Table of Contents

Overview

Each year, more and more people are turning to the Internet to find romance. At the same time, cyber-criminals continue to seek opportunities to exploit the vulnerability of singles on a global scale. Security is a major challenge for internet dating sites, which can attract scammers, spammers, stalkers and predators, not to mention fraudsters there to mine other members' identities.

For dating sites to succeed, they must maintain a high-quality prospect pool in order to retain their members. And if they do provide a satisfying environment, chances are high that some members will purchase premium services in the future. To keep the quality of their prospect pool high, they must find ways to prevent and detect fraudsters, and block them from future attempts. These unwanted members on dating sites range from misbehaving users to large and organized fraud groups. They spam members, run romance scams to obtain funds from members, phish for identity information, engage in cyberbullying and even predatory behavior.

In order to keep fraudsters out, romance sites must deploy effective solutions that look at information independent of what is supplied by users. A device fingerprinting solution such as iovation Fraud Prevention provides unique insight into the computers being used to create multiple accounts and exposes hidden device-account relationships that identity-based fraud solutions often miss.

Device fingerprinting helps identify the bad guys so online dating sites can eliminate their accounts from the network once and for all. Working in conjunction with existing fraud detection techniques, a device fingerprinting solution provides Internet dating sites with a comprehensive solution for closing the door on repeat offenders. This white paper will help you understand what new and innovative techniques can be used to protect the reputation of your business, keep your members in a safe and trusted environment, while keeping the fraudsters out.

Organized Fraud Targeting Members: Online Dating's Greatest Threat

Online dating sites attracted more than 22 million people looking for love in 2008. According to Forrester Research, that number was a 10% increase over 2007. As more people turn to the Internet to find romance, cyber criminals seek out opportunities to exploit the vulnerability of singles on a global scale.

Today's organized criminals pose a greater threat to online dating sites and their members than ever before. They use the Internet as a conduit for mining, buying and selling people's personal information such as their name, address, social security number and credit card details.

Within online communities, fraudsters work together to perpetrate a number of illegal and abusive activities.These can include financial fraud, romance scams, phishing and email spam, account takeover, chat abuse, cyber bullying and predatory behavior. While online dating sites use various techniques to detect suspicious accounts, Internet-savvy criminals attempt to mask their true identity by changing account information to circumvent conventional methods, such as IP address and geo-location

verification, in-house country block lists, manual photo reviews, profile analysis and other backend administrative tools (see Figure 1).

Separate ID Queries

Registration/Profile Analysis

IP Address / Geo-location Verification

Customized Backend Admin Tools
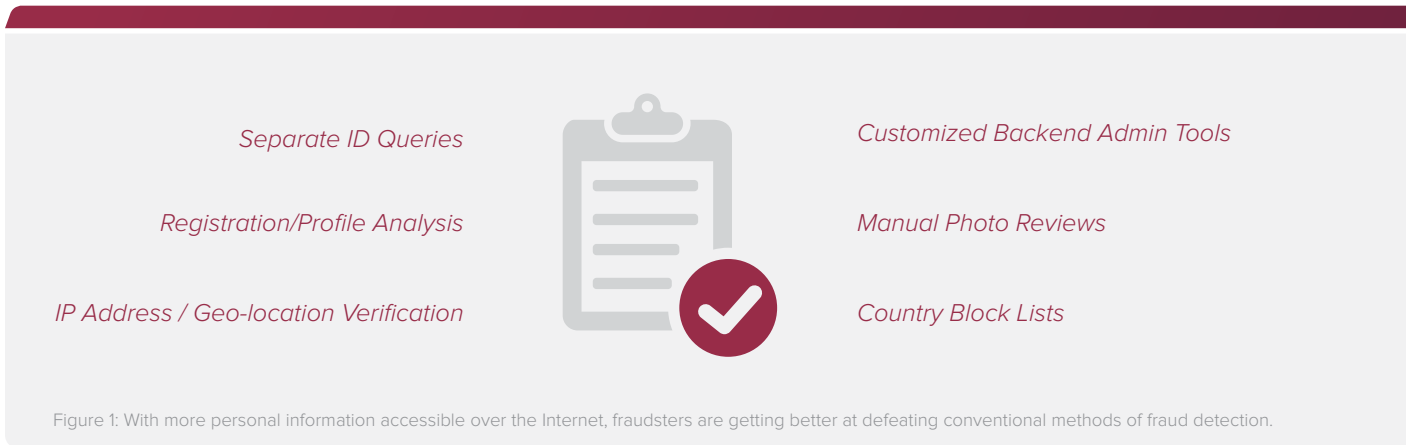
Manual Photo Reviews

