WHITE PAPER

Fighting Banking Fraud Without Driving Away Customers

Effective Methods for Targeting Cybercrime in Financial Services

iovation®

Table of Contents

Nowadays the ability to stop fraud is only half the story.

Risk mitigation and fraud prevention efforts must also support a financial institution's strategic goals of increasing customer satisfaction and contributing additional revenue—all while protecting customers and the organization's reputation.

Fraud prevention services must provide a unified approach across all lines of business including retail, card and commercial, while simultaneously preserving the customer experience and improving profitability. As it relates to the online channel, financial institutions need customer-friendly technology that provides protection for their online portals at login, as well as account and transaction creation associated with the entire suite of products and services that they offer.

Perhaps no single threat jeopardizes banking relationships with their customers more than account takeover and the subsequent fraudulent transactions and identity theft that accompanies it. Having the ability to identify suspicious logins and prevent high-risk transactions helps protect customers and their accounts before losses occur. Preventing unauthorized account access also helps keep personal data safe from being used to create synthetic accounts and ensures funds are delivered where and when they were intended. Because of the severity of these types of incidents, banks are placing an emphasis on prevention as opposed to after-the-fact detection. Doing so can help banks prevent customer defections, lengthy investigations and efforts to recover funds that often prove futile.

In today's online banking environment, rarely does an account compromise affect a single banking account. Customers often have multiple accounts that can cross business units or brands, and a breach or loss of trust has consequences that extend well beyond a single business unit. If the customer discovers the incident rather than the bank, there is a multiplier effect on losses as the bank is in a reactive as opposed to a proactive role. A unified prevention strategy that protects customers across all of their accounts will deliver immediate and long-term value.

This white paper presents how iovation's advanced device identification and reputation services strengthen current online fraud controls while simultaneously improving the customer experience and increasing revenue. iovation offers a service that reduces fraud, improves customer satisfaction with online banking, and delivers an impressive return on investment.

STOPPING FRAUD:
One Goal Among Many

Banking customers demand solid security, and simultaneously expect it to be relatively unobtrusive. With too many hurdles in place, customers may be become frustrated. Unfortunately, business goals can often diverge significantly from fraud management goals. Business teams pursue seamless interactions with trusted customers, and security teams look to apply the right tools at the right time to stop fraud and account takeover while granting legitimate customers access.

Excessive friction between bank technology and legitimate customers leads to lower levels of satisfaction, higher rates of attrition, and abandonment of optional security measures. Fraud prevention technologies must be capable of reducing fraud without simultaneously causing customer attrition or decrease in the use of cost effective delivery channels such as online banking.

Ultimately, fraud prevention technology must encompass an enterprise wide view of fraud. Banks today often utilize fundamentally similar tools from multiple providers. For example, a bank may use credit data from numerous sources, to contribute to their decision-making tools and processes. Banks are now moving to consolidate the use of such tools across business groups including credit cards, retail and commercial. This initiative reduces costs, optimizes fraud prevention effectiveness, and delivers a consistent customer experience across all channels, lines of business and products. The move to consolidate tools places a premium on technology that is flexible enough to adapt to the unique challenges inherent in monitoring a broad range of banking products and services as well as incorporate existing technology solutions and platforms.

Moving Toward a Unified, Secure Customer Experience

Banks often employ inconsistent fraud risk management strategies specific to each line of business, which in turn confuses customers since they view the bank as a single entity. The resulting disconnect causes variations in the customer experience, which often translates in to poor customer service that directly affects the bank's relationship with the client as a whole.

So why do variances persist? Differences in fraud strategies create inconsistent risk tolerances. This often produces a slowdown in the adoption of new fraud prevention technology as representatives from the line of business and bank operations attempt to reach a compromise regarding the level of risk that the bank is willing to assume.

On top of this, individual tools implemented in response to a real or imagined threat, or recent loss do not facilitate cross business unit alignment as they have limited application beyond the products or services that they police within that line of business. Rarely is there the opportunity to deploy the same technology throughout the enterprise so that there is consistent customer experience and and level of protection across all lines of service.

As a risk mitigation and information-sharing tool iovation's data platform and community of fraud investigators located around the globe provide banks with consistent, actionable intelligence across all of their business units. The strategies embedded in iovation's Fraud Prevention solution allow

banks to connect the dots between individual customer interactions across multiple business units. Ultimately, this approach provides an enterprise wide view of legitimate customer interactions, potential fraudsters, the accounts that may be at risk and the associated devices.

