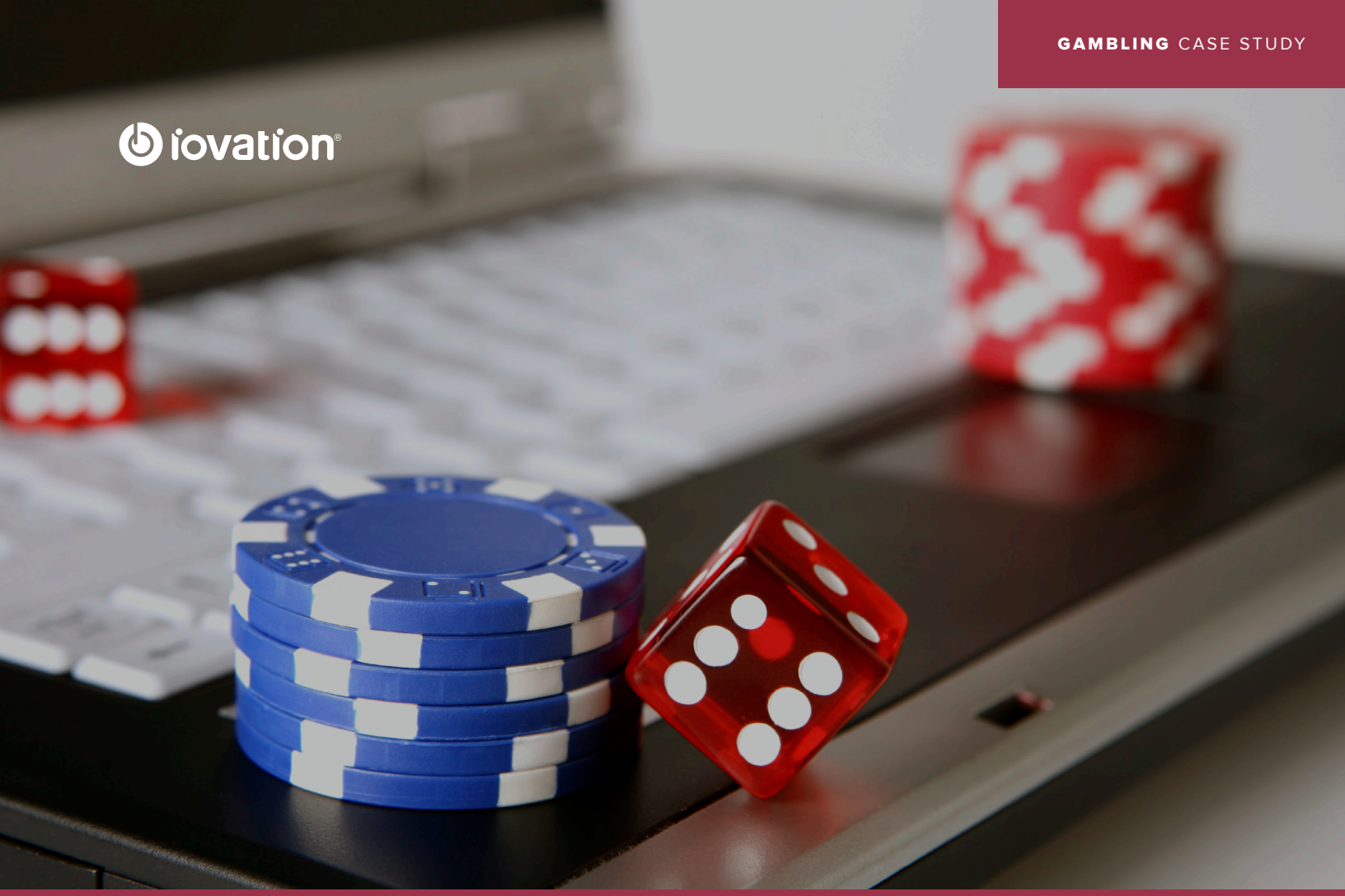
iovation®



PLAYCHERRY CASE STUDY

PLAYCHERRY STOPS FRAUD €50,000 AT A TIME

CHALLENGES

Unable to detect devices working together, PlayCherry was dealing with a community of sophisticated fraudsters who were regularly taking advantage of their player protection policy.

