



INTERNET GAMBLING SITES:

**Expose Fraud Rings
and Stop Repeat Offenders
with Device Reputation**

Confident Casinos: How to stop fraud before it starts

The convenience and excitement of gambling online has been the driving force behind the phenomenal growth of the online gambling industry. But as more people turn to online poker, roulette, blackjack, sportsbooks and other casino games, cyber criminals are becoming more sophisticated in finding ways to defraud legitimate players and the gambling sites they play on. As a result, gambling sites are forced to deal with a wide spectrum of Internet crimes and other in-game abuses that cost the industry hundreds of millions of dollars in fraud losses each year. Despite efforts to thwart criminal activities such as fraudulent deposits, chargebacks, cheating, collusion and money laundering, today's sophisticated fraud rings pose a greater threat to online gambling providers than ever before.

With more personal information accessible over the Internet, identity-based fraud management systems alone do not provide a comprehensive solution for effectively detecting and preventing online fraud. Fraudsters, using the Internet to buy, sell and trade personal and financial information, have built thriving illegal networks to share data and techniques on how to defraud online gambling businesses. In order to reduce fraud loss that directly impacts their bottom line, online gambling sites must adapt more effective solutions that look at information independent of what data is supplied by players. A device fingerprinting solution—such as iovation ReputationManager 360™—provides unique insight into the computers being used to connect to online gambling sites, exposing a computer's reputation and uncovering hidden device-to-account relationships that other fraud tools often miss.

Device fingerprinting helps identify fraudsters at the source so online gambling sites can shut down repeat offenders and keep them out. Working in conjunction with existing fraud detection techniques, a device fingerprinting solution provides online gambling sites with a comprehensive fraud management solution. This white paper will help you understand what new and innovative techniques can be used to combat online fraud and abuse, and how online casinos can realize a true return on investment by reducing losses from fraud exposure and increasing operational efficiency within the fraud detection process.

Organized Fraud: A Growing Threat to Online Casinos

The online gambling industry has experienced phenomenal growth. According to H2 Gambling Capital research firm, online casinos generated \$22.6 billion in global revenues in 2008, up from \$17.6 in 2006. Unfortunately, while the online gambling industry grows, so does organized fraud; cyber criminals are working hard to uncover and sell people's personal information—such as name, address, social security number and credit card details—and share techniques on how to defraud online gambling sites. As a result, the online gambling industry stands to lose hundreds of millions of dollars annually to fraud exposure if effective anti-fraud strategies aren't put in place.

Fraudsters perpetrate a wide range of fraud and in-game social abuses including credit card fraud, fraudulent deposits, chargebacks, cheating and collusion, chip dumping, promotion and bonus abuse, email spam, money laundering and account takeover. Despite gambling sites' efforts to detect suspicious players, Internet-savvy criminals have learned how to mask their true identity by changing account information to circumvent conventional methods of fraud detection such as IP address and geo-location validation, third-party credit verification, and other tools that monitor and analyze player activities such as winning percentage, hands played, and who they've won and lost to (see Figure 1).

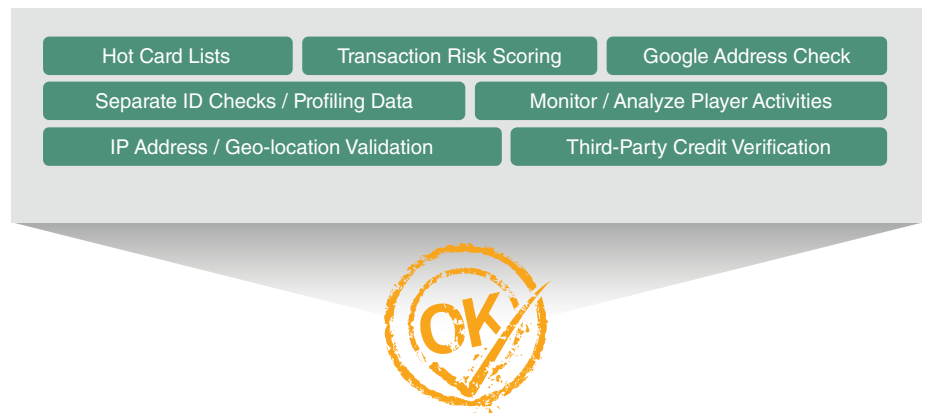


Figure 1: With more personal information accessible over the Internet, fraudsters are getting better at defeating conventional methods of fraud detection.

