methods of identifying and tracking fraud that are tailored to their organizations' needs.

FIGURE 4:
Who is responsible for fraud management?

4A: Person responsible for reducing loses related to select abuse types



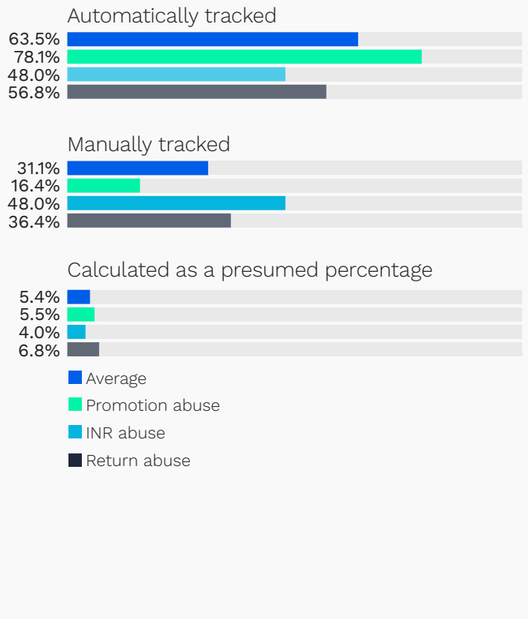
4B: Person responsible for reducing loses related to select abuse types, by revenue (average)



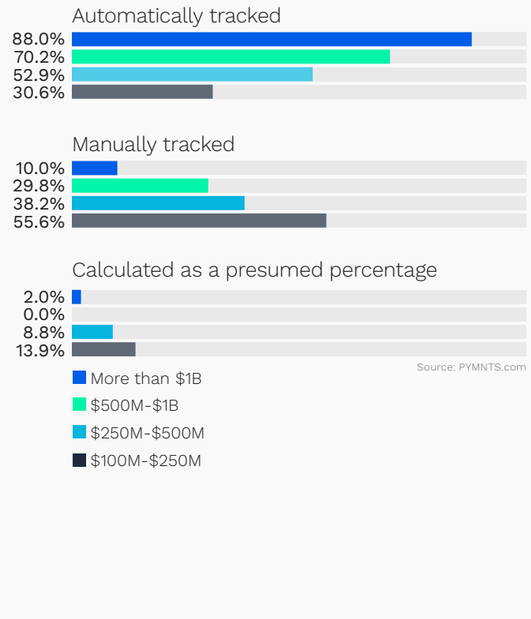
Source: PYMNTS.com

FIGURE 5:
Current methods used to track fraud

5A: Method used to track the magnitude of losses related to select abuse types



5B: Method used to track the magnitude of losses related to select abuse types, by firms' revenues



Source: PYMNTS.com

© 2021 PYMNTS.com All Rights Reserved

The build your own dilemma:

Retailers' efforts to develop anti-fraud programs often fail to identify and track fraud

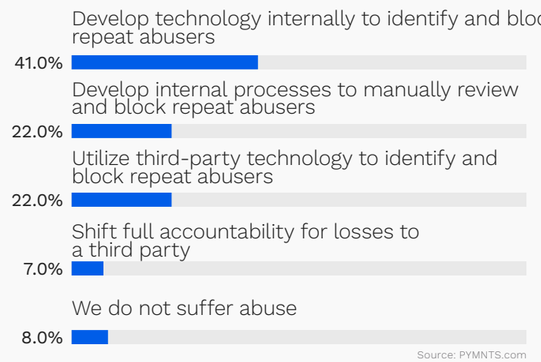
PYMNTS' research finds that developing technology internally is the most preferred strategy among retailers hoping to reduce abuse-related losses, yet few efforts manage to automatically identify and track serial abusers. A large share of survey respondents representing the largest retailers (44 percent) prefer to develop internal technology to identify and block repeat abusers, and 11 percent prefer to develop internal manual processes for the same goal. Smaller firms are more likely to prefer developing internal processes to manually review abusers (50 percent) than developing internal technology (27 percent). Retailers that experienced INR abuse are most likely to prefer to develop internal technology (52 percent) to halt abuse.

Repeat abusers cause significant losses for firms, and only a minority have successfully enacted methods to automatically identify repeat abusers.

FIGURE 6:

Retailers preferences for addressing policy abuse

6A: Share of firms that would prefer to reduce abuse-related losses in select ways

