

Fortifying Retailing from Online Fraud

Executive Summary

The Web is fast becoming a vital sales channel for retailers. In the U.S., online retail sales have grown almost 10% year over year in the past decade and are projected to reach \$248.7 billion by 2014, accounting for 8% of all U.S. retail sales.¹ The Web will also continue to play a major role in offline sales, influencing \$1.4 billion worth of in-store sales by 2014.

The robust growth of e-commerce, apart from other factors, is the result of a focused effort by retailers to attract customers online and make the Web shopping experience a compelling proposition. With the imperative to quickly seize time-to-market advantages in the fast-growing e-commerce channel, little attention has been paid to robust checks and balances for fraud management. This has left e-commerce implementations with numerous vulnerabilities. In most cases, e-commerce fraud management has been an afterthought, and where it has been considered, retailers have relied primarily on manual and reactive processes and tools.

Retailers have been able to get away with this view, as online business volumes have accounted for only a tiny fraction compared with traditional retail. Not anymore!

This white paper discusses the impact of online fraud on retailers and the obstacles preventing

proper fraud management. The paper offers new thinking on ways retailers can effectively utilize the dollars they invest in fraud solutions to better detect and prevent the rising tide of increasingly sophisticated fraudulent activities perpetrated across the Internet.

E-Commerce Fraud: A Wakeup Call

The economic crisis has forced retailers, like other organizations, to closely examine every aspect of their business for inefficiencies. This investigation has exposed the holes that exist in their e-commerce operations. Retailers are waking up to the realities of e-commerce fraud and are realizing the inadequacies of their current fraud management processes (see sidebar, "The Cost of Fraud"). Fraud is fast becoming an area of concern for retailers as they gear up for further growth in online commerce.

A director at one of our large U.S.-based retail clients who is responsible for fraud management in her organization sheds light on why e-commerce is more prone to fraud than other channels: "'Card Not Present' fraud is growing rapidly due to the perceived lack of risk to the person making the purchase," she says. "You don't have to be bold to use a stolen credit card if you think someone can't identify you. In fact, it only takes seconds from the time a credit card is stolen for someone to begin using it."



The Cost of Fraud

Fraud leads to significant loss of revenue and products. According to a Cybersource² survey, e-commerce fraud cost merchants \$3.3 billion in lost online revenues in 2009, up 18% from 2005.

- Not only is fraud itself costly, but manual fraud management also represents a significant operating cost for retailers.
- According to Cybersource,² in 2009, merchants spent nearly 0.3%-0.4% of their online revenues on managing fraud, and more than 50% of this spend was on order review staff.
- As fraud management resolution often requires retailers to contact customers and validate orders, it results in longer fulfillment cycles. Rusty fraud management practices also result in rejection of valid orders. This causes a negative impact on the customer's overall shopping experience and results in customer churn and a drop in order volumes.
- Site vulnerabilities, in this modern era, spread like wildfire. If an e-commerce site has vulnerabilities, it can severely damage a retailer's brand image and reputation, and deter good customers from transacting on the site.

Fraud Management: Current Challenges

Inadequate Toolset

Typically, retail e-commerce fraud management techniques have relied on front-end payment card validations (MOD 10 checks, BIN checks, authorization responses, etc.), customer profile checks (security questions, login analysis, etc.), or basic site rules (number of orders through one account, value of orders, etc.) or back-end manual order reviews. Transaction monitoring systems have been implemented, but these have been home-grown and have not kept pace with changes in the fraud domain. Some investments have been made in automatic fraud detection, but manual review processes remain the norm.

Information Silos

Lack of adequate focus on fraud management over the years has resulted in a lack of proper development of and integration between internal IT systems that can quickly provide data on fraud in a way that can be converted into swift action. Often, retailers do not have the right data readily available to measure their current fraud levels because there is no enterprise-wide view of fraud available. Creating these insights requires significant IT investments that are, again, in limited supply given current economic conditions.

Various business groups (e.g., marketing, customer service, cash and banking, analytics,

and loss prevention) often work in silos, with little concerted effort spent on identifying and preventing e-commerce fraud. Sadly, there is little proactive data sharing among these teams, and quite often, they have different business goals and incentives that are not aligned with fraud management.

