ACI UNIVERSAL PAYMENTS℠

PANDEMIC-DRIVEN PATTERNS OF eCOMMERCE FRAUD

INTRODUCTION

COVID-19 has drastically impacted the way consumers shop and the way businesses function. At the start of the pandemic, many businesses were forced to shut their brick-and-mortar operations and focus primarily on their eCommerce sales channels. This, in turn, led many consumers to shift their shopping to the online realm. From January to June 2020, ACI reported a 15% increase in volume of eCommerce purchases. May 2020 saw online retail transaction growth of 81% compared to May 2019.

But, with such a large spike in eCommerce traffic comes an associated change in fraud patterns. ACI recently reported that the average transaction value of attempted fraud has increased by 4.7%, while fraud volume decreased by 3.2% in the period of January to June 2020. It might seem a relief to merchants that the fraud rate by volume is down, but the increased value of attempted fraud means there is no room to relax fraud strategies.

Also, the main reason for the percentage decrease in fraud volume is the overwhelming increase in the overall volume of genuine transactions. This can be a misleading representation of fraud activity. Fraudsters often use peak trading periods as an opportunity to boost their activities because the increase in eCommerce traffic creates an ideal environment to hide or disguise their attacks among genuine transactions.

The risk of causing unnecessary friction for genuine customers also increases as overall volumes increase, so it is even more vital to be able to separate good transactions from bad to avoid losses on multiple fronts.

Fraud or risk teams must be able to adjust their approaches to combatting fraud at times of rapid change. Working with fraud strategy experts can help ensure that businesses are prepared for shifts in fraud patterns and can mitigate increased chargeback activity.

SPOTTING THE SIGNS

Fraudsters are borderless and agnostic to sector, payment method and channel. They will look for the weakest link and the easiest way to use data to exploit merchant websites and gain goods and services fraudulently. The focus for merchants is to spot this behavior and block it, without detriment to genuine customers.

It is important, for example, to monitor the types of products being purchased, since fraudsters usually target popular, more expensive items with high resale value (e.g., electronics, beauty products, luxury brand clothing/accessories). This means one of the layers of a merchant's risk strategy should be directed at higher risk items. At the same time, though, these same items are in demand with genuine customers — high value doesn't simply mean high risk — adding pressure on merchants to separate fraudulent and genuine transactions.

Many merchants still rely heavily on manual review processes — and, for those who do, prioritizing the review of suspicious high-value (and other high-risk) orders is vital. Using prioritization processes allows fraud agents to quickly put a stop to fraudulent orders and make sure genuine orders get passed through. The review process can also help the fraud team to better understand fraudster behavior and identify anomalies within the transaction data. This, in turn, can support more effective, in-depth risk strategies.

Fraudsters work around the clock to try and perpetrate fraud by testing fraud strategies and identifying any weaknesses in a fraud detection solution. They adapt quickly and attempt to learn the thresholds that are in place so they can change their approach to ensure their orders are successful. Yet, a fraudster's activity slightly deviates from genuine customer behavior. **Working with experienced fraud experts to analyze and track changing behavioral characteristics associated with fraud will help to ensure that risk strategies also adapt to keep pace with the fraudster.**

SPREADING THE NET

Fraud experts have numerous features and tools at their disposal to create a complex and multi-layered fraud strategy that will increase the accuracy of fraud detection. Positive lists (marking trusted, genuine customers) and negative lists (for fraudulent activity) are a valuable tool for helping to keep the balance between customer experience and fraud prevention — especially when volumes are high and merchants don't have time to review huge numbers of transactions.

Velocity rules are also an important part of the screening process since they focus on limiting the quantity of items being purchased, or the number of orders one customer can place in a certain time frame. These rules are basic but very effective at stopping high-volume fraud attempts that use the same customer information.

That said, it is common for fraudsters to continually adjust their account details to appear as a different customer. In this case, velocity rules will be ineffective. An additional layer of rules will be needed to take into consideration the broader data points on a customer's account details (e.g., email address/phone number/card number/address). For instance, fraud rules can trigger an alert or red flag if a variety of different card numbers are used with one email address in a short period of time. This can signal a common characteristic of fraud — where fraudsters test cards to see which one successfully passes card authorization.

