WHITE PAPER

Credit Issuers

Stop Application Fraud at the Source with Device Reputation

iovation®

Table of Contents

Overview

Online credit applicants can fool you with any number of tricks to get their fraudulent or stolen identities approved and confirmed for credit, while leaving you holding the bag for losses. You can spend time, money and duplicative tool verifcations in an attempt to protect your business. But these fraudsters are clever, they will repeatedly hit you for approved applications, and they can disguise themselves in a thousand ways.

Instead of verifying and re-verifying identity information of fraudulent applicants, consider this: Verifying the reputation of the device being used to submit the application. When a fraudster connects to your business, the computer being used can be instantly evaluated for its criminal history.

If you know the device has a history of fraud, the detail of checking identity specifics is supplemental. You don't have to spend time, resources, and money checking identity information - you know the source is suspect and you can block the transaction immediately. Right now. Before you have put your business at risk.

Device fingerprinting coupled with the device's reputation helps identify the bad guys in the acquisition channel, so you don't have to rely on other fraud detection tools that drive up the cost to decision an application. Working in conjunction with existing fraud detection techniques, a device fingerprinting solution gives you a more complete solution for fighting identity theft and other forms of fraud that plague the financial services industry.

In this white paper, we will tell you more. You will understand what new and innovative techniques and solutions can be used to combat fraud, and how you can realize a true return on investment by reducing losses from fraud exposure and increasing operational efficiency within your fraud prevention process.

Why you need more than conventional methods of fraud detection

The Internet has revolutionized the way people apply for credit. Unfortunately, it has done the same for cyber criminals. For example, fraudsters who used to be forced to go to a bank or apply for credit cards in person now can hide behind the Internet's anonymity to apply for credit, with more speed to approval and lower risk of getting caught.

The financial, banking, and credit industries have been proactive in terms of data protection. But they know the times are changing and the antes have been upped. They are responding to the challenge of more personal and financial data being all too accessible over the Internet. They know criminals are now working together to devise more complex schemes to circumvent conventional methods of fraud detection such as credit reports, IP addresses and geo-location validation, home-grown block lists, and out-of-wallet questions. As a result, fraud detection tools that were once your strongest lines of defense against Identity theft are becoming less effective (see Figure 1).

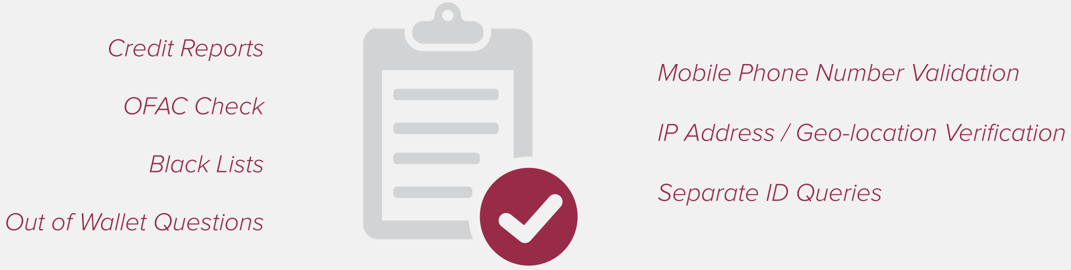


Figure 1: With more personal information accessible over the Internet, fraudsters are getting better at defeating conventional methods of fraud detection.

It is not just credit approval—it is the gateway to more fraud

For fraudsters, credit is not the goal; it is the entry point for all other types of fraud including account takeover, chargebacks and money laundering. If you can't immediately identify fraud in the acquisition channel, you need to deploy highly effective solutions that work in conjunction with existing tools to expand your fraud detection capabilities. A device identification solution such as iovation Fraud Prevention allows you to identify fraudulent applications early in the process, providing a comprehensive and efficient solution for fighting identity theft and other forms of fraud that continue to plague the financial services industry.

