August 5, 2011

Case Study: Online Retailer Uses New Fraud Detection Systems To Cut Fraud Loss Rates

by Andras Cser
with Stephanie Balaouras and Lindsey Coit

EXECUTIVE SUMMARY

A North American online retailer found that fraud losses ate at profits and affected the customer experience. The retailer's manual fraud management processes could not scale with the volume of its online and phone-based sales. As a result, fraud professionals at the company decided to implement a new fraud management solution. Unfortunately, the first solution didn't have a decision engine to create more-advanced fraud detection rules to fight increasingly sophisticated fraud techniques. The retailer implemented a different solution that allowed them to create advanced fraud detection rules and increase efficiency of fraud management functions within the department to review more orders faster. The team was also able to absorb additional fraud-related functions (chargebacks and collections) that other departments previously handled, without increasing staff. Managers could track overall performance with online reports, which allowed analysts to work from home. The advanced rules, increased efficiency, robust user interface, and analyst motivation resulted in a large reduction in fraud rates.

SITUATION: LIMITED AND MANUAL FRAUD MANAGEMENT HAMPERS GROWTH OF BUSINESS

This large North American retailer sells items through its website and over the phone. To help improve its fraud management capabilities, the company implemented a hosted fraud management solution in 2001. The company set up about 25 fraud detection rules. This helped automate some aspects of fraud prevention by flagging suspect orders and placing them on hold for fraud review; however, many fraud orders were bypassing the rules because they received low fraud scores and were automatically approved. The fraud rule engine lacked features to write more versatile rules that could consider more order fields. Without this additional intelligence, it was difficult to flag more suspect orders for review.

Over the years, the company gradually decreased its fraud rate using this solution, but the team was still overwhelmed with the manual effort that was needed to identify and cancel fraud. The team was canceling more than $100,000 a month in approved orders that were actually fraudulent. The company had to create reports to review approved orders because so many orders bypassed the fraud rules. The sooner the approved fraud orders could be identified, the better chance the retailer had to cancel the order before its warehouse shipped the product. There was no user interface for the reviews or a case management system, so the retailer had to develop these components internally. As part of the review, the analysts had to painstakingly gather data from eight different internal and external systems to ensure that they had the full picture of the order. Only then could they determine if the order was fraudulent or legitimate. The process was inconsistent and error-prone.

BEST PRACTICE: SELECT A SOLUTION WITH VERSATILE RULES AND REVIEW USER INTERFACE

The online retailer decided that it had to switch solutions. In preparation for the new vendor selection process, the company reexamined its drivers and determined that the ability to configure versatile rules was a top requirement. They also needed a fraud case review interface that offered a single-screen approach for fraud analysts to review all order information. And to keep up with constantly changing fraud techniques, the company wanted the ability to integrate the solution with third-party intelligence sources. More specifically, it looked for the ability to:

- **Add flexible rules quickly to combat new fraud types.** Fraudsters aim to stay one step ahead of fraud analysts by constantly evolving their techniques. The ability for fraud managers to add rules quickly on their own to combat fraud on a timely basis was a primary requirement for the company. For example, the company learned that many fraudsters use the same "tumble" in email addresses: The same fraudster probably created freetorhyme3422@yahoo.com and freetorhyme5834@yahoo.com. To recognize this pattern, the solution had to be capable of discarding any numbers at the end of an email user name and compare the remaining part with known fraudulent addresses. Further anomalies, such as shipping 10 computers to a single home address or freight forwarder, can also be a sign of potential fraud. Recognizing this activity requires flexible rule sets that can recognize not just static strings but also regular expressions or wildcards.

- **Look at as many order fields as possible — when needed.** Fraud managers wanted to write rules using many previously unavailable fields. For example, rules based on the name and category of the product are important; high-value products deserve more scrutiny and higher risk scores. A single view of all cases and the ability to take action on them in one place are also very helpful features — both had been sorely missing in the retailer's old fraud system.

- **Have a review interface with case management capabilities.** The company's fraud team wanted a solution that offered a one-screen review approach. They were tired of reviewing eight different systems or websites to gather information for their review decisions and wanted all of the key information to be displayed on one screen. The thinking was that the team would be able to review the orders faster and make fewer mistakes because all the information would be highlighted on the one review screen. This included a notes section so that the team could discard their legacy access database, which kept track of all order reviews previously.

- **Have out-of-the-box integration with third-party fraud information sources.** Integration with Ethoca, Quova, and Targusinfo and with device fingerprinting partners such as BlueCava, iovation, and ThreatMetrix can be costly but is extremely important in building a complete picture about the order. To reduce the cost and complexity of integration, the company looked for solutions that had out-of-the-box integration with a device fingerprint provider.

