

# Visa e-commerce cross-border handbook for U.S. retailers

## Chapter 10: fraud management and security





# **Visa e-commerce cross-border handbook for U.S. retailers**

## Chapter 10: fraud management and security

For inquiries, contact:

Stephanie Wallat  
Visa Canada  
416-860-3861  
[swallat@visa.com](mailto:swallat@visa.com)



# Visa e-commerce cross-border handbook *for U.S. retailers*

## Chapter 10: fraud management and security

---

### Preface

To finish off this set of guidelines and tips for your cross-border initiative, a discussion of fraud management and security is essential. Chapter 10 drives its focus on these topics.

Specifically, this section covers key metrics, validation services and some of the unique factors and conditions of the Canadian market place. The chapter combines general best practices with a Canadian focus.

While the handbook is not meant to answer all of your questions on this or any of the covered topics, it is our ardent hope that the information contained in this chapter and others, provides your organization with a general overview, as you examine the opportunities present in the Canadian market.

# Chapter 10: fraud management and security

Authored by: Paul Brock, CyberSource Corporation

## Introduction

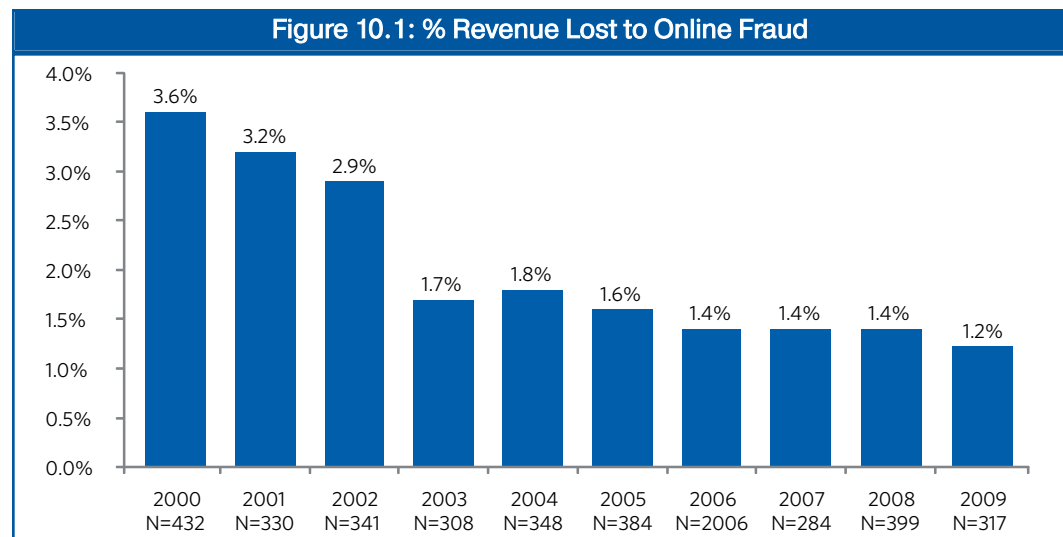
To understand how to approach online fraud management for the Canadian market, it is first useful to understand key, end-to-end process metrics. These below are derived from CyberSource Corporation’s annual survey of online fraud among U.S. and Canadian merchants. Following that discussion, we’ll discuss general best-practice approaches and how the nuances of the Canadian market impact the tuning and application of these practices for Canadian orders.

### Sub-topics:

- Key metrics
- Validation services
- Canadian market: unique factors and conditions

## Overview

Over the past ten years, the percent of online revenues lost to payment fraud has been stable or declining. From 2006–2008, the number was 1.4%. In 2009, it declined to 1.2%.



## Key Metrics

The percent of accepted orders that are later determined to be fraudulent has also been relatively stable or declining. Over the past six years, the average has hovered around 1.0. In 2009, the rate was 0.9%, the first time this rate has dropped below the 1% threshold.

Put more simply, merchants are accepting a higher percentage of orders. In 2008, the overall order rejection rate due to suspicion of fraud dropped to 2.9% compared to 4.2% in 2007. By 2009, that number had dropped to 2.4%.