It is also important to create rules that look at multiple different characteristics within a transaction to reduce the risk of blocking genuine customers. This isn't just down to rules — **neural models and machine learning are critical in reducing the false positive rate to keep conversion rates high and fraud levels low**. These technologies continually learn from fraud trends and can help inform adaptive fraud strategies to enhance the fraud detection rate and minimize false positives.

THE RISE OF RESELLERS

Another growing challenge for merchants during the COVID-19 pandemic has been reseller activity. Resellers are generally classified as individuals or companies that buy large quantities of items for the purpose of selling onwards. Many resellers are genuine of course, and it is important for merchants to think carefully about whether they wish to conduct business with resellers or place additional restrictions on their activity.

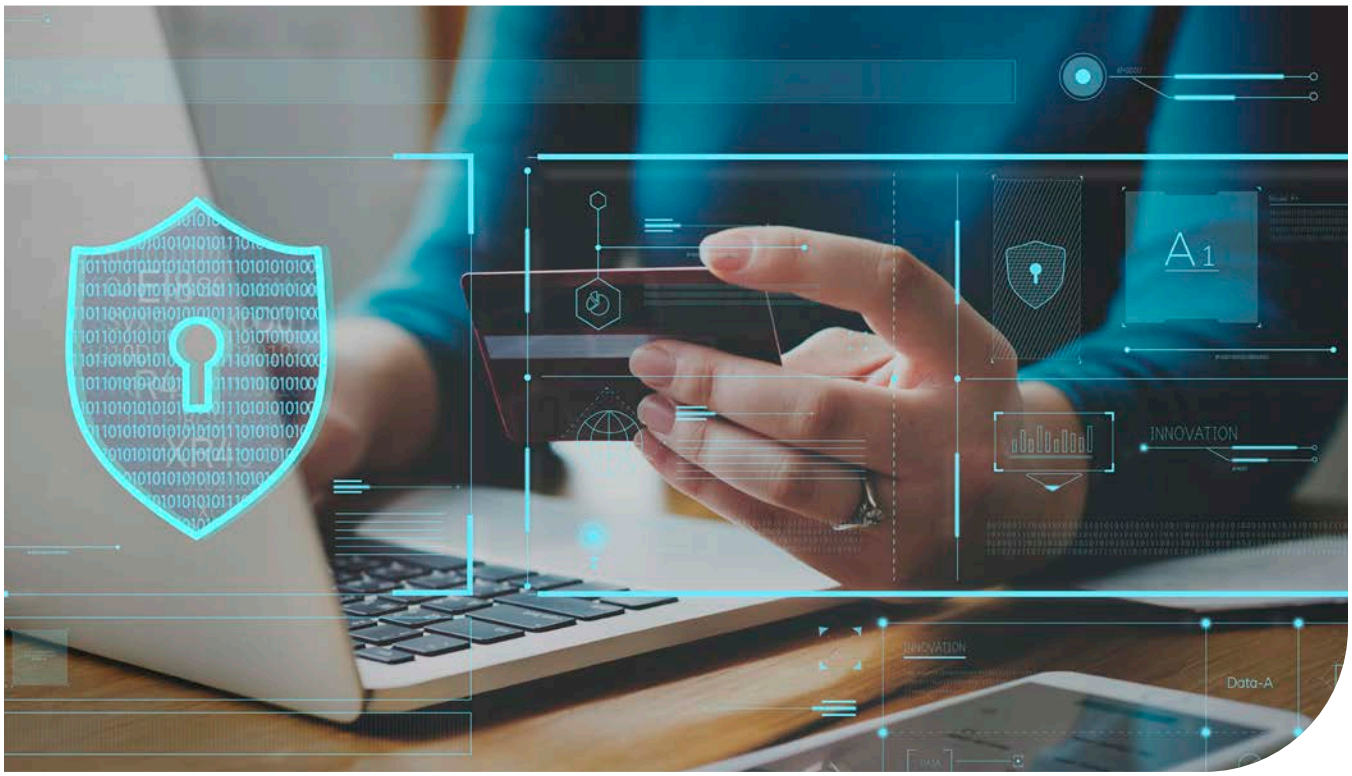
Most merchants will have velocity rules in place to flag and/or block high-volume orders. Fraudulent resellers will try to circumvent these rules by changing the data elements in their purchases, such as email addresses/phone numbers/card numbers/address location, to appear as a different customer.