Closing the Revolving Door on Repeat Fraud

As fraudsters routinely change identities, many online gambling sites are being abused by the same people over and over again without even knowing. Unfortunately, for online casinos that lack the ability to identify fraudulent computers, even if a fraudulent account is detected and shut down, there's nothing to prevent the fraudsters from immediately creating a new account under another identity. This creates a revolving door for repeat fraud and abuse.

As fraudsters continue to hide behind the Internet's built-in anonymity, identity and financially-based fraud management systems alone are not sufficient in catching sophisticated fraud and abuse. The inability to identify fraudsters sitting alongside legitimate players at a virtual poker table underscores the growing need for online casinos to deploy more effective solutions that look at information independent of what data is supplied by users.

Working in conjunction with existing fraud detection techniques, a device reputation solution, such as iovation ReputationManager 360, provides a comprehensive solution for fighting all forms of online fraud and abuse.

The Financial Impact of Fraud

If fraudulent accounts are not identified in the network, online gambling sites suffer from a multitude of setbacks that significantly impact their bottom line, including:

- **Revenue Loss:** The more successful cyber criminals are at creating fraudulent accounts or illegally accessing existing accounts, the greater the loss an online casino will experience.
- **Higher Fraud Expenses:** Fraud detection tools that cannot effectively identify bad guys drive up fraud expenses and lengthen the fraud detection process.
- **Operational Inefficiencies:** More suspicious accounts that require additional review create huge operational inefficiencies and require additional personnel for deeper investigation of risky accounts.
- **Member Attrition:** Once a player experiences financial loss as a result of online fraud, retaining that customer becomes extremely difficult. This can result in additional customer attrition and revenue loss.
- **Tarnished Reputation:** An online gambling provider struggling with high fraud activity can find it difficult to earn new business with both customers and advertisers.

A Comprehensive Defense

In order to effectively combat identity theft, online gambling sites must move beyond relying almost solely on personal information for fraud analysis. As identity-based fraud management systems continue to crunch the same identity data in a variety of ways, an entirely different technique, one that looks at information independent of what is provided by the user, creates significant value and uplift in the fight against fraud.

A device fingerprinting solution, such as iovation ReputationManager 360, focuses on the device—not the person—to identify and re-identify a user. This kind of device-centric solution provides online casinos with unique insight into account creation and relationships and exposes fraud that is invisible to other tools. Working in concert with other preventative techniques, a solution that identifies fraud through

the historical behavior of a device provides a multi-layered defense that reduces both the rate and impact of online fraud and abuse.

Eight “Must-Haves” for a Device Fingerprinting Solution

To effectively combat online fraud and abuse, a device fingerprinting solution must have several key components that allow online gambling providers to instantly identify known fraudulent devices without impacting the user experience or good customers. The following are things to look for when shopping for a device fingerprinting technology:

- 1. Instant Decisioning:** The ability to receive an ‘accept,’ ‘deny’ or ‘review’ response in real-time saves significant time and money. You can automate decisioning when a new player creates an account, logs in, or makes a financial transaction.
- 2. Transparency:** A fact-based approach is necessary to uncover hidden associations between problematic accounts and the devices used to create those accounts.
- 3. Low False Positives:** Distinguishing good accounts from bad ones allows providers to instantly act with certainty, without devoting precious time and resources to reviewing and analyzing good accounts.
- 4. Flexibility:** A solution that offers flexible implementation options—such as a software download, web print, and risk scoring for new devices—leverages multiple variables to provide the strongest data available to identify devices.
- 5. Pattern Matching:** Pattern matching analyzes individual non-unique identifiers to expose unusual activities and abnormalities in what is often perceived as normal behavior.
- 6. No PII:** A solution that looks at information independent of what data is supplied by the user, not requiring any personally identifiable information (PII), provides a substantial uplift over existing PII-based fraud management and risk scoring solutions.
- 7. Scalability:** As fraud detection processes struggle to keep up with an increasing number of accounts, a highly scalable solution allows online gambling providers to grow their business—adding new games, partners, and affiliates—all while keeping their business protected by a fraud detection system that scales.
- 8. Cost Effectiveness:** A highly effective fraud tool that is also cost-effective provides a real return on investment through fraud reduction and improved operational efficiency within the fraud-detection process.

Flexible Integration Options for Internet Gambling Sites

iovation ReputationManager 360 offers a range of integration options that support existing fraud prevention strategies, including download device print, web device print, pattern matching and risk assessment. These multiple integration options provide the flexibility to fight a wide range of online fraud and abuse issues while mitigating both false positives and false negatives in the fraud-detection process (see Figure 2).

