iovation
A TransUnion® Company

GAMING CASE STUDY

GAMING PUBLISHER STOMPS OUT 90% OF FRAUD IN ONE MONTH

CHALLENGES

With fraudsters exploiting the company's primary customer acquisition strategy, and no way to keep identified offenders from returning, the company faced higher fees from its payment providers, and lost 25% of one title's revenue to chargebacks in just one month.

SOLUTIONS

Leveraging evidence of credit card fraud from other game makers, iovation FraudForce revealed connections between devices attempting fraud without interfering with customers' experience.

RESULTS

Using iovation, the company stopped $100,000s in chargebacks every month, saw a 90% reduction in its chargeback rate, kicked out fraudsters and their partners permanently, and restored its standing with payment providers.

THE REAL-TIME STRATEGY GAME MAKER ADDS IOVATION TO FIGHT OFF FRAUD SUCCESSFULLY.

They were under attack. In one month, the online gaming company's unsuccessful transaction rate, an indicator of chargebacks, spiked from an already steep 24% to a ruinous 100% of successful transactions. For every honest payment processed on one of its titles, another transaction was returned as fraudulent. Worse still, many of these unsuccessful transactions were coming from trusted customers' accounts. As customer complaints mounted, the specter of a large-scale fraud and account takeover assault took shape.

"It was horrific," says 'Ben,' the Game Operations Manager. "We could repair in-game damage to trusted customers' accounts, but that was a reactive move. It was much harder to regain players' trust. We want to keep the playing environment fun and fair to sustain user retention and average revenue per user."

Their payment partners were also losing trust. If the company didn't fend off the fraudsters quickly, it would be added to payment providers' warning lists, with the real pain of higher transaction fees and less favorable service conditions following close behind.

Worst of all, their defenses had a major vulnerability: "We had no way to kick fraudsters out permanently," says Ben. "They were opening new accounts faster than we could detect and close them."

Successful business model included fraud loophole.

Since its launch nearly 10 years ago, the company has worked to create innovative experiences for mobile and online competitive gamers. With hundreds of employees in multiple countries, and millions of avid customers around the world, this gaming company has been a rising star in the industry since its first breakout title. The company's success has been lauded as proof that higher average revenue per user is not a function of a large user base.

All of its games are free to play on multiple platforms, including Facebook, iTunes and Google Play. Players can choose to pay for advantages: some spend US$10, others spend US$10,000. Since there's no subscription model,

there's a perennial need to keep games fun and accessible for all players.

"Account creation on the website is lenient," explains 'Rebecca,' the Security Manager. "There's no two-factor authentication. You don't have to provide a real email address in order to keep playing."

"That's on purpose," Ben adds. "We want a low barrier to entry to contain our user-acquisition costs. iovation helps us keep the door wide open and welcoming on our site, while still protecting our players."

Fraudsters mounted large-scale ambush.

In a single month last year, before implementing iovation, one of their title's revenue plummeted 25%. For every successful transaction processed, another transaction was rejected. The culprit: credit card fraud leading to chargebacks. As chargebacks increased, so did fees and penalties from payment providers, biting deeper into revenue.

"A quarter of a game's revenue is a huge problem," Ben says. "We scrambled in the following month. That's when we discovered that we were under attack by this fraud ring. They had access to tens of thousands of stolen credit cards. They were attacking customers' accounts, and racking up fraudulent transactions. Up to this point, we never realized how big of a problem this could be."

The toxic mix of chargebacks and account takeovers threatened to destabilize the game's community. Dissatisfied players could further damage the game maker's brand on social media and chat forums.

Internal efforts didn't effectively staunch losses.

Before seeking outside support, the gaming company made two attempts to defend itself. First, it tried blacklisting the geographies and IP addresses that were responsible for most of the problems. When that didn't work, they adjusted velocity rules in the game. Neither attempt yielded satisfactory results.

"Blacklisting an entire country is too broad. It punishes good customers and cuts into revenue," Ben explains. "And anyway, IP blacklisting is fairly easy to get around. It wasn't effective against these attackers, who were quite savvy."