If a reseller is compromised or unauthorized, this can have a large and negative impact on a merchant, sharply increasing chargeback rates. If this problem does occur, quick and appropriate adjustments to the fraud strategy will be needed to detect and stop orders coming from the fraudulent reseller.

There are several ways to identify reseller activity, including:

- Large amounts of one or several related products being purchased in a short period of time
- New email/phone number/card number being used
- Address manipulation patterns — for example, the reseller is trying to use the same address for each order, but alters it slightly (123 Main Street, 123 Main Streets, 123 Main streets)
- High increase in orders being sent to a specific area in a short period of time

Merchants can also create a positive list for genuine resellers to ensure their transactions are completed smoothly.



THE FRIENDLY FRAUD UPRISING

An additional obstacle faced by eCommerce merchants during the COVID pandemic has been a large increase in friendly fraud chargebacks.

Comparing April 2020 to April 2019, ACI has reported an increase of 27% by volume in chargebacks. This can be due to multiple factors, including unavoidable delays or failure to fulfill orders due to operational restrictions. Aside from the increase in genuine chargebacks, though, there is still a notable increase in friendly fraud. Some of this is directly due to the financial impact that COVID-19 has had on consumers. The U.S. unemployment rate rose from 3.8% in February to 13.0% in May 2020*, causing financial strains on many families. An unfortunate side effect of the increase in unemployment is the "quick" way some consumers have attempted to recover income, filing chargebacks on items they previously purchased online. Customers will commonly claim one of the following when perpetrating this type of chargeback:

- Did not receive item
- Transaction was not authorized by the cardholder
- Item received was not as described

Businesses need to decide if they want to block this type of customer. Generally, if there is only one offense, there is little risk in keeping relationships with the customer and allowing future transactions. However, repeat offenses may warrant blocks for certain customers to prevent future purchases.

As eCommerce sales continue to rise, fraud professionals and businesses must stay vigilant to ensure fraud and chargeback rates are held down, and genuine customers are not adversely affected. A layered fraud strategy is essential to stop fraudsters as they change their approaches and methods of attack. Fraud experts can use a variety of tools and techniques to detect and prevent fraud, including velocity thresholds, the analysis of multiple data points, updating positive/negative lists and incorporating machine learning capabilities into their fraud strategy. **As the pandemic continues, flexibility and a fast response to changing patterns of genuine and fraudulent behavior are more important than ever**.

* Unemployment rose higher in three months of COVID-19 than it did in two years of the Great Recession, Pew Research, June 2020

ACI UNIVERSAL PAYMENTS

ACI Worldwide powers digital payments for more than 6,000 organizations around the world. More than 1,000 of the largest financial institutions and intermediaries, as well as thousands of global merchants, rely on ACI to execute $14 trillion each day in payments and securities. In addition, myriad organizations utilize our electronic bill presentment and payment services. Through our comprehensive suite of software solutions delivered on customers' premises, through the public cloud or through ACI's private cloud, we provide real-time, immediate payments capabilities and enable the industry's most complete omni-channel payments experience.

LEARN MORE

WWW.ACIWORLDWIDE.COM

@ACI_WORLDWIDE

CONTACT@ACIWORLDWIDE.COM

Americas +1 402 390 7600
Asia Pacific +65 6334 4843
Europe, Middle East, Africa +44 (0) 1923 816393

ATL7422 10-20

Authored by:
Steven Ng
Risk Analyst, ACI Worldwide