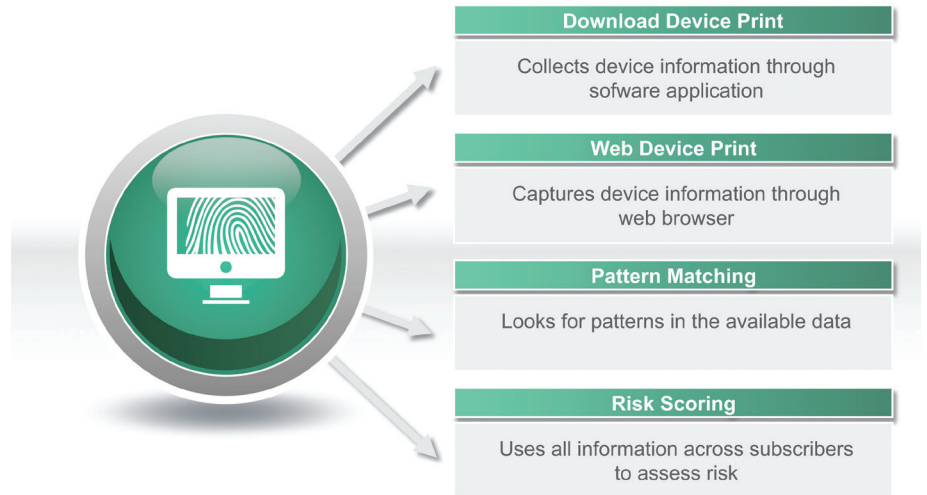


Figure 2: Device printing technologies provide multiple ways to identify or re-identify a unique device.

Unlocking the Power of Device ID

While device printing is integral to preventing the creation of fraudulent accounts, its effectiveness also depends on how the data is used. To make the most use of device fingerprinting technology in a fraud management system, the solution must go beyond collecting data from a single site. With online criminals no longer limiting themselves to a single target or industry, a system that restricts information to a local system limits its ability to recognize fraudsters using multiple identities to create hundreds of fraudulent accounts across the Internet. However, sharing device information across a larger, centralized network utilizes the data more effectively and exposes extended device-to-account relationships across multiple networks and industries.

iovation ReputationManager 360 draws on the power of its shared Device Reputation Authority™ (DRA), a global fraud database which stores over 650 million device reputations and their associations with other computers and accounts across the Internet. Once a unique account identifier and device fingerprint are in iovation's network, fraud teams will receive alerts whenever a device that has been associated with fraud comes to their online community. This allows subscribers to determine in real-time if they want to accept, decline, or review new and existing accounts (see Figure 3).

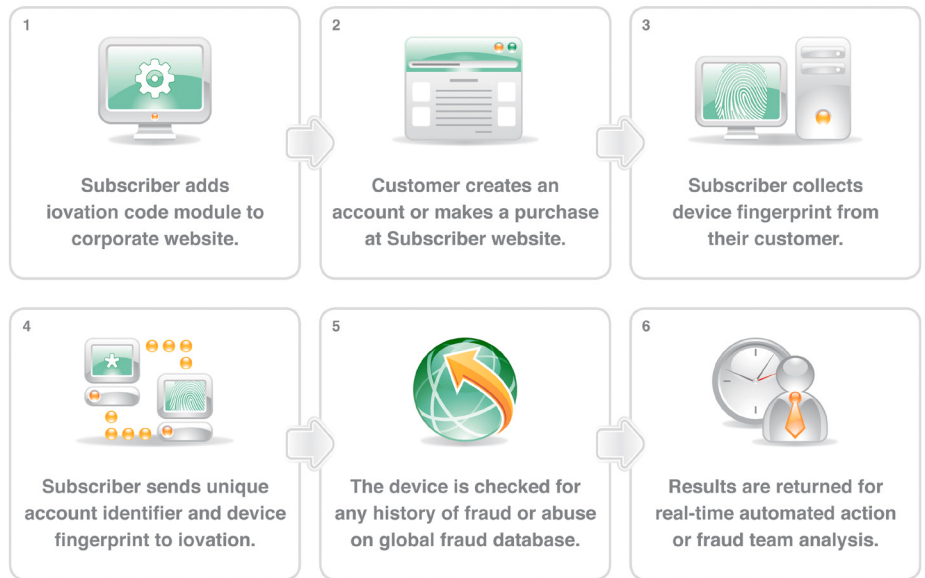


Figure 3: Once device information is added to the network, alerts are sent to subscribers when a device returns.

