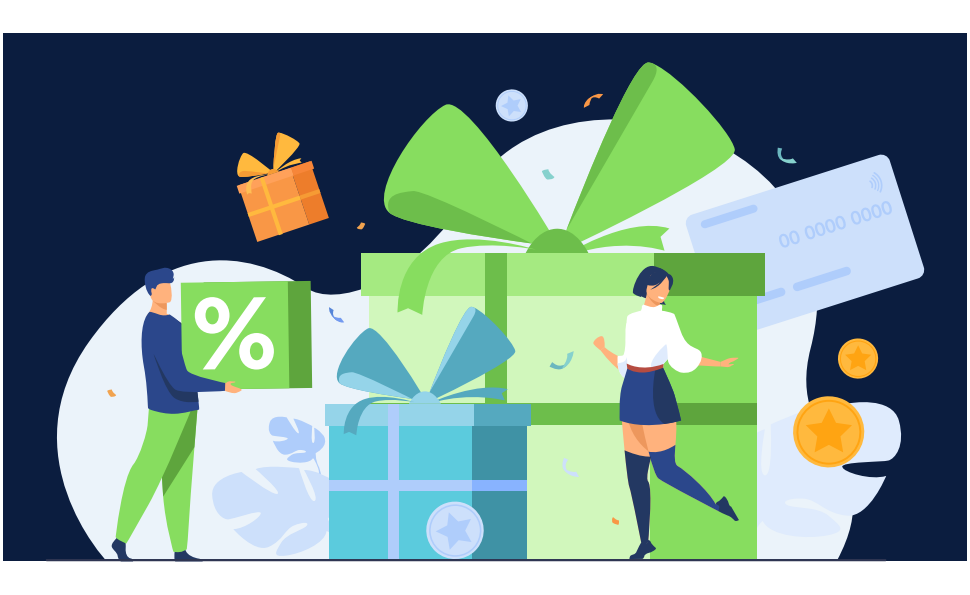
DATAVISOR

The Dummy Handbook on PROMOTION AND POLICY ABUSE PREVENTION

Policy abuse, promotion abuse, first-party fraud (aka friendly fraud) and related issues affect merchants and financial institutions alike. This handbook provides condensed information about what these activities are, providing clear examples of the most common forms of policy abuse faced by modern businesses. It also discusses the need to take them seriously and gives five actionable steps businesses can take to stop policy abuse on its tracks. Additionally, it explains why traditional fraud strategies have a hard time detecting these forms of fraud and offers a viable solution.

FIRST THINGS FIRST. WHAT'S THE COMMON THREAD?

While not identical in meaning, policy abuse, promo abuse, first-party fraud, friendly fraud, and similar issues share an identity in the fact that they are illicit acts perpetrated by individuals or coordinated attackers that don't necessarily hide or misrepresent their identities. In these forms of fraud, which we will refer to as policy abuse for simplicity, customers who are who they say they are behave in illicit ways to exploit companies' policies to their advantage.



The implications of this definition are noteworthy. First, because traditional fraud-prevention measures and tools are not great at detecting policy abuse because they are designed to look for instances where identities, credentials, and payment methods are compromised, as is not the case with these issues. Second, because organizations are responsible for designing the policies that they offer their customers and must do so taking into account the possibility of abuse.

It is also worth keeping in mind that policy abuse vulnerabilities can also be exploited by organized criminals. In this sense, the line between policy abuse and third-party fraud can be quite thin. Fraudsters could exploit policy abuse vulnerabilities such as lax sign-up bonuses using bots and batches of false identities, leading to exponential losses for well-intentioned financial institutions and retailers.

While most policies could potentially be exploited by fraudsters, some types of them tend to be particularly prone to abuse. Some of them are:

Promotion abuse

In recent years, industry and venture capital expectations for growth in transactionality and user acquisition metrics have increased dramatically. To meet these expectations, companies everywhere have implemented aggressive growth strategies that rely heavily on promotions.