Next, they attempted to fight back from within their games. They allocated game engineers' time to in-game velocity rules, for example: requiring a certain amount of play time or level status before players could make purchases. This too proved to be a waste of effort.

"Those in-game solutions are costly," Ben explains. "We want our game engineers to spend their time making the game better and more fun. It didn't make sense to use them to combat bad players. And it didn't get to the heart of the issue: kicking fraudsters out for good."

iovation turned one-time victories into permanent wins.

Facing heavy losses to revenue and reputation, the gaming company realized that it would need reinforcements. The solution: combine iovation's FraudForce with a third-party payments fraud specific tool.

"The combination of the payments fraud tool and iovation did the trick," says Ben. "The two work hand in hand very well for us."

They now use the payments tool to evaluate each customer's payment method and profile. When a fraudulent transaction is identified, the company denies and flags the device attempting to make the transaction, and feeds that device's fingerprint – and other devices associated with it – to iovation. From then on, iovation prevents any of those devices from ever opening another account.

Evidence shared between allies added greater impact.

In addition to the payment fraud tool, the gaming company leverages relevant evidence (fraud and abuse reports added by other users) from iovation's globally-shared device reputation database.

"We love how iovation allows for incredibly granular control over our business rules," says Ben. "For example, we take into account specific evidence entered by about a dozen other gaming companies in our market. We don't pay attention to evidence relating to their policy violations because our user policies differ. However, we pay very close attention to evidence of credit card fraud. If we see that has been associated with a new user's device, we don't want it –or other devices associated with it- on our platform."

With access to iovation's global database of 5 billion devices and 55 million recorded fraud incidents, the online gaming company receives unparalleled breadth and depth of control over the way it keeps out confirmed fraudsters. Every piece of evidence that they contribute to iovation's database - tens of thousands every month- further hardens its defenses.

"We take great care to ensure that the evidence we're placing is accurate," says Ben. "It's not based on suspicions that they're thieves in the real world, or because they're stealing credit cards. The evidence we upload is based on the fact that we've caught them cheating in our games, violating our policy or attempting to commit fraud. We really like that granular level of control, and all the different evidence types we can draw from."

Defenses now set at every point of attack.

To get the most out of the solution, the gaming company has integrated iovation into the payments, registration and login parts of its website. From that point forward, they never have to worry about the same device returning to open a new account.

"We implemented iovation at the points where we saw the attacks were coming from," Ben explains. "It has helped us to keep the bad people out. That's the big value we get from iovation. From that point, there's a cascade of benefits: reduced chargebacks, higher user retention, and stronger relationships with payment processors. Removing bad users benefits all of those metrics."

Since their primary gaming platform has realized so much value from iovation, the company has since implemented the solution on its other platforms.

Deeply reduced chargebacks indicate strong ROI.

Before iovation, for every honest payment processed on one of its titles, another one was returned as fraudulent. Since implementation, that percentage has dropped by 90%.

"Compared with what we see in our other titles and platforms, 10% is more in line with our expectations," says Ben. "Chargebacks are really important as a way for us to measure the ROI for iovation."

"When we look at fraudulent chargebacks, we definitely see a reduction on the order of hundreds of thousands of dollars per month, thanks to iovation."

ABOUT IOVATION

iovation, a TransUnion company, was founded with a simple guiding mission: to make the Internet a safer place for people to conduct business. Since 2004, the company has been delivering against that goal, helping brands protect and engage their customers, and keeping them secure in the complex digital world. Armed with the world's largest and most precise database of reputation insights and cryptographically secure multi-factor authentication methods, iovation safeguards tens of millions of digital transactions each day.

iovation.com

Global Headquarters

iovation, a TransUnion company
555 SW Oak Street, Suite #300
Portland, OR 97204 USA

PH +1 (503) 224 - 6010
FX +1 (503) 224 - 1581
EMAIL info@iovation.com

United Kingdom

PH +44 (0) 800 058 8731
EMAIL uk@iovation.com

iovation®
A TransUnion® Company