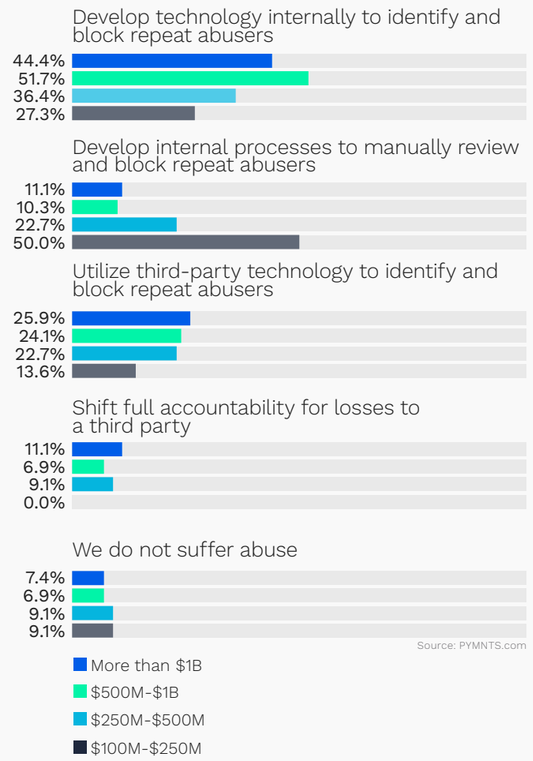


Source: PYMNTS.com

44%

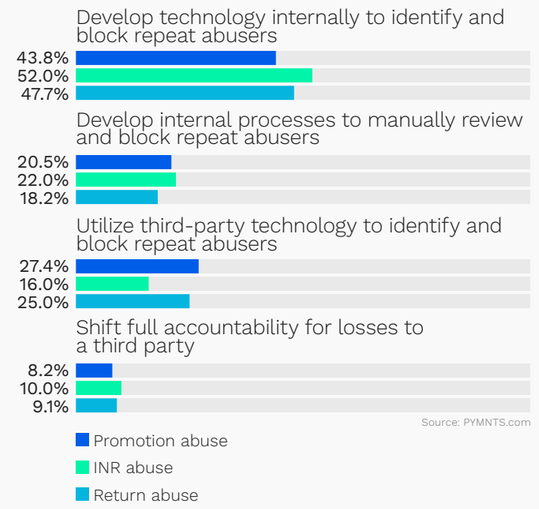
Share of large retailers that prefer to **develop internal technology** to prevent abuse

6B: Share of firms that would prefer to reduce abuse-related losses in select ways, by firms' revenues



Source: PYMNTS.com

6C: Share of firms that would prefer to reduce abuse-related losses in select ways, by type of abuse suffered in the past year



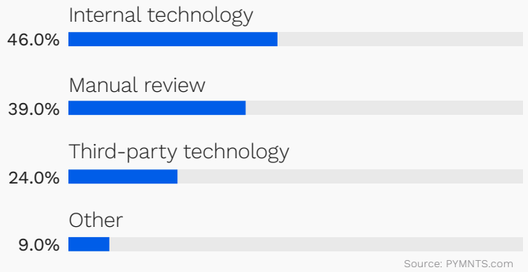
Source: PYMNTS.com

© 2021 PYMNTS.com All Rights Reserved

FIGURE 7:

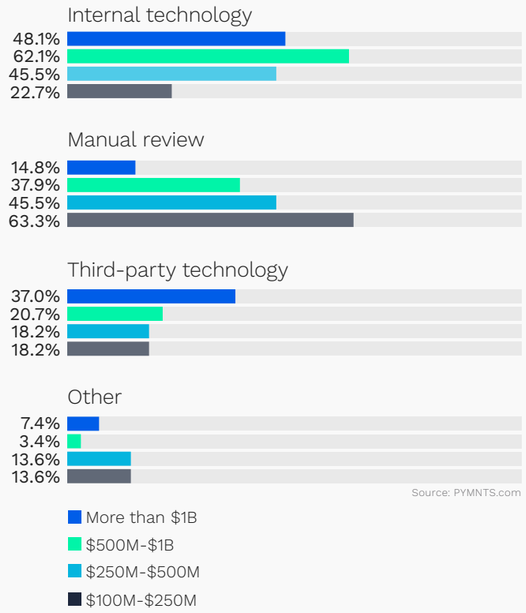
How retailers identify repeat abusers

7A: Share of firms that use the following ways to identify repeat abusers



Source: PYMNTS.com

7B: Share of firms that use the following ways to identify repeat abusers, by firms' revenues



Source: PYMNTS.com

63%

Share of retailers earning between $100 million and $250 million that **track losses from abuse manually**

Finding the right third-party solution

Many retailers may intend to engineer their own anti-fraud technologies in-house, often with hit-or-miss results. Only a minority of firms earning between $100 million and $500 million annually automatically identify and track serial policy abusers. Firms seeking to uncover patterns of policy abuse and block repeat abusers might consider working with a third party. Here are three features to look for when partnering with an anti-fraud solutions company:

Real-time decision-making to block serial abusers instantly
Advanced technologies stop serial abusers. Look for a solutions provider that can pinpoint the online identities that have proven to repeatedly abuse policies either in your network or across a wider network of businesses.

Look for customization options that fit your business
Regardless of how policy abuse impacts your company's revenue, your anti-fraud solution should scale as your company does. Choose a third-party partner that can tune models to match your requirements and deliver desired outcomes as your audience and sales volume changes.

Adjust policies to match the persona
Sophisticated solutions know the identity behind an interaction and can adjust policies accordingly. For example, a buyer who has claimed INR in the past may be required to sign for delivery, or a repeat returner may be offered purchases as final sale.