Our client agrees: "There is definitely a lack of an enterprise-wide effort around fraud. Typically, one person spearheads an effort, and folks begin to piggyback on it," she says. "An organization must know exactly what type of fraud they are dealing with in order to effectively fight it. Unfortunately, with current systems, this takes a lot of time and data."

Insufficient Knowledge and Experience

Another fallout from the economic downturn is the across the board headcount reduction many retailers have enacted to contain costs. Since fraud management is not considered core to e-commerce operations, many fraud management teams have been radically reduced, causing significant shrink of domain knowledge and bandwidth. As a result, existing teams are finding it challenging to simultaneously work on analyzing and preventing current fraud schemes, while keeping up with the pace of change in the fraud domain and formulating robust strategies for detection and prevention.

Fraud Management: Preparing for Tomorrow

Forward-thinking retailers have already started including Web fraud management as a core component of their e-commerce strategy and have implemented (or are implementing) robust fraud management tools. This is seen in a modest 8% growth of the Web fraud detection market in 2009, despite the global economic downturn.³

Despite the slowdown, many merchants are either keeping their fraud management budgets constant or are increasing them, with automation of fraud detection seen as a priority.

There are numerous third-party solutions that can be deployed, fairly quickly, to enhance the e-commerce fraud management process by making it real-time and automatic. Most of these solutions use standardized data interfaces and provide a high degree of flexibility in configuring fraud business rules that help fraud teams quickly adapt to changing business needs. Retailers have started adopting such solutions to provide a much needed boost to their e-commerce fraud management efforts. Making

fraud detection real-time, automatic and proactive reduces the manual effort and frees up capital that can be invested elsewhere.

Working with e-Commerce merchants on implementing fraud management solutions, we have seen that, more often than not, the focus of the fraud teams is on solution

aspects that are relatively easy to identify and quantify (e.g., the feature set, ease of integration, cost of implementation, etc.). However, there are various “softer” aspects that retailers should keep in mind while implementing such solutions, which will help them achieve a better return on their investment:

- 1. Invest in expertise, not just the solution:** Retailers should consider implementing a third-party solution not only to enhance their current toolset, but also to gain access to the solution provider’s fraud management domain expertise, which internal fraud teams may lack. A retailer should focus not only on the strength of the solution, but also on the

expertise and experience of the provider’s key personnel. The provider should be seen as an extension of the retailer’s fraud management team providing guidance and education on emerging threats and best practices while enhancing the solution to keep it a step ahead of fraudsters.

One of our clients, who recently led the successful implementation of a third-party fraud management solution in her organization, says, “While a third party cannot typically speak about your customer base, they do offer a wide variety of expertise in fraud. This makes situations like downsizing or attrition less impactful.” The benefits of tapping into the provider’s expertise are immense: “The two teams (internal and provider) together created a synergy to ward off over 70% of our fraud issues,” she notes.

- 2. Keep the vision in view:** A retailer should look for a solution that not only meets its current e-commerce needs, but can also potentially scale up to meet fraud management requirements in a cross-channel retail environment. The retail industry is changing rapidly, new channels such as m-commerce are emerging, customers are demanding more cross-channel convenience. Retailers with multichannel operations, or a roadmap to enable this, should assess a fraud solution’s cross-channel capabilities to ensure that it can be easily scaled to meet future needs.
- 3. Be sensitive to sensitive data:** As most of the fraud management solutions rely on transaction data processing, a high volume of sensitive data would pass to and be potentially stored by the solution provider. Retailers should clearly understand the data security aspects of this approach and establish clear standards and audit needs for data protection at the third-party. It may be beneficial to clearly spell out, in the contract, liabilities in the event of a breach.
- 4. Build business bonds:** Implementing a fraud management solution provides an opportunity for a retailer to create a collective ownership of fraud management across different business units. As part of the implementation efforts, retailers should bring together different business owners in the decision-making process so that they understand in totality how their actions affects fraud. This opportunity should also be used to establish a contin-

In a recent survey by Cybersource, 60% of merchants surveyed cited improving the automated fraud detection and sorting capabilities of their systems as the top process improvement focus area for 2010.

uous process of fraud review by different units so that timely analysis can be conducted and corrective action taken -- rules tweaked, "bad" affiliates turned off, or front-end/back-end processes improved. Discussions should also include sharing plans on product launches, marketing programs, new customer service schemes, etc., so that they can be looked at from a fraud prevention point of view and adjusted, if necessary, at the initial stages to plug potential fraud holes.