Phased Implementation Allowed The Company To Fine-Tune Rules And Prove Value

To reduce day-to-day operations costs, the company chose to implement a hosted solution from Accertify, a specialist vendor for online retailers and travel agencies, in conjunction with iovation, a specialist vendor for device fingerprinting. Iovation provides intelligence on a device's associations with other devices and accounts and then pairs that information with its shared global fraud and abuse database of over half a billion devices. The company also decided to take a phased approach to the solution implementation. This approach had several benefits, including the ability to:

- **Spread costs and improve accuracy over time.** Because of the financial meltdown of 2008, the company decided to spread the project over two fiscal years. This allowed it to fine-tune rule sets and improve fraud prevention for each channel covered.

- **Use a soft-launch method to go live with the new solution.** The company spent three months training the Accertify product with fraud truth data and tuning the rules to fire on known fraud orders.[1] The company then went live with a two-week soft launch. This approach required that it continue to run the old system in production and Accertify in test mode simultaneously. Both systems were scoring orders at the same time. Analysts monitored how Accertify scored fraud orders based on its newly configured rules. When needed, fraud managers tweaked the Accertify rules. At the end of the two-week soft launch test and after the online retailer was satisfied with the Accertify solution, it switched over fraud operations. The Accertify solution was now scoring all orders for fraud, and the company eliminated the old fraud system from production.

- **Track analysts' performance in a dashboard and allow them to work from home.** The company improved its fraud management performance by quantifying fraud analyst performance based on a fraud dashboard or scorecard (see Figure 1). The implementation of the Accertify and iovation solutions significantly improved this scorecard because more fields could be tracked due to new reporting capabilities. The online reporting shows when employees log in and out of the system, how many orders they review, and how long it takes to review each order; it also quantifies the fraud/nonfraud order decisions. Because the company had a convenient way to track analyst performance, it decided to allow fraud analysts to work from home. The scorecard increased competitiveness within the team, which translated into better overall performance and contributed to a better work-life balance and better retention rates for sought-after fraud analysts.

Figure 1 Fraud Analyst Dashboard

Volume	Time	Money
Total orders reviewed	Reviews completed the same day	$ amount of orders reviewed
Canceled orders	% reviews completed within one business day	$ amount of orders canceled
Confirmed fraud orders		Fraud chargebacks
Confirmed fraud %		
Number of incorrect decisions		
Fraud rate		

57026 Source: Forrester Research, Inc.

Next Steps: Pulling In Device Fingerprinting And Contextual Information

The online retailer uses iovation's device fingerprinting and Real IP technology. Device fingerprinting gives analysts the ability to recognize desktops, cell phones, tablets, etc. that have been repeatedly involved with fraudulent order submissions. Iovation has a substantial database of "bad" devices (devices that have been associated with known fraud) that are shared with all of its clients. Rules within Accertify use the iovation device information to flag suspect orders for review. Additionally, Real IP information, which is an enhancement from iovation, builds credibility of the IP geolocation rule sets. Real IP data reveals the computer's true IP address (in a "bad" country) even if the fraudster hides behind a masquerading proxy (in a "good" country). This boosts accuracy of physical distance between the user's computer and the physical shipping address.

BEST PRACTICE RESULTS: RETAILER REDUCES FRAUD LOSSES

With more-effective rules and a one-screen review interface, the retailer was able to eliminate manual reports from the review process and take on additional responsibilities (such as chargebacks and collections) within the company without increasing headcount. It could also absorb more order volume without adding headcount and allow riskier business initiatives to increase sales without exposing the company to more fraud losses. This meant not only better employee job satisfaction but also higher fraud-detection accuracy. As a result, fraud losses dropped from a peak of $2 million in 2001 to $180,000 in 2010 after the Accertify and iovation solutions were implemented in 2009.[2]

ENDNOTES

[1] Fraud truth data is a collection of known fraudulent transactions and transaction details. It's commonly used in developing rules-based and statistical models: The solution identifies what it believes to be fraudulent data, and then fraud analysts tune the rules and model so that the solution identifies only those transactions that were fraudulent.

[2] Many eCommerce merchants issue refunds for fraudulent items to hide chargebacks and show a lower fraud rate. While this practice shows a rosy picture, it hides not only fraud but also the opportunity to detect and reduce it. The company also realized that it made almost no sense to call credit card issuer banks on suspect orders, as they were not helpful toward fraud detection. This caused the company to stop calling banks.