Online applications pose a high risk

When it comes to online application fraud, identity theft is the top concern for today's credit issuers. Unfortunately for issuing banks engaged in the daily fight to stop fraudsters from obtaining credit under another person's name, the threat is not going away anytime soon. According to the Federal Trade Commission (FTC), identity theft is growing at a staggering 20% each year, with 50% of customers complaining of fraudulent credit cards being issued in their name. With the Internet acting as a conduit for the buying, selling and trading of people's personal and financial information such as their name, address, social security number and credit card details, online credit applications pose a much higher risk to issuing banks than more traditional channels such as phone or in-person applications.

Today's Internet-savvy criminals are persistent and work extremely fast. Once fraudsters get ahold of a list of stolen IDs they work around the clock to apply for credit with as many online merchants as possible. Even if dozens of their applications are blocked, fraudsters will continue to probe the Internet channel using other fake IDs in an effort to get one through. Once they do, minutes can equate to thousands of dollars lost to fraud. For example, the minute a fraudster is approved for credit he can have an entire credit line of $150 to $2,000 or more spent before the detection process decides he is bad. While a really strict channel may force a fraudster to go somewhere else, they always circle back and ping the channel. At that point, if the credit issuer has lowered its fraud threshold, it will open up again, and the issuing bank will find itself right back where it started.

The financial impact of fraud

If fraud is not identified early in the application process, credit issuers can suffer from a multitude of other financial setbacks and legal penalties that can significantly impact their bottom line. The following are ways credit issuing banks can be hit by fraud beyond the initial credit line:

- **Costly Fraud Tools and Identity Checks**: Running additional costly and time-consuming fraud tools and validation checks can significantly drive up the average cost to decision an application.
- **Increasing Overhead and Process Inefficiencies**: More applications queued for review creates huge inefficiencies and often require additional personnel to handle calls, manage records and analyze applications.
- **Fraudsters Exploiting Higher Credit Lines First**: If a fraudster is approved for credit lines of $200 and $2,000 he'll drain the larger account first to get away with the most cash possible in case the accounts are blocked.
- **Inflating Credit Lines**: When fraudsters expand credit lines by phone and other tactics such as check kiting it increases the amount an issuing bank is liable for.
- **Closing a Channel**: Closing an entire channel because fraud rates are too high results in significant revenue loss due to lost business opportunities.
- **Impact on User's Application Experience**: More controls and checks create a larger barrier to entry and diminish the user experience.

- **Sharing Fraud Penalties**: In profit-sharing agreements, an issuing bank and merchant agree to share fraud penalties. If fraud rises above a certain level, credit issuers can experience higher fraud losses.
- **Federal Regulations and Other Legal Issues**: Not meeting regulations related to identity theft, Red Flags laws, consumer protection and credit acts can result in higher expenses and losses for credit issuers.
- **Tarnished Corporate Reputation**: A credit issuer struggling with high fraud rates can find it difficult to earn new business with retailers, renew contracts with existing partners, and may experience more fraud.

Device reputation is key to your multi-layered defense

Credit issuers understand the relative ease with which criminals obtain identity information and have responded by being more careful. Ironically, being more careful often means deploying tools that rely on even more personal information, leaving issuing banks more susceptible to identity theft. As a result, identity-based fraud management systems have reached their limit to effectively fight online fraud. As more organized fraudsters share personal information to create multiple identities and defraud credit issuers, identity and financially based fraud detection tools can no longer guarantee the true identity of a user through the name, address, geography, or credit card details.

There is a growing recognition that in order to effectively combat identity theft, credit issuers must move beyond relying almost solely on the personal or financial 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 and device reputation solution such as iovation Fraud Prevention focuses on the user's devices – not the person – to identify and re-identify the actual computer applying for credit online. A device-centric solution provides credit issuers with a unique insight into online applications and exposes fraud that is invisible to other tools. Working in concert with other fraud 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 identity theft.

Eight “must-haves” for a device fingerprinting solution

To effectively combat online application fraud, a device fingerprinting solution must have several key components that allow credit issuers to instantly identify and decision an application without impacting the user experience. The following are things to look for when shopping for a device fingerprinting technology:

1. **Instant Decisioning**: The ability to instantly decision an application with an accept, deny or review response, the moment it is submitted online, can save credit issuers significant time and money. Operational efficiencies are gained in avoiding reviewing good applications and losses are reduced by not processing known bad ones.