SOLUTIONS

Using iovation, PlayCherry leveraged credit card fraud evidence from other game makers to reveal connections between suspicious devices, creating a multi-layered defense.

RESULTS

PlayCherry saved tens of thousands of euros from bogus claims alone, and is shutting out fraudsters and their partners permanently. Today, PlayCherry's chargeback levels are less than 66% of the industry average.

IOVATION HELPS ONLINE GAMBLING OPERATOR KEEP CHARGEBACK LEVELS LOW, AND BONUS ABUSERS OUT.

Magdalena Gniadzik-Johansson, Head of Payments and Fraud at PlayCherry Limited, had a bad feeling about a group of new accounts.

"It was all too clean," says Johansson. "Our payment processors didn't detect any risk, but we noticed suspicious patterns. They all played the same high-stakes games with the same large bonuses."

After tracking these players' seemingly separate devices for several days, Johansson and her team connected them as a sophisticated group of bonus hunters capable of raking in tens of thousands of euros if left unchecked.

"These individuals weren't afraid of gambling with big money," explains Johansson. "If they won, they would win a lot. If they had only opened a single account in accordance with our usage policy, that wouldn't have been a problem. But this group was opening many accounts to multiply their chances. With enough time, accounts and patience, they could win €20,000, €30,000, even €50,000."

WE'RE VERY SATISFIED WITH IOVATION. IT HELPS US STOP MULTIPLE REGISTRATIONS, A GIVEAWAY SIGN OF BONUS ABUSE.

Magdalena Gniadzik-Johansson,
Head of Payments and Fraud at PlayCherry

Remarkable success online attracts fraudsters in droves

For more than 50 years, PlayCherry's parent company has offered fun and excitement for millions of European gamblers. Two years after entering the digital casino space in 2012, PlayCherry grew by an impressive 44%, the second fastest in the industry, while deposits increased by 50%. For the second consecutive time, it also earned International Gaming Award's Online Gaming Operator of the Year.

Its successful growth has also attracted more fraudsters. Johansson estimates an increase of 20-30% in attempted fraud and registrations from restricted countries.

PlayCherry now relies on iovation's fraud prevention service as an integral part of its anti-fraud stack. Their implementation of iovation has expanded from just registrations to include the cashier, says Johansson. "We included iovation on deposits and withdrawals to prevent fraud, account takeover, and deposits from restricted countries."

Why the gambling institution chose iovation when it went digital

Working in conjunction with existing fraud-detection techniques, iovation's device fingerprinting solution provides online gambling operators with a multi-layered defense that reduces both the rate and impact of credit card fraud and bonus abuse.

By tracking a device's historical behavior—not the players' personal identifying information—online casinos like PlayCherry gain unique insight into account creation and relationships, and uncover fraud that is otherwise invisible. iovation's industry-leading database of 3 billion devices and 30 million recorded fraud incidents provides penetrating knowledge of the devices used to access its sites.

Other operators' evidence a key part of PlayCherry's strategy

Having calibrated iovation's configurable business rules, account relationship monitoring, device profiling and device anomaly checks, PlayCherry receives a real-time decision to allow, deny or review each transaction. From evidence of credit card fraud to geolocation mismatch to blacklisted countries, Johansson has complete control.

For example, evidence of chargebacks from other operators triggers an immediate denial, says Johansson. "We've learned to pay close attention to a select group of [iovation's] subscribers that supply the most relevant evidence for our needs. Even then, we only account for a subset of their evidence. Their criteria for bonus abuse may be different from ours, but credit card fraud always means an unwelcome player."

