



CASE STUDY

# TOP 10 BANK CUTS FRAUD LOSS FROM ONLINE ACCOUNT APPLICATIONS

## CHALLENGES

The bank's legacy account application process was frustrating its customers, which slowed the account booking rate and impacted profits. Plus, the bank had not fully trusted mobile device movement.



## SOLUTIONS

Device reputation scoring was implemented at the very beginning of the account application process, which offered the best opportunity to reduce customer friction.



## RESULTS

The bank saw a significant reduction in fraud loss, and more than doubled account bookings while reducing customer friction by more than 50%.



## NEW APPLICATION PROCESS IMPROVES CUSTOMER EXPERIENCE AND ACCOUNT BOOKINGS.

The exploding use of mobile devices by consumers sent a clear message to the bank in 2012: 'If we're going to remain competitive, we have to meet our customers online and on their mobile devices.' With a deep heritage rooted in face-to-face banking, the prospect of entering the digital arena was both exciting and intimidating.

"The prevalent thinking was that fraudsters are lurking online, and good customers would only want to open an account in person," recalls 'Jen,' a Vice President at the bank. "I knew this wasn't the case. Our customers are busier than ever. When they want to open a new account, they want to do so in the moment."



## INCORPORATING DEVICE REPUTATION RIGHT UP FRONT AS THE FIRST LINE OF DEFENSE REALLY MADE A DIFFERENCE.

Jen, VP of Fraud

Every application from a website or mobile device went through manual review which caused frustrating delays for customers and increased overall costs for application review. Serving the wave of new account applicants expected from online and mobile sources meant that something would have to change.

### The Objective: Reduce costs and customer friction

As one of the 10 largest financial institutions in the United States, this bank has thousands of physical branches across the country. Jen's team seeks ways to optimize new account application processing and fulfillment: "We focus on mobile and Internet applications, but we do take the branch channel into consideration, as that is our heritage. We see the mobile and Internet spaces as incubators for new products and services that we might introduce to our branches later."

To book more accounts online, the bank needed to streamline the application process while containing costs and keeping

out fraudsters. “We understood that it was paramount to give our customers a frictionless process. Along with that, we wanted to minimize our costs, increase fraud prevention, handle increasing regulation, and streamline our back-office workload.”

After a thorough review of the available solutions, the bank chose iovation’s risk service. “iovation’s technology and business ethos aligned best with our needs and culture,” says Jen. “At the time, it made the most sense. It still does today.”

### Early implementation brings immediate results

After choosing iovation’s device reputation solution, the bank identified the front end of the application process as the greatest opportunity to reduce friction. In doing so, they hoped to curb costs associated with their compliance, fraud and risk departments, and weed out the worst fraudsters. “In the first week that we implemented iovation, we audited the reports every night. We saw applications from places we’d never expected, like Nigeria and Russia,” Jen recalls. “This is common now, but back then we were shocked. We had no indication these ‘applicants’ were making it through the door.”

### Manual review queue cut in half

Every time a device submits a new account application to the bank, iovation evaluates that device’s reputation and riskiness, and makes a configurable recommendation. Unrecognized devices are assessed for patterns iovation associates with fraud.

iovation’s recommendation is determined by business rules selected and weighted according to the bank’s needs and appetite for risk. These rules represent the specific traits and behaviors the bank wants to respond to immediately. Applications from devices deemed as trustworthy continue through the real-time process. High-risk devices may be denied instantly. The rest get flagged for manual review.

The decision engine Jen and her team implemented brought striking improvements. Using iovation as a first-stage filter, applicants’ devices that exhibited extremely suspicious traits or behaviors were declined automatically. The applications that didn’t trigger enough rules to raise suspicion continued through the real-time application process.

“When an application goes into review, one of our back-office bankers will reach out to the applicant,” Jen explains. “In those cases, many good applicants will abandon the process voluntarily, after having expected a real-time decision.



## IOVATION HELPED US ELIMINATE THE WORST OF THE WORST, SERVE HONEST CUSTOMERS FASTER, AND REDUCE THE NUMBER OF QUESTIONABLE APPLICATIONS SENT TO REVIEW

Jen, VP of Fraud

### iovation reliably predicts losses

After processing tens of thousands of applications, the bank has concluded that their implementation of iovation enables them to accurately predict if an application will be problematic. If iovation indicates high risk, the application is more likely to be declined for other reasons, such as high risk or compliance issues.

“It’s really significant that device reputation is a predictor of future problems in our applications,” Jen says. “This conclusion has led us to a natural question: ‘Why spend money to have applications manually reviewed when most of them are either withdrawn under further scrutiny, or they could potentially be declined?’ Thanks to iovation, we now have an opportunity to hone our process and further reduce potentially bad applications going to review.”

### Results exceed expectations

When the bank began planning to implement iovation, it had three primary goals: improve the experience of customers submitting applications online or via a mobile device, increase the number of account bookings overall, and keep fraud rates steady.

“With iovation’s help, we reduced customers’ friction in the application process by half. Right now, most of our applicants receive a real-time decision,” Jen says. “As we fine tune our process, we expect to put more reliance on iovation and reduce our review queue even more. In the same time period, account bookings improved two-fold over the original process. Because iovation helps reduction friction, more customers can confidently be approved in real-time. That’s huge.”

“Finally, our biggest revelation had to do with our losses. They went down dramatically. Now our risk folks are asking ‘Why don’t you do more with iovation by expanding it to additional services and products?’ Who hears that from those folks? It’s wonderful.”

## 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, customer 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 more than 3 billion 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 16 million transactions and stop an average of 300,000 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.

### 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](mailto:info@iovation.com)

### United Kingdom

PH +44 (0) 800 058 8731  
EMAIL [uk@iovation.com](mailto:uk@iovation.com)

[www.iovation.com](http://www.iovation.com)