As the growth rate of online sales has slowed during 2008 and 2009, it appears merchants are now focusing even more attention on sales conversion and reducing their fraud-related, order-rejection rates. The survey results indicate most merchants have successfully increased their order acceptance rate with little or no increase in fraud rates. It remains to be seen if online merchants can continue to control fraud rates while increasing order acceptance in 2010.

#### Chargebacks Understate Fraud Loss by as much as 50%

Overall, merchants continue to report that chargebacks accounted for less than half of fraud losses. The remainder occurred when merchants issued credit to reverse a charge in response to a consumer's claim of fraudulent account use.

#### International Order Risk 3½ Times Higher than Domestic Orders

On average, merchants say orders from outside Canada are twice as likely to be fraudulent than domestic orders. While that may seem huge, it represents a considerable improvement over the year before where fraud rates associated with international orders were three-and-one-half times their domestic counterparts. To mitigate losses, merchants reject international orders at a rate three times higher than domestic orders.

#### Manual Review Rates

Over the past five years, the overall percent of online orders that enter manual fraud review has fluctuated between 20% and 27%; about 1 out of 4, on average. In some segments, fraud risk is low enough for merchants to rely entirely on automated review, which lowers the aggregate review ratio. But most merchants do manually review orders for fraud risk. Over the past five years, these merchants review, on average, 1 out of every 3 orders.

Over the past five years, merchants who engage in manual order review have maintained this average review rate. Large online merchants, who typically employ more automation, continue to have much lower manual review rates. Over the past three years, large merchants (\$25M+ in online sales) performing manual order review have, on average, reviewed approximately 15% of orders. Looking back over the past several years of survey data, we conclude that most merchants have made little progress in reducing their reliance on manual review and are likely reviewing far more orders today than they were just a few years ago.

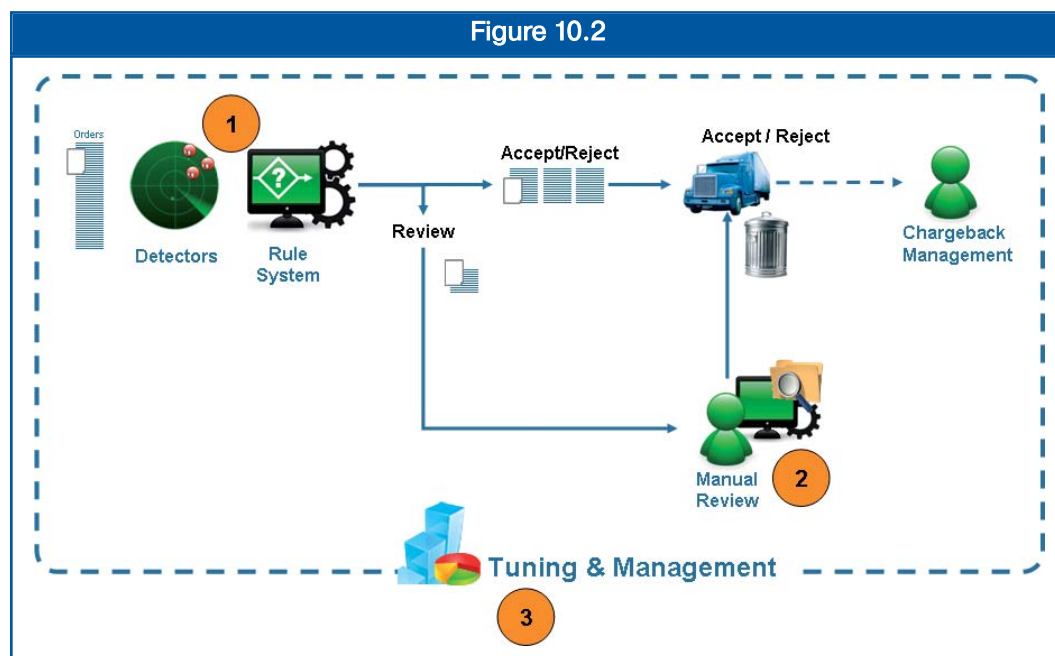
#### Efficiency Gains Required

As e-commerce sales continue to grow and budgets and resources remain relatively fixed, merchants face the challenge of screening more online orders while keeping order rejection and fraud rates as low as possible to maximize sales and profits. Continued reliance on manual review presents a serious challenge to scalability. Can merchants grow their review staffing sufficiently to keep pace with fraud? Similar to 2008, in 2009 only 13% of online merchants expect to increase manual review staff in the coming year and 9% anticipate decreasing staff levels. These are the lowest levels of planned staff increases we have seen in the 11-year history of the survey. At the same time, merchants report that improving their automated detection and sorting capability is a key area of focus for 2010.