How does PlayCherry choose among the other users it 'listens' to? Every subsriber decides to remain anonymous or self-identify. Self-identified users can see the contributor of each piece of evidence, allowing for additional fine tuning of their business rules.

iovation stands guard where PlayCherry needs it most

"We're very satisfied with iovation," says Johansson. "It helps us stop multiple registrations, a giveaway sign of bonus abuse. By checking new account applications, we eliminate accounts from countries we're not licensed to serve. For example, US customers coming through UK. It's easy for savvy visitors to change their apparent IP address. But iovation can pinpoint the true IP. This way, we can be sure we're not breaking any terms or conditions of our licensing." iovation is always PlayCherry's first checkpoint for deposits. If the associated device has certain evidence placed on it from another subscriber, the deposit will stop right there, says Johansson. "We don't want that traffic. If no one has evidence on the device, we'll allow the deposit. In some cases, it's the payments provider that catches it. Whenever we can, we add evidence to iovation's global fraud database. It benefits everyone to stop fraudsters." In addition, PlayCherry uses iovation to check accounts at withdrawal.

> **THANKS IN LARGE PART TO THE EVIDENCE COLLECTED FROM IOVATION, MGA TENDS TO SIDE WITH US. JUST A SINGLE CASE COULD EASILY BE WORTH €20K, 30K, 50K.**

The company always confirms that its players are requesting withdrawals to the same devices where the deposit came from. This prevents account takeovers and confirms that the player is in a country where PlayCherry is licensed to operate.

iovation also covers loopholes left by accepted e-wallet services. Since players may register an account with a verified e-wallet, there's no reason to stop them. When the fraudster is discovered heating, PlayCherry withholds the winnings while they review the account. Fraudsters complain quickly to the Malta Gaming Authority (MGA) to try to force a pay out. iovation's extremely detailed device fingerprint helps PlayCherry defend itself against these claims, says Johansson.

"We have to refund their original deposits, but we don't have to pay out their winnings, which can mount into the tens of thousands of euros."

"Several times each year, fraudsters will go to the trouble of complaining to the MGA," says Johansson.

Flexibility to meet evolving anti-fraud needs

Two years after implementing iovation, Johansson hasn't made substantial changes to her original rule set: "It works well for us. When we launch a new site, we apply the same rule set and make adjustments as we go. It's really nice to be able to implement iovation so easily on our new websites as they come online."

The easy user interface saves PlayCherry's IT resources. Instead of relying on IT to set a new alert based on evidence in the company's system, Johansson can easily adjust the rule set in iovation: "It's far easier to block fraudsters in iovation than redesign our system. We really appreciate the simplicity."

"iovation helps keep our chargeback level low."

Why has PlayCherry stayed with iovation since it launched its online gambling business in 2012? First, iovation is very helpful in contesting fraudsters' complaints to the Malta Gaming Authority (MGA).

AS WE HAVE TO KEEP OUR CHARGEBACKS LOW TO CONTROL OUR FEES, THAT'S REALLY IMPORTANT FOR US.

Second, PlayCherry credits iovation for helping to keep its chargeback level enviably low. Where Johansson estimates that the industry suffers an average chargeback level between 3-6%, she believes that PlayCherry's chargeback level rests below 1%, a 66-83% difference.

ABOUT IOVATION

iovation protects online businesses and their end users against fraud and abuse, and identifies trustworthy customers through a combination of advanced device identification, shared device reputation, customer authentication and real-time risk evaluation.

More than 3,500 fraud managers representing global retail, financial services, insurance, social network, gaming and other companies leverage iovation's database of more than 3 billion Internet devices and the relationships between them to determine the level of risk associated with online transactions.

The company's device reputation database is the world's largest, used to protect 16 million transactions and stop an average of 300,000 fraudulent activities every day.

The world's foremost fraud experts share intelligence, cybercrime tips and onlinefraud prevention techniques in iovation's Fraud Force Community, an exclusive virtual crime-fighting network.

Global Headquarters

iovation Inc
111 SW 5th Avenue, Suite 3200
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

www.iovation.com

iovation®