In essence, promotions are economic incentives designed to stimulate business, but such incentives can have the unintended effect of opening windows for abuse by less-scrupulous users. This abuse could come in the form of misused discount codes, multiple account openings to obtain signup bonuses, and the use of multiple free trial periods by single users.

With so much at stake here, preventing promotion abuse is really a matter of setting up companies for long-term sustainability and success.

Did you know? In 2014, Uber offered a $20 referral bonus for each new customer referred. A fraudster created a referral code, shared it on Reddit, and accumulated $50,000 in free ride credits. Where should companies draw the line?

Bonus: Read this case study about a leading fintech in the cryptocurrency space that used machine learning to stop 92% of fraudulent account openings before the disbursement of promotions.

Return fraud

Modern online shoppers expect a lot from who they do business with, especially in connection with return policies. Sellers need to allow good customers to return the goods they are dissatisfied with, and many of them even adopt "no questions asked" policies to promote shopping on their sites. But bad customers can exploit these policies by performing excessive returns (buying several items and keeping only one or none) or by returning items after they have used them (aka wardrobing fraud). This can drastically increase costs for retailers.

Did you know? In a survey, 57% of retailers said that dealing with returns has a negative impact on the day-to-day running of their business, and 30% of shoppers admitted to deliberately over-purchasing and subsequently returning unwanted items.[1]

False item-not-received claims.

Disingenuous buyers can exploit policies designed to retain good users by falsely claiming that goods that they ordered were not delivered. Since most retailers do not handle deliveries themselves and instead work with third-party logistics providers, it is hard for them to know for sure whether or not customers are telling the truth. In some cases, they seek to prioritize the customer experience by providing instant refunds upon receiving these claims.

Fraudulent chargebacks.

Unscrupulous cardholders acquire goods and services using their credit cards and, after receiving them, raise chargebacks with their issuers. The issuers, seeking to retain their customers, often side with them and merchants are left to foot the bill for the goods and services. Fraudulent chargebacks cause problems for all parties involved since the costs for processing these disputes are quite high.

Source: https://www.salecycle.com/blog/featured/ecommerce-returns-2018-stats-trends/

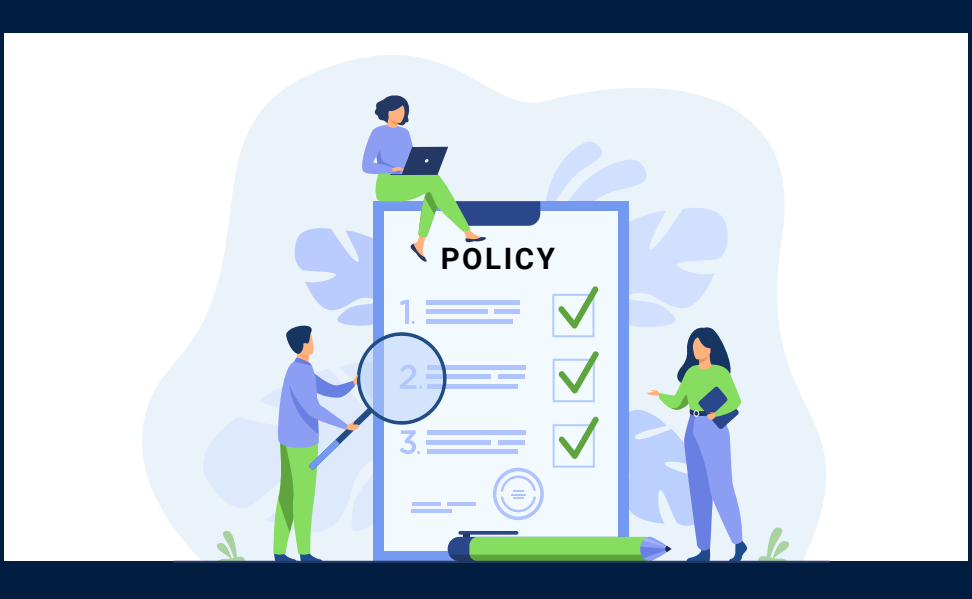
WHY IS POLICY ABUSE RELEVANT (AND BECOMING MORE SO EACH DAY)?