Country Block Lists

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

Fraudsters are not necessarily out to defraud online dating businesses. Their goal is to take advantage of the existing platform and scam the members of the community. While the National Consumers League reports the average loss for an online dater is more than $3,000 per scam, Internet dating sites also suffer from a multitude of setbacks including loss of members' trust and satisfaction, tarnished reputation, possible government intervention and ultimately hindered business growth.

Stop The Revolving Door of Repeat Offenders

When it comes to stopping online community fraud and abuse, the biggest challenge is keeping repeat scammers and spammers out of the community. As fraudsters routinely change identities and create multiple accounts, many sites get abused by the same people repeatedly without even knowing it. Fraudsters can literally create hundreds of virtual identities within a single community. For Internet dating providers that lack the ability to detect fraud in the registration process, even if fraud is detected later and a bad account is shut down, there's nothing that prevents a fraudster from immediately creating a new account under another false or stolen identity. This creates a revolving door for repeat fraud and abuse.

As fraudsters take advantage of the Internet's anonymity, identity-based fraud management systems are becoming less effective in catching fraud. In order to keep fraudsters out of the system once and for all, online dating sites must apply more effective solutions that look at information independent of what data is supplied by users. A device fingerprinting solution such as iovation Fraud Prevention provides a unique insight into devices creating online accounts, and exposes fraud that other tools miss. Device fingerprinting helps online dating sites identify bad guys within a network and uncovers hidden associations between their computers and accounts to stop additional fraud, repeat offenders, and fraud rings within a single network and across multiple industries. Working in conjunction with existing fraud detection techniques, a device fingerprinting solution provides online dating sites with a comprehensive solution for fighting the types of fraud and abuse that continue to plague the online dating industry.

The Financial Impact of Fraud

If fraudulent profiles are not identified up front, online dating sites suffer from a multitude of setbacks that significantly impact their bottom line, including:

- **Member Attrition:** Once a good member has been emotionally or financially abused, retaining that customer becomes extremely difficult. This can result in additional customer attrition and revenue loss.

- **Loss of Ad Revenues:** Romance sites that generate monthly revenues from advertisers can lose potential sales opportunities if their online community has a reputation for having excessive spam and online scams reported.

- **Tarnished Reputation:** An online dating provider struggling with high fraud activity can find it difficult to attract new members, retain existing customers, and may even experience more fraud and abuse.

- **Higher Fraud Expenses and Operational Inefficiencies:** Fraud detection tools that cannot effectively identify fraudsters drive up business expenses as more layers of tools are then needed to detect and prevent fraud. Ineffective tools can produce high false-positives driving up personnel costs, as more accounts are required to be manually reviewed.

A Multi-Layered Defense

Online dating providers understand the relative ease with which criminals obtain identity information over the Internet and have responded by being more careful. Ironically, being more careful often means deploying tools that rely on even more personal information, leaving online dating providers and their members more susceptible to fraud and abuse.

In order to effectively combat identity theft, online dating sites must move beyond relying almost solely on personal information for fraud analysis. As identity-based fraud management systems crunch the same identity data in different directions, a totally different technique 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 Fraud Prevention focuses on the user's device (or computer)—not the person—to identify and re-identify the actual computer creating online accounts. A device-centric solution provides unique insight into users creating new online profiles and exposes fraud that is invisible to other tools. Working in concert with other fraud prevention 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 dating providers to instantly identify known fraudulent devices without impacting the user experience or their good customers. The following are things to look for when shopping for a device fingerprinting technology:

1. **Instant Decisioning:** The ability to instantly decision an action real-time with an accept, deny or review response saves significant time and money. You can make real-time decisions when a member creats a profile, logs into his/her account, or goes through checkout.

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 the bad 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 brand new devices, leverages multiple variables to provide the strongest data available to identify devices and their reputations.

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 profiles, a highly scalable solution allows online dating providers to grow their fraud management system according to their business needs.

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-prevention process.

Act with Certainty on Fraudulent Accounts

iovation Fraud Prevention offers a range of integration options including a web device print, download 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 prevention process. (see Figure 2).