There are many teams within a financial institution that can benefit from collaboration and a unified view of online interactions, including fraud countermeasures, fraud operations, customer service, customer experience, mobile banking, and marketing. The following section of this paper examines typical organizational roles that interact with fraud and the various benefits these teams receive by using iovation Fraud Prevention.

- **Fraud Countermeasures:** This team typically determines fraud rule deployment within, and across channels. Countermeasures typically play a role in defining fraud priorities and goals as well as the type of fraud technologies to implement. The business rules defined and set within the iovation system are a direct reflection of Countermeasures' approach to detection and prevention of fraud and abuse.

- **Fraud Operations:** Based on their experience reviewing fraud suspects, the operations team helps amend and adapt iovation's Fraud Prevention solution's effectiveness through changes made via the Business Rules Editor. Each customer touch point (payment, application, login, account change, etc.) has its own unique set of business rules, scores and thresholds. This team is also responsible for implementing and providing feedback to iovation Fraud Prevention regarding the tracking of individual instances of fraud or other types of abuse.

- **Online Customer Service:** This team answers customer questions, helps with account reset/change, and helps customers navigate the financial institution's extensive list of online services. Service reps have access to the iovation score and transaction details to help make decisions in real-time.

- **Customer Experience:** A customer experience team member measures customer satisfaction via surveys and tools such as the Net Promoter Score, and monitors cost and operating expenses associated with customer service calls. They track the linkage between satisfaction and attrition rates and corresponding technology.

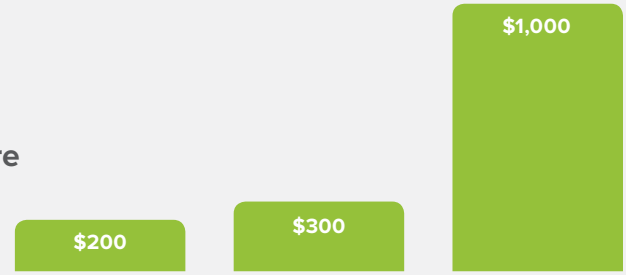
- **Online Marketing:** This group looks for opportunities to drive incremental revenue, often through better targeting based on activity across channels. This team introduces new site services and functionality and correlates accounts and activity between business lines. iovation helps by associating accounts with devices (such as computers, tablets and mobile phones) used to access them, tying accounts not previously known to be related, and providing additional insight for targeted marketing.

- **Compliance:** This team ensures the bank is meeting its regulatory obligations and maintaining a positive reputation with regulators. The compliance team verifies that tools address regulations and meet compliance objectives. iovation directly addresses FFIEC, by ensuring transactions are assessed for risk and scored, and by exceeding complex device identification requirements. iovation also identifies and prevents fraud and flags risky transactions in response to suspicious activity.

- **Corporate Security:** A member of Corporate Security interacts with law enforcement and government agencies in the event of crime or serious fraud. This team is provided investigative detail on transactions and associations by iovation to help drive cases to conclusion. Many times the associations of accounts and devices provided by iovation expands the scope of an investigation and highlights associated activity that might have otherwise been missed.
- **Mobile Banking:** This team designs the customer experience via the mobile channel, and determines the features available via browsers and apps. As the use of mobile expands, access to higher risk functionality is being offered. iovation supports both mobile web and mobile app delivery, and provides the same depth of fraud detection in this fast-advancing channel as in traditional online channels. A specialized SDK for app development provides some of the strongest device identification available for the protection of mobile transactions.

400%

increase in Android malware since summer of 2010.[1]



The average fraud amount was $200 on debit cards, over $300 on credit cards used by the consumer and much higher (over $1,000) for commercial accounts.[2]

ONLINE RETAIL BANKING:

A Focus on Customer Satisfaction

Today, iovation protects key points of entry within online banking such as new account opening, logins, remote deposit capture and high-risk transactions including the initiation of wires, ACHs and online bill pay. iovation's ability to protect multiple accounts held by the same customer pays significant dividends. Previously, if one account was compromised, all accounts were at risk.

Consider the following areas within online retail banking where iovation can help:

- **New Account Opening:** When iovation detects risk or a history of fraud, account creation can be immediately put on hold or denied, requiring the customer to contact Customer Support before establishing the account. In addition to stopping fraudulent account creation, iovation avoids false positives that can severely impact back office efficiency.