2. **Transparency**: A fraud tool that accepts good applications and declines bad ones with complete transparency increases customer satisfaction and provides a level of convenience and security that all credit issuers strive for.

3. **Low False Positives**: False identification of fraudulent devices can undermine fraud prevention tools. You can end up turning away good customers and increasing operational costs with time-consuming reviews.

4. **Flexibility**: A solution that offers flexible implementation options such as a web print, software download, and risk score leverages multiple variables to provide the strongest data available to identify a device applying for credit.

5. **Pattern Matching**: Pattern matching analyzes individual non-unique identifiers to expose unusual activity and anomalies 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 and doesn’t require any personally identifiable information (PII) provides a unique insight into computers applying for credit online and exposes fraud that identity-based tools miss.

7. **Scalability**: As fraud detection processes struggle to keep up with increasing online credit applications, a highly scalable solution allows credit issuers to grow their fraud management system according to their business needs.

8. **Cost and Effectiveness**: A highly effective fraud tool that is cost-effective to run provides a real return on investment (ROI) through fraud reduction and improved operational efficiency within the fraud detection process.

Act with certainty on fraudulent applications

iovation Fraud Prevention 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 device fingerprinting technologies provide a multi-layered approach to fighting identity theft while mitigating both false positives and false negatives in the fraud 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 once had a high degree of anonymity in the past are now visible through device recognition. As a result, credit issuers can immediately act with certainty on devices by accepting good customers and blocking bad applications in the acquisition channel.

Unlocking the power of device identification

While device printing is critical to identifying fraudulent applications, 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 apply for multiple credit cards 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 a billion unique 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, credit issuers receive alerts whenever the device returns to apply for credit online, 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, decline, or queue an online application 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 credit issuers to benefit from tens of thousands of additional resources, tools and experiences, without adding to their initial fraud detection investment.

Strength in numbers

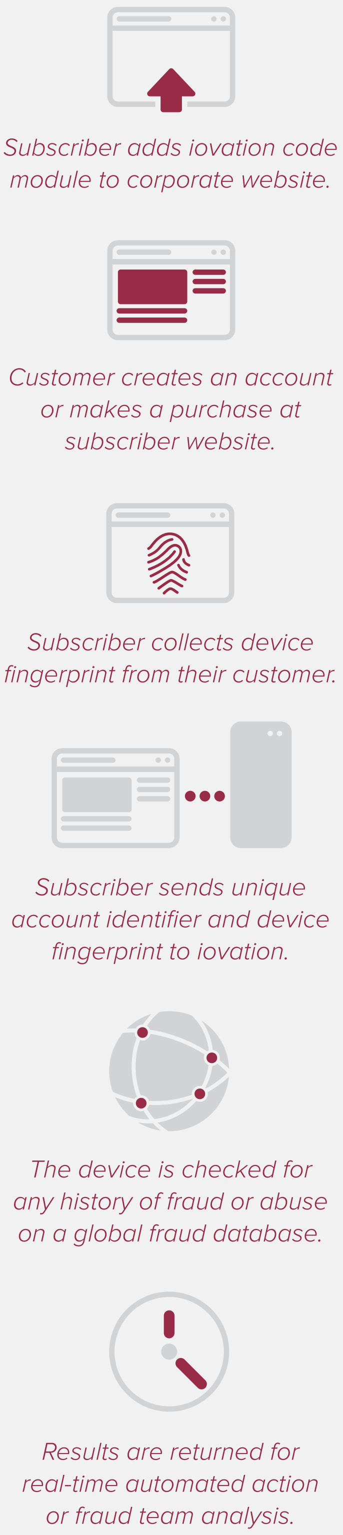
Combining innovative device fingerprinting technologies with a shared network of device intelligence allows credit issuers to expand their existing fraud detection capabilities with the following components:

- **Software Downloads and Web Technologies**: Software downloads such as ActiveX and Web technologies for cookies, flash-stored objects and java script leverage IP addresses, geo-location and other non-unique identifiers to recognize or re-recognize a device every time it applies for credit online.
- **Shared Intelligence**: Sharing fraud intelligence with peers and other industries provides additional resources, tools and experiences that expand a credit issuer's ability to identify devices that have previously committed fraud or abuse against other subscribing sites.
- **Forensic Analysis**: When computers applying for credit don't have a device ID, risk scores and custom reports analyze suspicious activities based on business rules and identify 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 financial services industry, fraud experts can proactively spot a wide spectrum of fraud trends and assist in the development of more effective fraud management strategies.

