IDVision with iovation

Social

Case Study

Social network fights back on affiliate fraud and wins

Challenge

Fraudsters were abusing the social network's affiliate programs by creating fake memberships, disrupting good community members and receiving commissions on those phony registrations.

Solution

iovation's FraudForce provided deep intelligence around the IP and ISP used by member devices, and associated member accounts with the devices accessing them – all without disrupting the user experience.

Results

The company was able to efficiently pinpoint suspicious activity and identify problematic sites, resulting in the closure of 400 bogus accounts related to a single publisher.

Social communities are complex networks that are driven to provide an outstanding membership experience, offer quality content and generate revenue.

This online social community gives people the ability to network and stay connected. They have a large database that covers tens of millions of people.

iovation's fraud prevention service gives this social community the ability to dig deep into their network to root out fraud. Tracking down affiliate fraud can be a complex puzzle, especially when the pieces involved are completely unknown. iovation offers the ability to uncover links and connections between devices, accounts, and locations that fraudsters work hard to hide.

Affiliate marketing drives customer acquisition

This social community uses publishing networks to place ads on affiliate sites to recruit new members. When a membership request originates from the affiliate's marketing efforts, they reward the affiliate with a commission. Affiliate marketing has grown in complexity with multi-tier programs distributing a percentage of the commission into a referral network of sub-publishers.

Affiliate fraud was almost impossible for us to uncover before iovation. We saw nearly all our fraud drop after implementation. The reduction was absolutely huge.

Director of Policy Compliance

"At any one time we could be working with 10 to 15 publishers, who in turn are working with groups of sub-publishers," said the Director of Policy Compliance. "Some have bounty referrals with placement all over the Internet."

Since affiliates generate income based on the number of registrations they can collect, volume is important to them. Financial motivation is the key driver as to why some downstream participants decide to defraud the system. Fraud that spans large networks of publishers, sub-publishers, and websites can be very challenging to detect and stop. These layers create a rampant and overwhelming tracking issue when it comes to pinpointing a specific site and link being exploited by fraudsters.

Unraveling complex affiliate fraud

It's essential to verify the legitimacy of new members that come through affiliate links since the social network pays a commission on each one. Payouts on fraudulent registrations are a cost that cuts directly into revenue with absolutely no benefit.

This community used iovation's FraudForce to uncover hundreds of new member accounts associated with one device and ISP. This immediately raised a red flag that prompted a deeper investigation into where these new registrations were originating and the general level of fraud on their affiliate networks.

"The quality of our content and member interactions is extremely important to us. We never want fraud to intrude on our member's experience of the community. Our team is very conscientious and proactive when it comes to reaching out to publishers when we have a concern," said the Director of Policy Compliance.

Abusing domain services for fraudulent email activity

One example of acquisition fraud is when a person opens multiple new accounts using fake email addresses. When online banners go up with a sign-up link and the sales ID of the publisher, the publisher will then receive a percentage of the commission.

By leveraging iovation's global network of device intelligence, the social network will also know if any other iovation clients have had a problem with a device and the type of problem.

The fraudster then begins to create fake registrations. Domain services are used to create an unlimited number of email addresses. Since the email addresses are technically legitimate, even though they've been created purely for abusive activity, the application process accepts them because the domain has been verified. This creates a huge problem for the advertiser, when a fraudster spends hours every day creating hundreds of fake registrations.

"This is where iovation is so invaluable. I'm able to look at the ISP that registrations have come through (two to three times a day) and determine if it is a proxy or odd in some way. The more suspicious details and anomalies I find, the more I keep digging. From there I look at the account information to see if they all come from the same Sales ID. When I saw 400 accounts created, all through the same suspicious ISP, and all coming through a link from the same publisher, it was obvious that I had uncovered the problem," said the Director of Policy Compliance.

Pinpointing 1 bad affiliate ad = significant fraud reduction

The suspicious ISPs are discovered with iovation's device reputation technology and matches the ISP internally to the referring URLs. This helps them identify the exact web page where the publisher placed the ad that is being used for fraud. In one instance, when the compliance director made a publisher remove a specific ad based on her investigative work, it obliterated nearly all of the fraud they were experiencing. This site had previously been considered an excellent source of traffic but this social network was able to show that although the traffic volume was high it was full of fraud.

"We wouldn't know any of this without iovation. There is no way. Running the ISP report and seeing how many accounts are created during a short window of time is key to stopping affiliate fraud. At first we stopped hundreds of dollars a month in affiliate fraud, and now it's thousands. That's very significant," said the Director of Policy Compliance.

Without iovation, it would be nearly impossible to effectively manage fraud risk. Their FraudForce solution has streamlined our process and gives us the tools to shut down fraud rings, and essentially know who to trust online.

Director of Policy Compliance

This social network uses iovation's risk service to place evidence (fraud or abuse reports) against accounts and devices that have abused their service. The most common forms of fraud and abuse placed into the system by the social network includes affiliate fraud, scams and solicitations, spam, harassment, bullying and inappropriate content. When a repeat offender tries to come back to the service, having this device history upfront helps stop the revolving door of abuse, regardless of which fake or stolen identity they attempt to use. By leveraging iovation's global network of device intelligence, the social network will also know if any other iovation clients have had a problem with a device and the type of problem. With more than 5 billion devices, 55 million fraud experiences recorded in iovation's service, and 4,000 global fraud professionals all contributing to and leveraging the service, the network effect is extremely powerful.

Using iovation to know who to trust online

When this social network brings on a new publisher, they monitor for risk very carefully. The legal, new acquisition and fraud teams work together to keep the company free from phony registrations.

—

For more case studies visit **iovation.com/resources**

Get in Touch

Find out more about our authentication and fraud prevention solutions. Contact us for a demo or visit iovation.com

About TransUnion Global Fraud & Identity Solutions

TransUnion is a global information and insights company that makes trust possible in the modern economy. We do this by providing a comprehensive picture of each person so they can be reliably and safely represented in the marketplace. As a result, businesses and consumers can transact with confidence and achieve great things. We call this Information for Good.®

TransUnion Global Fraud & Identity Solutions unite both consumer and device identities to detect threats across markets while ensuring friction-right user experiences. The solutions, all part of the IDVision with iovation suite, fuse traditional data science with machine learning to provide businesses unique insights about consumer transactions, safeguarding tens of millions of transactions each day.

TransUnion
Formerly iovation

Portland Office
555 SW Oak Street, Suite #300
Portland, OR 97204 USA
PH +1 (503) 224 6010
EMAIL info@iovation.com

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

iovation.com