According to PYMNTS, retail customers perpetrating policy abuse cost U.S. firms with more than $100 million in annual sales and a collective $89 billion in revenue each year. The situation is quite similar for financial institutions seeing their referral programs and signup bonus promotions gamed by fraudsters.

And all signs point towards policy abuse as a growing threat for retailers and financial institutions. The massive mindshift towards customer-centricity initiated by companies like Amazon and PayPal has now become the norm. Fintechs, banks, retailers, and practically every company offers favorable policies in an effort to remain competitive and meet ever-so-stringent customer expectations.

According to a survey, 70% of U.S. consumers will actively seek promotions and coupons when holiday shopping, and 45% said that discounts will be one of the most important factors in deciding where to shop. Consumer sentiment for promotions is similar globally. For example, another PYMNTS study found that 44% of U.K. shoppers say they spend more at grocery stores with loyalty programs.

Considering the potential loss of market share for businesses who do not offer promotions and favorable customer-facing policies, simply discontinuing these offers in response to fraud attempts is not a viable option. The trick is to weave in fraud prevention strategies that ensure that companies minimize the risk of fraud while maximizing the customer experience for honest people.



FIVE STEPS TO STOP POLICY ABUSE ON ITS TRACKS

Policy Abuse Is a Form of Fraud, Treat It as Such

Some firms still treat policy abuse as a cost of business, a customer support issue, or another type of matter other than fraud. The lack of clarity regarding the ownership of policy abuse within organizations increases the difficulty of creating cohesive, company-wide strategies designed to ensure that policies are effective in their goals and do not lend themselves to abuse by deceitful agents.

According to Pymnts, only 31% of companies that face policy abuse issues have assigned their fraud teams with the responsibility of mitigating the ensuing losses. About 30% of firms, meanwhile, assign this responsibility to eCommerce managers, 28% to payments leaders, and 26% to business executives. This is problematic because at the vast majority of organizations, only dedicated fraud specialists have the field knowledge and access to the tools and resources required to mitigate fraud, including policy abuse cases.

In sum, organizations that recognize policy abuse as a form of fraud increase their chances of success by clarifying the nature of the issue and assigning ownership of its resolution to the people with the right expertise and tools to handle it.

Zoom Out!

Transaction-level fraud detection, by itself, is incapable of detecting most forms of policy abuse, especially those that consist of deceitful behavior perpetrated by the same customers over and over. For example, transaction-level analysis would be ineffective at mitigating the damage caused by the customer of a financial company abusing sign-up bonuses by opening hundreds of accounts using different email addresses. When seen in isolation, each of these account openings could seem valid, but when analyzed in bulk, it would be evident that a problem exists.

Unlike traditional fraud detection systems, DataVisor's unsupervised machine learning model allows its clients to see the big picture and analyze entire datasets to detect fraud patterns that are invisible to the naked eye. The secret lies in uncovering connections among seemingly unrelated events. In the example above, a serial account-opening scheme could be stopped by linking several accounts to a common element, such as an IP address, an email domain, a zip code, or even a pattern of in-app or in-site behavior.

Have any questions about how we can help your team do this? Schedule a free consultation session with an expert now.

Fool Me Once, Shame on You. Fool Me Twice…

If you detect that a certain group of people has a tendency to make use of friendly policies in a manner that deviates from a reasonable standard, you can act preemptively to prevent this from becoming outright abuse.

For example, if a set of customers is flagged as raising chargebacks or performing returns on more than 5% of the items they purchase, a new rule requiring that such customers' returns or chargebacks are reviewed in more detail could be warranted. Or if a customer requests a refund under the argument that they did not receive an item your company did ship, you could perform the refund once and request that all future deliveries made to that customer, address, or building request a signature or be evidenced with a digital photograph.

