



“ We look for best-of-breed suppliers and what iovation has delivered far exceeded our expectations. Device reputation doesn't only help stop fraud; it also helps prevent it in the future. ”

Leonid Nezgoda
Managing Director,
Entraction Estonia

Entraction Uses Device Reputation to Carry Out "Zero Tolerance" for Fraud

One of the leading and fastest growing suppliers of systems for online betting, casino, poker and bingo uses iovation to combat online fraud and abuse.

Challenge

- Entraction's successful platform attracted online criminals
- Risk of financial fraud, collusion, money laundering and infringements of rules
- Existing tools did not meet Entraction's high standards on reducing fraud

Solution

- Required additional sophisticated solutions that would not disrupt the player experience
- Required solution to be efficient, scalable, cost-effective with low or no false positives
- Needed top-of-class provider to tackle not only fraud detection but also prevention

Results

- Quickly gained ability to stop repeat offenders
- Easy for fraud team to adopt and add into existing workflow
- Results were remarkable – way beyond expectations
- iovation's fraud management service returned more than five times the investment

Background

Founded in 2000, Entraction supplies complete systems for online gaming, meaning that, for example, a media company wishing to integrate gaming into its website does not need to invest in payment solutions, customer support and other infrastructure. Over and above systems for poker, casino, betting and bingo, Entraction supplies support, affiliate systems, promotional tools and payment solutions.

Entraction has developed proprietary systems for poker, betting and parts of the peripheral systems on offer. Other systems are supplied by third parties. Entraction's strategy is to successively replace third party systems with those it has developed or acquired, where commercially justified. A prerequisite for success in Entraction's endeavours to be one of the world's three largest suppliers within the digital gaming industry is to be able to control the development of new products and services to ensure that Entraction has the best offerings in the market.

Partners can choose between an integrated solution containing a customized mix of different products or a turnkey solution in which the partner is responsible only for marketing. The company has proprietary software for poker and sports betting and licenses casino services and bingo from third parties.

With success comes threat

The company's success, skyrocketing since 2006, has been attributed to its excellent technology platform provided to customers and partners alike. However, with growth came the reality of fraud.

The types of fraud seen by Entraction included credit card fraud, friendly chargebacks, chip dumping, player collusion, identity theft, and bonus abuse. In addition, fraudsters were increasingly trying to use Entraction's gaming software to launder money.

Entraction has a "zero tolerance" policy towards fraud, collusion, money laundering and other forms of infringements of laws and rules. With its popularity and growth, Entraction needed iron-clad protection.

According to Entraction Estonia Managing Director, Leonid Nezgoda, "Fighting fraud and money laundering is the ultimate social responsibility. The majority of companies have to realize that while being better at fraud detection and prevention is a competitive advantage, it shouldn't be, really. The industry should stand together on the issue of zero tolerance for money laundering."

Tool evaluation

With the influx of fraud, Entraction focused on getting their house in order. They developed in-house tools and procedures necessary to reduce fraud. They had good results, but were still looking for ways to enhance efforts. They needed top-of-class providers to tackle fraud detection and prevention. To remain focused on what they excel at, Entraction began the search for key technology partners.

The primary criteria for selecting a fraud detection tool was that it must:

1. Not interfere with player's experience
2. Provide efficiencies in the review process
3. Detect and prevent fraud effectively
4. Be cost-effective / affordable

Initially this seemed like a simple list – finding a product with a proven track record, that is cost-effective, and that does not interrupt the user experience. What they found was that many of the tools evaluated did interrupt the user experience. In other cases, there were new and unproven tools on the market which were very expensive and lacked sophistication. While those tools may have reduced fraud, they had a significant effect on the good players as well. Nezgoda says, “Many times, the other software programs identified our good players as fraudsters. We did not find that to be the case with iovation ReputationManager.”

Solution: iovation ReputationManager

Entraction had no reservations about the effectiveness and efficiencies that were possible using device fingerprinting paired with device reputation; this is real data pulled from the user's computer, coupled with fact-based fraudulent evidence from that computer's past. Entraction's list of iovation advantages included:

- Device reputation
- Players' experience
- Internal audits
- IP address checks
- Manual checks
- Proactive approach
- Cost-effective

If Entraction encounters a fraudster in their network, they now tag all associated devices to prevent the individuals from coming back repeatedly with new profile and credit card information.

Lightning-fast integration

Integration was simple and fast. The time from choosing iovation as a partner to having ReputationManager in production was just one month. During this process, Entraction went through five steps to implement iovation ReputationManager.

1. Decide the integration points

- Account Login
- Registration/Account Creation
- Cashier/Financial Transaction

2. Apply the code to the website or download

- Sample code supplied in various languages by iovation

3. Determine the business rules

- Which fraud and abuse evidence types do we care about?
- When should we Allow, Deny, or Review transactions?

4. Integration testing

- A client integration environment was provided to fully test the code and production data

5. Go live

Results were beyond expectations

After implementing iovation, the computers connecting to Entraction's online gaming sites established reputations based on how they were used. If a device caused a serious problem on one gaming site, this fact-based evidence is shared with other iovation subscribers. By linking the computer's reputation to its related online accounts, Entraction fraud managers can now see exactly how a particular computer has been used in the past and are better equipped to expose and prevent the fraudsters from coming back.

