The Virus Drives Us Virtual

What recent rapid transaction growth means for fraud prevention in gaming

April 2021

ACI Worldwide
Real-Time Payments

Introduction

2020 started out much like any other year, with new resolutions, travel plans and an overall enthusiasm for the year to come. Unfortunately, as the year progressed, we became all too familiar with a seemingly invisible enemy known as COVID-19 that would drastically re-shape the year and impact businesses, our communities and our lives. The virus forced countries and businesses alike to set travel restrictions and issue stay-at-home orders. Schools had to shift to virtual sessions; businesses deemed "non-essential" had to close their doors indefinitely. With millions of people now abiding by the stay-at-home orders, individuals looked for a safe outlet to distract themselves, stay social, quell their boredom and ease their minds. For many, video games proved the perfect solution.

This shift to a more virtual way of life via video games resulted in a massive increase in transaction volumes and revenue for merchants in the gaming sector:

- ACI saw increases in gaming transaction volumes of 109% in August, 52% in July, 70% in June, 84% in May, 126% in April and 97% in March, compared to the respective months in 2019[1]
- Sony's PlayStation platform experienced a digital software sales increase of 83% year on year as of August 2020[2]
- Microsoft's Xbox platform saw revenue increase 65% in Q3 of 2020[3]
- Steam, a popular PC video gaming platform, reported its highest ever concurrent player count at over 20.3 million players in March 2020[4]

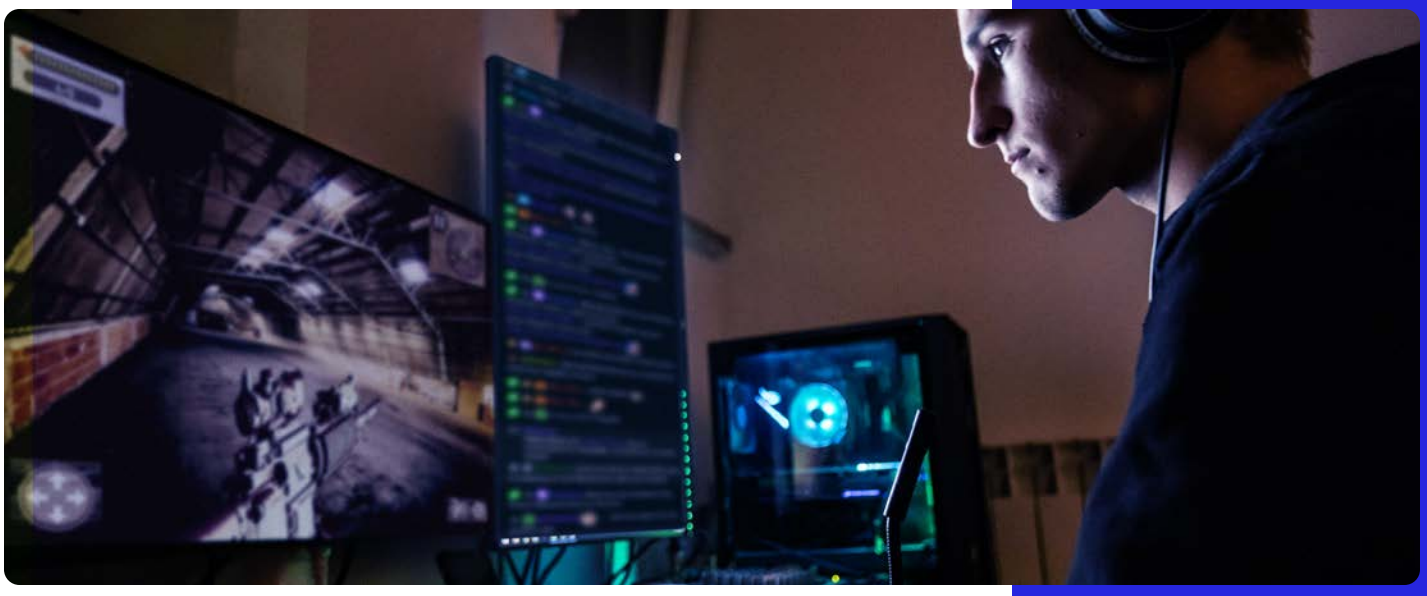
Great Sales Demand a Great Fraud Strategy