Business benefits of device fingerprinting

A device fingerprinting solution that enables credit issuers to instantly decision an online application provides a number of significant benefits, including:

- **Reducing Losses From Fraud Exposure**: When fraudulent applications are blocked early in the process, costly detection tools and procedures to validate the personal or financial information are eliminated from the fraud detection process. This drives down the average cost to decision an application. Pulling more bad guys out of the stream up front also eliminates the number of suspicious applications that are queued for review, allowing credit issuers to reallocate resources and reduce the need for additional headcount.



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.

- **Increasing Process Efficiency**: By reducing time spent analyzing, evaluating, diagnosing and closing potentially good and bad applications, credit issuers increase the profitability and efficiency of their fraud detection process. Streamlining the decisioning process allows issuing banks to accept good business faster, eliminate processing delays, and improve overall customer satisfaction.
- **Fewer False Positives**: Low false positive rates enable credit issuers to block bad applications without turning down good customers. Once confidence in device identification is established, accepting legitimate business up front reduces the number of reviews, lowers the cost to decision an application, and improves the overall efficiency of the fraud process. iovation's device fingerprinting technology has been highly effective in mitigating false positives. For one Fortune 100 financial services issuer that received more than 3.2 million online applications over the course of a single year, iovation Fraud Prevention had a false positive rate of .000284%. "The tool is extremely effective in carving out frauds from the goods," said a representative from the financial institution. "It has proven to be one of the best false positive rates of any fraud acquisition tool we've seen."
- **Proven ROI** : A published Forrester Total Economic Impact™ study found that a Fortune 100 financial services credit issuer using iovation Fraud Prevention achieved a 321% ROI over a two-year period, saving the customer $8 million through reduced fraud losses and improved operational efficiency (Figure 4).

Forrester Reports 321% ROI

- Identified over 43,000 fraudulent applications in the 1st year.
- Improved operational efficiency within their fraud detection process.
- Experienced a breakeven payback within 6 months.
- For every dollar spent on iovation, customer saved more than $7.

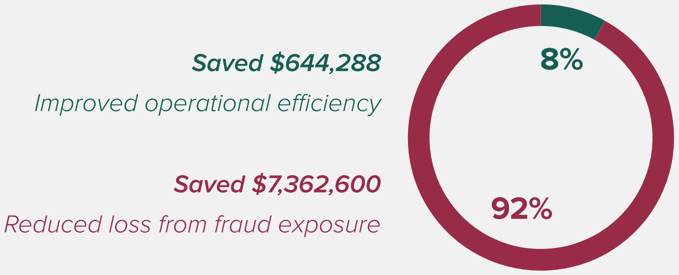


Figure 4: iovation helped a financial services issuer reduce significant fraud loss and improve overall efficiency. For every dollar spent with iovation, the customer saved more than $7.

Conclusion

Technology is fueling the growth of the credit card industry like never before. Unfortunately, while the Internet makes it faster and easier for individuals to apply for credit, online applications pose a higher risk for credit issuing banks. As more organized cyber criminals get better at defeating conventional methods of fraud detection, credit card issuers must deploy different techniques that work together with existing fraud tools to detect bad applications early in the process and reduce the rate and impact of identity theft. A device fingerprinting solution such as iovation Fraud Prevention provides credit issuers with a number of significant benefits that reduce loss from fraud exposure, increase efficiency within the fraud detection process, lower false positives, and realize a return on investment that is essential to both the success and growth of their business, and the credit card industry as a whole.

To begin making real-time decisions on your
online credit applications, please call (503) 224.6010
or email info@iovation.com.

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, device-based 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 billions of 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 15 million transactions and stop an average of 250,000 fraudulent activities every day. The world's foremost fraud experts share intelligence, cybercrime tips and online fraud prevention techniques in iovation's Fraud Force Community, an exclusive virtual crime-fighting network. For more information, visit www.iovation.com.

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