Conclusion

Known customer abuse is a growing concern, but it has a clear solution. Businesses that approach this challenge will find success when they focus on identifying and tracking serial abusers and designating a team to own the solution. It is critical to first gain visibility to the types and magnitude of abuse you face and then take targeted action. Policy abuse will keep evolving as eCommerce continues to grow, so forward-thinking firms must modernize their approaches to avoid losing more revenue to these avoidable attacks.

Methodology

Beyond eCommerce Fraud: How Retailers Can Prevent Customer Policy Abuse, a PYMNTS and Forter collaboration, is based on a survey conducted between Aug. 25 and Sept. 14 of 100 executives representing businesses in the retail sector that generate at least $100 million in annual revenue who possess intimate knowledge of — and leadership responsibilities in — customer service, the customer experience and fraud prevention.

© 2021 PYMNTS.com All Rights Reserved

About

PYMNTS.com is where the best minds and the best content meet on the web to learn about "What's Next" in payments and commerce. Our interactive platform is reinventing the way in which companies in payments share relevant information about the initiatives that shape the future of this dynamic sector and make news. Our data and analytics team includes economists, data scientists and industry analysts who work with companies to measure and quantify the innovation that is at the cutting edge of this new world.

Forter is the leader in eCommerce fraud prevention, processing over $250 billion in online commerce transactions and protecting more than a billion consumers globally from credit card fraud, account takeover, identity theft and more. The company's identity-based fraud prevention solution detects fraudulent activity in real time, throughout all online consumer experiences.

Forter's integrated fraud prevention platform is powered by its rapidly growing global network, underpinned by predictive fraud research and modeling, and the ability for customers to tailor the platform for their specific needs. As a result, Forter is trusted as the sole or primary risk mitigation engine by Fortune 500 companies, including Farfetch, Sephora, Nordstrom, Instacart, Adobe and Priceline, to deliver exceptional accuracy, a smoother user experience and elevated sales at a much lower cost.

Forter has raised more than $500 million in capital from top-tier venture capitalists including Sequoia, Bessemer Venture Partners, NewView Capital, Tiger Global Management, Scale Venture Partners, March Capital and Salesforce Ventures.

We are interested in your feedback on this report. If you have questions, comments or would like to subscribe, please email us at feedback@pymnts.com.

DISCLAIMER

Beyond eCommerce Fraud: How Retailers Can Prevent Customer Policy Abuse may be updated periodically. While reasonable efforts are made to keep the content accurate and up to date, PYMNTS.COM: MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, REGARDING THE CORRECTNESS, ACCURACY, COMPLETENESS, ADEQUACY, OR RELIABILITY OF OR THE USE OF OR RESULTS THAT MAY BE GENERATED FROM THE USE OF THE INFORMATION OR THAT THE CONTENT WILL SATISFY YOUR REQUIREMENTS OR EXPECTATIONS. THE CONTENT IS PROVIDED "AS IS" AND ON AN "AS AVAILABLE" BASIS. YOU EXPRESSLY AGREE THAT YOUR USE OF THE CONTENT IS AT YOUR SOLE RISK. PYMNTS.COM SHALL HAVE NO LIABILITY FOR ANY INTERRUPTIONS IN THE CONTENT THAT IS PROVIDED AND DISCLAIMS ALL WARRANTIES WITH REGARD TO THE CONTENT, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT AND TITLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES, AND, IN SUCH CASES, THE STATED EXCLUSIONS DO NOT APPLY. PYMNTS.COM RESERVES THE RIGHT AND SHOULD NOT BE LIABLE SHOULD IT EXERCISE ITS RIGHT TO MODIFY, INTERRUPT, OR DISCONTINUE THE AVAILABILITY OF THE CONTENT OR ANY COMPONENT OF IT WITH OR WITHOUT NOTICE.

PYMNTS.COM SHALL NOT BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND, IN PARTICULAR, SHALL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE, OR LOSS OF USE, ARISING OUT OF OR RELATED TO THE CONTENT, WHETHER SUCH DAMAGES ARISE IN CONTRACT, NEGLIGENCE, TORT, UNDER STATUTE, IN EQUITY, AT LAW, OR OTHERWISE, EVEN IF PYMNTS.COM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME JURISDICTIONS DO NOT ALLOW FOR THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, AND IN SUCH CASES SOME OF THE ABOVE LIMITATIONS DO NOT APPLY. THE ABOVE DISCLAIMERS AND LIMITATIONS ARE PROVIDED BY PYMNTS.COM AND ITS PARENTS, AFFILIATED AND RELATED COMPANIES, CONTRACTORS, AND SPONSORS, AND EACH OF ITS RESPECTIVE DIRECTORS, OFFICERS, MEMBERS, EMPLOYEES, AGENTS, CONTENT COMPONENT PROVIDERS, LICENSORS, AND ADVISERS.

Components of the content original to and the compilation produced by PYMNTS.COM is the property of PYMNTS.COM and cannot be reproduced without its prior written permission.