With a sudden surge in transaction volumes, fraud experts must react quickly to adjust eCommerce fraud and risk strategies. Millions of new customers purchasing gaming consoles equate to millions of new accounts. ACI data indicates that gaming merchants continue to experience **1 to 1.5 million more new accounts transacting per month**, compared to the same period last year. These new accounts will be transacting for high-demand goods, with low time on file and minimal (if any) purchasing history. These are characteristics typically associated with a higher likelihood of fraud, but this shift in customer behavior means that **risk strategies need to be adjusted to exercise more leniency**. A seamless experience for new users may help transition them into long-time and loyal customers, so it is imperative to keep acceptance rates high and customer insults low. Making the proper strategy adjustments allows for more uninterrupted revenue, helps relieve costs and alleviates call center teams from increased call volumes and customer inquiries.

The massive sales numbers that the gaming — and wider digital downloads — industry is experiencing is supported by easy acquisition of digital products. Gaming products are either downloaded directly to the gaming console or PC, or consumers are provided a software key. These alternative forms of purchasing have gained more popularity during the COVID-19 pandemic because they give consumers the ability to purchase goods while avoiding physical contact with others. Instant downloads also avoid shipping delays.

Digital goods provide immediacy and convenience for the consumer — but, adversely, present a strategic challenge for merchants. In the case of direct digital downloads, there is no time for a merchant to review and validate a transaction before the product is delivered to the consumer. This requires a pass-fail fraud strategy and an approach adjusted to coincide with the shift in buyer behavior and the increase in new customers. It is important to block only those transactions that have an extreme likelihood of being malicious. Recouping or restricting purchases being made by a good customer can increase customer friction and prevent that customer from returning. It also increases escalations for customer support teams.

To determine if a merchant is going to deny a transaction, a strong risk strategy is essential, incorporating substantial historical and statistical evidence supporting that decision. Through access to a rich consortium database, merchants can determine if customers have a positive transaction history in the overall ecosystem. According to ACI's internal benchmarking, **40% of accounts with a new time-on-file value of 50 days or less for a specific merchant also contained over 200 days of history within the wider consortium database**. This meant they could be deemed non-fraudulent with low chargeback risk. Using a client-specific time value for customers in combination with a global database can equate to hundreds of millions in cost savings and additional revenues.



Gifting Gains

As social distancing guidelines were enacted, gaming merchants also experienced an **increase in gifting of software keys/virtual gift cards** by loved ones unable to attend in-person occasions and gift physical goods. When a software key is purchased as a gift, there is a higher possibility that the account purchasing the key will differ completely from the account receiving it. For example, the purchasing customer's email address will likely not match the recipient's. Such mismatched data elements would often be synonymous with a higher fraud risk but, as this gifting behavior for digital goods gains popularity, strategies need to be adjusted to account for these new situations.

Best Practice Rules for Resellers

Merchants also need to carefully determine how they conduct business with resellers in these trying times. Reseller transactions are usually comprised of unusual characteristics and/or mismatching data fields, like the gifting behavior previously mentioned. Working with an experienced fraud team and using due diligence can ensure that business is conducted only with resellers that are trustworthy and have not been associated with fraud or chargebacks at any point in the past. Fraud teams can **maintain lists of trusted resellers**, allowing genuine transaction volumes to flow through. This also assists in ensuring review teams' efforts are concentrated on identifying fraudulent resellers who may be using stolen or compromised cards. To proactively thwart unwanted exposure to negative and high-risk resellers, it is best to have a strong risk strategy in place and put thoughtful restrictions on high purchase amounts of software keys from unverifiable sources that could be conducting promotional abuse.