- **Suspicious Online Login:** Logins include account access and password verification pages. In best practice implementations, if iovation flags the login as high risk the transaction can be referred to stronger authentication technology such as Knowledge Based Authentication (KBA). If the customer answers the KBA questions correctly they are considered to be authenticated and online activity will proceed. The benefit of this approach is that it fights fraud while enhancing the customer experience by only requiring additional authentication when necessary.

- **Remote Deposit Capture:** Remote deposit capture allows customers to photograph or scan a check for immediate deposit into their account. Allowing such types of deposits is a tremendous convenience for the customer and offers potential cost savings to the bank. In order to balance the risk of these transactions, in the event that iovation flags a deposit as high risk, the transaction can be referred to a fraud monitoring team and directed through an automated KBA gate. If the customer answers the KBA questions correctly they are considered to be authenticated and the deposit will proceed.

iovation limits potential losses as it provides real time intelligence that allows the bank to protect a customer's entire relationship, at a faster rate than cybercriminals can exploit the data for their own benefit.

CREDIT CARDS:
Higher Costs and Less Chance of Recovery

Because losses on credit cards are materially higher than online banking losses, and the odds of recovering card-related funds are not in the banks favor, proactive fraud prevention as opposed to fraud detection becomes even more critical. Interestingly, while a higher incidence of fraud occurs at card registration and transaction, the highest financial losses occur at card acquisition. When a fraudster successfully registers a card, they can steal a higher dollar amount in a single transaction or several smaller transactions.

For bank-branded and private label cards, iovation Fraud Prevention is used at card acquisition, registration and online card account management. We cover interactions with new customers and existing customers alike.

CUSTOMER TYPE	CARD ACCOUNT STAGE	IOVATION ROLE
New Customer	Online Card Acquisition[5] (new card application)	Detects attack due to triggers such as high velocity behavior from the device, from sophistsicated and automated scripts.
Existing Customer	Online Registration[6] (post acquisition)	Negative authentication. A known bad device is identified by the bank and validated using iovation.
Existing Customer	Login to Card Account Management (post registration)	Negative authentication. A known bad device is identified by the bank and validated using iovation.

iovation automates the identification of accounts needing review through its real time Fraud Prevention solution. Suspect transactions are proactively flagged much earlier in the process than in the corresponding manual review. This allows the bank to stop problems before they occur, saving time, money and meanwhile protecting its reputation. In one case prior to implementing iovation, a fraud operations team had to wait until the next business day to get device-based risk information, at which point they missed the opportunity for a real-time review. Today that insight is in the fraud team's hands within seconds.

iovation's proactive solution keeps the bank in front of the fraud, rather than being alerted after the fact. This also promotes rapid resolution of questions to ensure that good customers can quickly proceed online to their accounts.

[3] Nilson Report: US Leads World in Credit Card Fraud, Nov 2011.

[4] Nilson Report, June 2010.

The Impact of iovation within Credit Card Operations

	BEFORE IOVATION	WITH IOVATION
1.	Fraud was identified manually by operations, at $6 per review.	Accounts are automatically flagged for review – eliminating the cost.
2.	Contact customer via phone, clean up profile, reset username and password. $3 per call, up to 30 minutes.	Review queues decreased since the bank could recognize known good accounts. Higher accuracy targeting the accounts that are truly at risk.

In 2011[3], Payment card fraud losses totaled

$3.5 BILLION

At the current growth rate, by 2015[4] card fraud is estimated to reach

$10 BILLION

Commercial Banking

Commercial accounts have much higher exposure to fraud as the account value and transaction amounts are significantly higher than retail or card accounts. They are also used for high-risk transactions like wire transfers. This makes commercial accounts almost irresistible targets for theft and account takeover. The dollar losses to the bank are typically limited because the business, rather than the bank, is responsible for losses, but the reputational risk can be high as legal action by commercial customers is becoming common in these cases.

Often the bank will require multiple layers of security including passwords, out-of-band (OOB) authentication, use of apps, and even physical tokens. Commercial customers know these approaches provide higher security but some may still choose not to adopt some or all of these measures. In cases like these, iovation provides an additional layer of defense. iovation Fraud Prevention identifies repeat offenders and those working in collaboration to attack commercial accounts. It can also be used to identify those individuals that have a history of fraud in the retail or cards channels or in other industry verticals—who are now working their way into commercial banking.

An Illustrative ROI Formula for Risk Solutions

Measuring the ROI of a fraud tool used to be more art than science. While previously viewed purely on cost, fraud tools are now evaluated based on their ROI. Let's take a look at an example of how the ROI of iovation's service can be modeled. The model presented is an abstracted, generalized model based on an actual customer model, and includes estimated values. Your model may differ.