Know Your Customers, But Really

One of the most important steps any digital organization can take in the fight against all forms of fraud is investing in true means of customer identification. The high degree of pseudonymity allowed by internet services nowadays allows individuals to change their identifying traits with relative ease and open new accounts using different email addresses and domains, IP addresses, devices, phone numbers, and a long etcetera.

Organizations that are able to look through this clutter and identify users with certainty dramatically increase their odds at detecting deceitful patterns of behavior, including those pointing at policy abuse scenarios.

DataVisor works with the most forward-looking companies in the digital world with solutions like its dEdge, which uses advanced machine learning algorithms and takes a holistic approach to analyzing abnormal signals and extensive device information to deliver a unique device ID for each phone, computer, tablet, and more, no matter how fraudsters might uninstall apps, reset devices, or change device parameters.

Wanna see this in action? Schedule a demo now!

Look at the Big Picture

Use company-wide performance data to evaluate your organization's policies and decide whether or not course corrections are called for. Once you have the tools and strategies to identify policy abuse, keep track of the incidence of each type of abuse, the performance of the respective policy, and that of the organization as a whole. Then, take a step back and analyze the big picture.

Is your return policy too lax? Are you spending too much effort reigning in abuse when compared to the benefits yielded by a promotion campaign? Do you need to hire new team members to ensure policies are successfully implemented and enforced? Answering these types of questions can lead to great benefits.

WHY ARE TRADITIONAL FRAUD DETECTION SYSTEMS INEFFECTIVE AGAINST POLICY ABUSE?

If you are using a legacy fraud detection platform to try to mitigate policy abuse, you may be experiencing the frustration of seeing costs soar for your company. The main reason for this is that abusive customers are real customers who have successfully completed on-boarding identification steps and in all likelihood have a transaction history with your company.

Traditional fraud prevention efforts, including two-factor authentication, identity validation measures, and biometrics recognition solutions are designed to prevent unauthorized individuals from passing as legitimate users to commit fraud. However, these measures are rendered null by legitimate users committing policy abuse in their own names and accounts.

Like we mentioned above, sometimes policies can be abused by criminal groups in more complicated fraud attack schemes. The use of bots to perform these large-scale attacks also poses additional challenges for teams without cutting-edge fraud detection tools that do not have the capabilities required to identify complex bot-scripted attacks.

Advanced fraud solutions like DataVisor's proactive detection suite offer additional layers of protection by continuously monitoring user activity at various levels and allowing fraud teams to act before it is too late. DataVisor allows companies to retain their most loyal clients and attract new ones without wasting marketing dollars on multi-accounting, fraudulent massive registrations, and user collusion. This is accomplished by building a resilient fraud architecture through detailed data analysis, a time-tested rules platform, bespoke SML and UML models, and intuitive visualization and decision tools.

Schedule a free 30-minute consultation to learn how DataVisor is different and experience proactive AI-powered fraud prevention today.

CONCLUSION

All in all, when companies implement favorable policies, be them friendly return rules, enticing promotions, or any other, they do so as an investment. They devote valuable resources and team efforts to attract and retain customers in the hope of achieving sustainable growth. Adopting a proactive and effective policy abuse prevention strategy and giving fraud teams the right tools to handle the problem is really about ensuring that these efforts don't go to waste. Good work and good money should benefit companies and their honest consumers, not criminals or abusive users.

Are you still curious? Do you want to know how machine learning can help your business fight fraud?

About DataVisor

DataVisor is the world's leading AI-powered Fraud and Risk Platform that delivers the best overall detection coverage in industry. With an open SaaS platform that supports easy consolidation and enrichment of any data, DataVisor's solution scales infinitely, enabling organizations to act on fast-evolving fraud and money laundering activities as they happen in real time. Its patented unsupervised machine learning technology, combined with its advanced device intelligence, powerful decision engine and investigation tools, provides guaranteed performance lift from day one.

For more information on DataVisor:

info@datavisor.com

www.datavisor.com

967 N. Shoreline Blvd. | Mountain View | CA 94043

DATAVISOR