Download Device Print / Collects device information through software application

Web Device Print / Captures device information through web browser

Pattern Matching / Looks for patterns in available data

Risk Scoring / Uses all information across subscribers to access risk

Figure 2: iovation's device identification technologies provide multiple ways to identify or re-identify a unique device.

Fraudsters who had a high degree of anonymity in the past are now visible through the uncovered hidden associations between the Internet-enabled device used to open accounts and all of the accounts related to that device. As a result, Internet dating providers can immediately act with certainty on devices by accepting good profiles and blocking bad ones.

Unlocking the Power of Device Identification

While device printing is critical to identifying fraudulent profiles, its effectiveness largely depends on how the data is used. To use device fingerprinting technology effectively in a fraud management system, the solution must go beyond simply recognizing a computer that has visited a single site to being incorporated in a broader system that establishes device reputations for computers across multiple vendors and industries. 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 fake 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 Fraud Prevention draws on the power of its shared Global Device Intelligence Platform, which stores more than 3 billion device reputations and their associations with other computers and accounts across the Internet. Once a unique account identifier and device fingerprint is in iovation's network, fraud teams receive alerts whenever the device returns to their online community, even if the computer's configurations have been changed since its previous visit. This allows subscribers to determine in real-time if they want to accept, deny, or review new and existing accounts for review (see Figure 3).

Collaborating with peers and other industries united against fraud unlocks the power of device identification. Working together in a shared environment enables Internet dating providers to benefit from tens of thousands of additional resources, tools and experiences, without adding to their initial fraud prevention investment.

Expanding Fraud Detection Capabilities

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

Subscriber adds iovation code module to corporate website.

Customer creates an account or makes a purchase at subscriber website.

Subscriber collects device fingerprint from their customer.

Subscriber sends unique account identifier and device fingerprint to iovation.

The device is checked for any history of fraud or abuse on a global fraud database.

Results are returned for real-time automated action or fraud team analysis.

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

- **Software Downloads and Web Technologies:** Software downloads such as ActiveX and Web technologies for cookies, flash-stored objects and java script leverage IP addresses, geo-location and other non-unique identifiers to recognize or re-recognize a device every time it creates an online account.

- **Shared Intelligence:** Sharing fraud intelligence with peers and other industries provides additional resources, tools and experiences that expand an online dating site's ability to identify devices that have previously committed fraud or abuse against other subscribing sites.

- **Forensic Analysis:** When computers creating new profiles don't have a device ID, risk scores and custom reports analyze suspicious activities based on business rules and by identifying the many characteristics of devices that repeatedly demonstrate a high-risk environment.

- **Industry Expertise:** With a breadth and depth of experience fighting fraud in the online dating industry, fraud experts can proactively spot a wide spectrum of fraud trends and assist in the development of more effective fraud management strategies.

The Business Benefits of Device Fingerprinting

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

- **Reducing Losses from Fraud Exposure:** When fraudulent accounts are out of the community, time-consuming and costly procedures to review, analyze and decision accounts are eliminated from the process. This drives down the average cost to decision an account. The ability to pull more bad guys out of the system also eliminates the number of suspicious accounts that are queued for review, allowing online dating providers to reallocate resources and reduce the need for additional headcount.

- **Increasing Process Efficiency:** By reducing time spent analyzing, evaluating, diagnosing and closing potentially good and bad accounts, online dating sites increase the profitability and efficiency of their operational process. Streamlining the fraud prevention process allows romance sites to decision good and bad accounts faster and eliminate unnecessary processing delays.

Conclusion

Technology is dramatically changing the way people look for true love and companionship. But while the Internet makes it easier for people to connect, it also provides the means for more organized cyber criminals to exploit the vulnerability of singles across the globe. As fraudsters get better at defeating more conventional methods of fraud detection, online dating providers must deploy different techniques that work together with existing fraud tools to better identify fraudulent computers creating multiple profiles, which can reduce the rate and impact that romance scams and other social abuses have on Internet dating sites. A device fingerprinting solution such as iovation Fraud Prevention provides romance sites with a number of significant benefits that reduce loss from fraud exposure, increase efficiency within the fraud prevention process, lower false positives, and realize a return on investment that is essential to both the success and growth of their business, and the online dating industry as a whole.