Beware BOTs

Unfortunately for merchants, fraudsters are ultra-aware of what is popular and often attempt to hide their activities among a larger number of genuine transactions. Fraudsters typically will attempt to run internet BOTs, or software applications, to purchase as many high-demand goods as possible and drain inventory. For the most part, internet BOTs are easily identifiable because they often contain gibberish values in either the email address or street addresses, will come from a single source (device or IP) and transact at a high frequency in a short period of time. Fraud strategies should be adjusted to be as strict as possible in these instances, and the use of velocity thresholds and restrictions is paramount. **It is strongly recommended that machine learning and neural model capabilities are used to better identify and restrict BOT activity**. Using machine learning allows fraud mitigation teams to build a profile of what is more than likely BOT activity and differentiate it from genuine transactions. If BOT behavior goes undetected, it can cause an increase in customer disputes, as well as a significant increase in chargebacks. One of the top priorities of a risk strategy should be to identify and restrict these types of transactions. Some fraudsters attempt to use BOTs that are not as rudimentary, so placing alerts on sudden spikes in purchasing behaviors or purchases from questionable sources can help fraud mitigation teams proactively respond and create blocks before BOT activity becomes overwhelming.

Taking Action Against Account Takeover

In addition to adjusting strategies to account for new customers transacting at a high rate, it's imperative to also **monitor existing accounts that have been dormant and suddenly become active**. These accounts will have high time-on-file values and positive purchasing history, which in most cases equates to the ideal customer for merchants. Unfortunately, such accounts are also the perfect targets for fraudsters attempting an account takeover. To thwart account takeover exposure, it is best to review time-on-file on all available individual attributes, such as card, email, device, etc. as part of the risk strategy. Monitoring accounts that have high time on file values on multiple attributes, but a sudden drop in one, can be a valuable indicator of account takeover. For example, if the customer's credit card and device have been listed on the account for a long period of time but suddenly the email is new or changed, and the customer attempts a high-value purchase, there is a higher likelihood that this account has been breached. Enabling restrictions and monitoring activity allows merchants to differentiate good accounts from breached accounts and ensures the safety and satisfaction of their long-time existing customers.

Value Your Volume

COVID-19 has significantly changed the way in which the world interacts and the **shift to a more virtual marketplace has yielded great results for eCommerce merchants and, specifically, for the gaming industry**. However, merchants must be flexible and willing to accommodate these changes. Having a strong and adaptable fraud strategy in place is a key factor for success and this strategy must prioritize the consumer experience. Adding new customers to the consumer base may come at a higher exposure to fraud if not properly planned but, with the right fraud tools and expertise, merchants can ensure a smoother overall experience for all. Fraud and chargebacks are unfortunately inevitable in the virtual world, especially when dealing with products that are in high demand, but having a fraud solution that can leverage the appropriate tools and ensure a resilient balance of genuine transactions to fraud transactions is critical in today's world. Focusing on stopping fraud alone will likely cause false positives and push consumers to shop elsewhere. Building a strategy that provides a fast, seamless experience for new and existing customers while meticulously stopping fraudsters helps create a satisfied end user and ensures there is less of a burden on manual review teams. When the world transitions to a new normal, you will notice higher revenues and new customers that have become loyal fans of your products or services.

1. ACI customer data, July 2020
2. https://www.theverge.com/2020/8/4/21353786/sony-ps4-sales-q1-earnings-2020
3. https://www.windowscentral.com/xbox-microsoft-q4-2020-earnings-gaming
4. https://www.theverge.com/2020/3/16/21181272/steam-concurrent-user-record-set-cs-go

ACI Worldwide is a global software company that provides mission-critical real-time payment solutions to corporations. Customers use our proven, scalable and secure solutions to process and manage digital payments, enable omni-commerce payments, present and process bill payments, and manage fraud and risk. We combine our global footprint with local presence to drive the real-time digital transformation of payments and commerce.

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

ATL1150 04-21

Authored by:
Sharell Barshishat
Risk Analyst, ACI Worldwide

ACI Worldwide
Real-Time Payments