The reduction in online fraud after putting iovation ReputationManager in place was remarkable. Entraction can now proactively identify risky and suspicious behavior, expose fraudsters before they cause a problem, and stop literally thousands of fraudulent and abusive activities each day.

After implementing iovation ReputationManager and other systems, Entraction has returned more than five times the investment. Their chargeback rates also declined to close to zero. "Even after the second year of having iovation in place, we still see our chargeback rate on volume of transactions continue to decline," said Nezgoda.

Ongoing reporting and forensic research

Business rules are set up for automating the process of accepting, denying or reviewing transactions. iovation also provides a web-based reporting tool for further forensic research.

Transaction history report

The “Transaction History” report is shown from the device perspective. You can see from the transaction history below that after evidence was placed on this device, all subsequent logins with associated accounts have been denied.

164996261 : This device is affected by associated evidence : 1-1 Credit Card Fraud

evidence : 1-1(Entraction);
0 Associated Devices (4 affected), 4 Associated Accounts. No exceptions.
No Other subscribers have seen this device.
First seen by you: March 24, 2009 1:13:51 AM First seen by anyone: March 24, 2009 1:13:51 AM

Device Details Open All Close All

Transaction History

Last 100 Trans Last 24 Hours Last 7 Days Last 30 Days Last 180 Days

Page: 1 of 1 Go Records found: 6

Date/Time	Result	Tracking Number	Rule	Reason	Account	IP Address
March 25, 2009 11:26:52 AM	Denied	1698961318	N/A	N/A	gimme_yerchips	91.211.104.1
March 25, 2009 8:45:19 AM	Denied	1698568737	N/A	N/A	gimme_yerchips	91.211.104.1
March 25, 2009 8:26:08 AM	Denied	1698525770	N/A	N/A	smokingaces_0155	91.211.104.1
March 25, 2009 8:17:20 AM	Denied	1698506402	N/A	N/A	bigtime_k8	91.211.104.1
March 25, 2009 8:14:12 AM	Denied	1698499578	N/A	N/A	bigtime_k8	91.211.104.1
March 24, 2009 1:13:51 AM	Allowed	1694645253	N/A	N/A	0155poker_k8	77.108.92.108

Page: 1 of 1 Go Records found: 6 Show: 25 Results

Association Matrix

Accounts	Devices
0155poker_k8	164996261
gimme_yerchips	↔
bigtime_k8	↔
smokingaces_0155	↔
gimme_yerchips	↔

Result	Account
Denied	gimme_yerchips
Denied	gimme_yerchips
Denied	smokingaces_0155
Denied	bigtime_k8
Denied	bigtime_k8
Allowed	0155poker_k8

Additional uses for device identification

Entraction found that device identification is reusable for many different purposes besides stopping external fraud and understanding hidden relationships between accounts.

- Internal audits
- Bonus fraud
- Risk assessment for different markets
- Understanding partner behavior
- Understanding the “true” number of players

Using evidence from other businesses

One of the common reports of interest to Entraction includes a list of “bad guys” at other online businesses that also have accounts on the Entraction network. It allows Entraction to understand what additional accounts in their network (tagged to devices associated with fraud) exist in their network and could potentially cause problems.

Gambling / Sportsbook			
Device	Evidence Type	Evidence Date	Association Date
device_101561011	1-1 Credit Card Fraud	11/17/2008 09:15 AM	03/16/2009 04:09 PM

Financial Services / Credit Issuer			
Device	Evidence Type	Evidence Date	Association Date
device_163151002	1-6 Potential Fraud	03/12/2009 01:18 PM	03/16/2009 06:27 AM
device_163151009	1-6 Potential Fraud	03/12/2009 01:18 PM	03/16/2009 06:27 AM

Online Community / Internet Dating Site			
Device	Evidence Type	Evidence Date	Association Date
device_150321003	1-1 Credit Card Fraud	03/16/2009 11:51 AM	03/14/2009 05:50 AM
device_160811004	1-1 Credit Card Fraud	03/16/2009 11:50 AM	03/08/2009 10:49 AM
device_160271006	3-9 Scammer/Solicitation	03/16/2009 02:23 PM	03/10/2009 12:52 AM
device_159541014	3-9 Scammer/Solicitation	03/16/2009 12:11 PM	03/02/2009 01:18 AM

Gambling / Poker Site			
Device	Evidence Type	Evidence Date	Association Date
device_45321007	1-6 Potential Fraud	03/16/2009 10:14 AM	02/17/2009 03:48 AM

True partners fighting cybercrime

iovation ReputationManager is and continues to be Entraction's number one strongest technology partner for continued business success. With iovation, Entraction can remain focused on running successful online betting, casino, poker and bingo networks, knowing that their best-of-breed partner is effectively and efficiently managing fraud for their business.

To learn more about iovation ReputationManager™ and how it helps organizations fight online fraud and abuse, visit www.iovation.com.



For more information about Entraction or their software systems and services, please contact:

Entraction
P.O. Box 3108169 03
Solna, Sweden
+46 8 564 884 60 tel
info@entraction.com
www.entraction.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