Collaborating with peers, and other industries united against fraud, unlocks the power of device ID. This "no tolerance" approach of working together in a shared environment allows gambling sites to benefit from tens of thousands of additional resources, tools and experiences, without adding to their initial fraud protection investment.

Expanding Fraud Detection Capabilities

Combining innovative device fingerprinting technologies with a shared network of device intelligence allows gambling sites to expand their existing fraud detection capabilities with the following components:

- Software Downloads and Web Technologies:** Software downloads, such as ActiveX, and Web technologies for cookies, flash-stored objects and java script that leverage IP addresses, geo-location and other non-unique identifiers, help recognize or re-recognize a device every time it creates or accesses an online account.
- Shared Intelligence:** Sharing fraud histories with peers across industries provides additional resources, tools and experiences that expand an online gambling site's ability to identify devices that have previously committed fraud or abuse.
- Forensic Analysis:** When computers are new to iovation's network, risk scores and custom reports help identify suspicious activities based on recognizing the characteristics that are often seen with high-risk devices.

- **Industry Expertise:** With years of experience helping online gambling sites fight fraud, our fraud experts can proactively spot a wide spectrum of fraud trends and assist in the development of new and effective fraud management strategies.

The Business Benefits of Device Fingerprinting

A device fingerprinting solution that enables remote gambling sites to shut down bad accounts in real-time provides a number of significant benefits, including:

- **Reducing Losses from Fraud Exposure:** In the case of one leading Internet gambling provider, iovation ReputationManager 360 helped the company reduce its chargeback rates from above 10% of its total deposits—equating to 20% of its gross revenues— to below 0.43%. “We started to see that many chargeback accounts had all logged in from the same device,” said the online gambling site’s fraud manager. “iovation ReputationManager 360 allowed us to instantly shut out their devices so they couldn’t log into the system anymore.”
- **Increasing Process Efficiency:** Being able to stop fraudulent accounts at the point of creation significantly reduces the costly and time-consuming review process. With fewer suspicious accounts queued for review, online gambling companies can spend less time analyzing, evaluating, diagnosing and closing both good and bad accounts. Streamlining the fraud process also allows gambling sites to decision accounts faster, eliminate processing delays, and improve overall player trust and satisfaction. iovation was instrumental in helping one company reduce its fraud losses fivefold without interrupting the user experience.
- **Lower False Positives:** Low false-positive rates enable online gambling sites to consistently block bad accounts without impacting good players. iovation’s device fingerprinting technology has been highly effective in mitigating false positives, which leads to more efficient, confident decisioning. “Many times, other software programs identified our good players as fraudsters,” said Leonid Nezgoda, Managing Director, Entraction Estonia, “This was not the case with iovation ReputationManager 360.”

Conclusion

Technology has been the driving force behind the phenomenal growth of the online gambling industry. Unfortunately, while the Internet makes it easier and more convenient to place bets, it also provides the means for more organized cyber criminals to defraud poker sites and their good players. Despite efforts to thwart the fraudsters’ more sophisticated schemes, fraudsters can still get past conventional methods of fraud detection. As a result, online casinos must deploy different techniques—that work in conjunction with existing anti-fraud tools—in order to identify fraudulent devices that are creating multiple accounts. This can reduce the rate and impact that fraud and other unwanted abuses have on Internet gambling sites.

A device fingerprinting solution such as iovation ReputationManager 360 provides online casinos with a number of significant benefits that reduce loss from fraud exposure, increase operational efficiency within the fraud-prevention process, lower false positives, and provide a return on investment that is essential to the success and growth of online gambling business.

About iovation

iovation protects online businesses and their end users against fraud and abuse through an industry-leading combination of shared device reputation and real-time risk evaluation. 2,000 fraud managers around the globe leverage iovation's database of Internet devices and relationships between them to determine the level of risk associated with any type of online transaction. Leading retail, financial services, social network, gaming and other companies make real-time queries to iovation's knowledge base of 650 million devices from every country in the world. Every day, iovation protects more than 7.5 million transactions and stops over 150,000 fraud attempts.

To begin reducing more fraud and abuse within your online casino, please call +1.503.224.6010 or email info@iovation.com.



iovation Inc.

111 SW 5th Avenue, Suite 3200, Portland, OR 97204
+1.503.224.6010 tel | +1.503.224.1581 fax
www.iovation.com