5. **Collaborate with cohorts:** Finally, collaboration with other fellow merchants can be a great tool for fighting fraud. Many third-party fraud solutions provide the ability to share fraud data anonymously with other participating retailers to build shared "negative" lists. This helps each participating retailer tap into an extended data pool for better fraud decision making.

Retailers should also encourage their fraud teams to participate in industry forums focused on fraud management (e.g., Merchant Risk Council) and gain from the experiences and expertise of other retailers. Such forums also provide updates on new development in the area of fraud management, know-how on best practices and insights from merchants in other industries.

Conclusion

E-commerce fraud costs merchants billions of dollars in lost products and services, but its prevention also remains a significant ongoing cost for retailers. Fraud can hit a retailer's reputation and cause huge customer churn, which can take years to regain.

Though retailers have historically neglected fraud management, amid growing online business volumes, the industry is now investing in better tools and processes to make fraud management more robust and proactive. However, it is important to understand that fraud management is also an art -- a balancing act between risk acceptance and customer experience. Undue focus on one of these aspects will adversely affect the other. There has to be a level of fraud risk that a retailer is willing to accept in order to minimize interference with the shopping experience of its loyal customers.

Apart from implementing sophisticated tools and automating fraud detection, retailers need to establish internal processes to make fraud management an enterprise-wide responsibility and a key component of strategic initiatives.

References

- ¹ "U.S. Online Retail Forecast, 2009 to 2014," Forrester Research, Inc., March 2010.
- ² Online Fraud Report, 11th Annual Edition, Cybersource, February 2010.
- ³ Magic Quadrant for Web Fraud Detection, Gartner, Inc., January 2010.

About the Authors

Surya Prakash Saurabh is a Consulting Manager in the Retail Practice within Cognizant Business Consulting. He can be reached at Surya.PrakashSaurabh@cognizant.com.

Rohit Chandel is an Associate Consultant in the Retail Practice within Cognizant Business Consulting. He can be reached at Rohit.Chandel@cognizant.com.

About Cognizant

Cognizant (NASDAQ: CTSH) is a leading provider of information technology, consulting and business process outsourcing services. Cognizant's single-minded passion is to dedicate our global technology and innovation know-how, our industry expertise and worldwide resources to working together with clients to make their businesses stronger. With over 50 global delivery centers and more than 85,500 employees as of March 31, 2010, we combine a unique global delivery model infused with a distinct culture of customer satisfaction. A member of the NASDAQ-100 Index and S&P 500 Index, Cognizant is a Forbes Global 2000 company and a member of the Fortune 1000 and is ranked among the top information technology companies in BusinessWeek's Hot Growth and Top 50 Performers listings.

Start Today

For more information on how to drive your business results with Cognizant, contact us at inquiry@cognizant.com or visit our website at www.cognizant.com.



Cognizant

Passion for building stronger businesses

World Headquarters

500 Frank W. Burr Blvd.
Teaneck, NJ 07666 USA
Phone: +1 201 801 0233
Fax: +1 201 801 0243
Toll Free: +1 888 937 3277
Email: inquiry@cognizant.com

European Headquarters

Haymarket House
28-29 Haymarket
London SW1Y 4SP UK
Phone: +44 (0) 20 7321 4888
Fax: +44 (0) 20 7321 4890
Email: infouk@cognizant.com

India Operations Headquarters

#5/535, Old Mahabalipuram Road
Okkiyam Pettai, Thoraiipakkam
Chennai, 600 096 India
Phone: +91 (0) 44 4209 6000
Fax: +91 (0) 44 4209 6060
Email: inquiryindia@cognizant.com