A simple ROI model is proposed

ROI =

$$\frac{\text{Fraud Savings - Operational Expense}}{\text{Cost of Fraud Tool}}$$

To illustrate, we assume there are 10,000 transactions per day being evaluated for fraud. Of those, 3%, (300) are flagged for review and 2% (6) flagged for review are actually 'bad'. Each review costs the bank $5 in operating expense, and the average loss of a fraudulent event is $1,000. The $1,000 is comprised of lost funds, cross- account impact, attrition of both directly and indirectly affected customers, and reputational damage. We also assume that a new fraud tool, such as iovation, is able to stop an incremental 50% of new fraud events.

The fraud tool cost is $10,000 per month, or $333 per day.

RETAIL ACCOUNTS

$$\frac{\$3{,}000 - \$1{,}500}{\$333}$$

ROI = 4.5X

In the case of wire fraud, where losses are significantly higher, the ROI gets above 13X. Wire fraud losses can be $3,000-$4,000 or more. Using $3,000 as the loss amount; and 2 instances/month ($6,000).

WIRE FRAUD

$$\frac{\$6{,}000 - \$1{,}500}{\$333}$$

ROI = 13.5X

Now, we look at how the ROI can be further improved by iovation. ROI increases can be the result of higher fraud savings as shown above, or by reducing operational expense.

OpEx REDUCTION
$\frac{\$3{,}000 - \$1{,}000}{\$333}$
ROI = 6X

iovation delivers ROI improvements by reducing OpEx through the reduction in manual reviews, increases fraud loss savings, and drives incremental revenue by providing marketing teams better visibility to customer crossover. Altogether, this improves the ROI calculation and value to the bank.

Finally, one of the costs of fraud not shown here are the losses at one institution that carry over to another as fraudsters recycle the account holders' information. This "re-use" fraud relies upon the same computer used to defraud the original bank. Cross-bank loss prevention is difficult to assign a value to, but iovation's unique ability to identify a common element - the device used to attempt or commit fraud - only enhances the ROI of our solution.

Tools in the Banking Ecosystem

Banking risk management systems are complex, utilizing various tools employing varying levels of integration. Fraud management platforms can include behavioral monitoring, risk profiling, credit analysis and device reputation to achieve a comprehensive defense in depth approach. iovation complements many fraud prevention tools in the following ways:

- **Clickstream navigation and behavioral tracking** systems flag anomalies that vary from common patterns. These systems support FFIEC and provide a unique perspective on fraud. However, they require time to learn about the 'normal' behavior of each customer, and of usage patterns in general. iovation provides additional coverage that is independent of customer profiling and can provide additional coverage from day one.
- **Risk Based Authentication (RBA) systems** are used to authenticate users appropriately at specific customer touch points. They are implemented when the risk of the transaction is recognized to be high. iovation is proactive, able to consider the risk of the current transaction(s), but also consider past behavior as a contributor to risk. This capability can be utilized to more selectively employ RBA as well as identify other potentially risky transactions where RBA is of additional value.
- **Fraud Management Platforms** have their own rules engines and incorporate multiple data sources to support workflow and analytics. iovation adds proactive decision making into the fraud management process. This allows fraud analysts to focus on transactions that exhibit the greatest risk to the bank.

- **Transactional Risk Models** build profiles of 'expected' and 'unusual' transactions. The challenge with these models is the time it takes to establish a baseline of normal activity, especially for new customers. iovation can provide coverage of accounts that appear new through their past associations with other devices and accounts.
- **Credit bureaus** offer a credit score used in determining credit thresholds. These are highly valued and frequently used, however they are dependent on the quality of the PII (personally identifiable information) used to identify the individual. iovation is an excellent complement to credit scoring by adding customer insight from the device perspective completely independent of the PII presented during account creation.

Conclusion

Banks recognize the importance of balancing effective, proactive security with a consistent customer experience. Today, leading banks are choosing highly complementary solutions such as iovation Fraud Prevention that reduce cost, lessen the burden on customer through the avoidance of unnecessary technology checks and processes, and increasingly support the pursuit of incremental revenue.

iovation is in use today by many of the world's leading banks and credit issuers because it delivers what a traditional security solution delivers, plus provides valuable insight that can be utilized across business units. iovation increases customer satisfaction, reduces risk and contributes to the bottom line.

Please contact us to learn more about online fraud protection by emailing info@iovation.com or calling (503) 224-6010.

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