### Managing Fraud Effectively in the Canadian Market

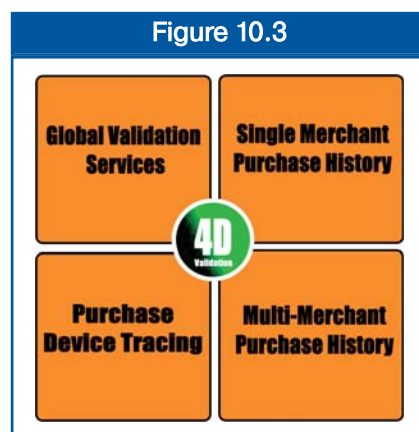
Similar to the U.S. market, a multi-layered, full-process approach to fraud management is recommended as a best practice for the Canadian market. This approach advocates that you adopt an automated screening and validation stage, including:

1. Multiple detectors and a rules engine to interpret the results;
2. A case-management system that supports queuing cases based on product category, shipping method or other attribute and consolidates order and validation data for efficient review and validation by manual reviewers; and
3. An adequate set of analytics that permits an understanding of critical metrics (e.g., fraud rate, rejected orders, rule results, etc.) throughout the process.



The area deserving the most attention when transitioning between the U.S. market and the Canadian market is Stage 1 – the application of detectors/validation tests and the interpretation of those results by your rules system. Before discussing the granular differences, it is important to understand that the best practice is to deploy a detection strategy based on four dimensions of detection. Studies have shown that merchants who derive the best results from their fraud management processes (lowest fraud, lowest review rate, lowest rejection rates) are twice as likely to deploy a four-dimensional detection approach.

By using these four dimensions, merchants are better able to uncover the abnormality in the fraudster’s identity—the fraudster may be able to mask one or more attributes of an identity, but likely not all. The following is a brief summary of detectors typically utilized within these categories.



---

## Validation Services 1. Global Validation Services

This category includes tests and services that validate the purchaser based on demographic or account enrolment data, including the following:

- Telephone Number Validation
- Delivery Address Verification: Validates address format and deliverability. Often used at time of order placement to detect “fat fingering” and eliminate the risk of invalid order rejection or mis-shipment.
- U.S. Export Compliance/DPL Lists: Real-time check of denied parties and persons of question across multiple lists maintained by U.S. government agencies.
- Payer Authentication Services: Validates cardholder identity based on enrollment in Verified by Visa and related card brand authentication programs.
- AVS/CVV Services: Real-time check of Address Verification Service (AVS) and card verification number services provided by card brands.

## 2. Single Merchant Purchase History

This category includes tests to evaluate and correlate the purchase behavior evidenced at the merchant site, including the following:

- Single Merchant Purchase Velocity : Monitors the frequency of orders placed at this merchant, the purchases of a particular SKU in a given timeframe, and the value of accumulated purchases, or a combination of these conditions. This helps identify abnormal purchase behavior such as the purchase of 10 flatscreen TVs, etc.
- Negative & Positive Lists: Lists maintained by merchant to denote customers they do not wish to sell to (based on prior fraudulent or related purchase history) or conversely, a list of loyal customers for whom they wish to always ensure order approval.
- Other Customer Data: Other data from customer purchase histories that may be useful to the merchant in determining fraud risk.

## 3. Multi-Merchant Purchase History

This category includes tests to assess purchase behavior across multiple merchants, including the following:

- Identity Morphing Detection: Tests to detect whether personal identifiers, such as email or name, have been used with other identities or credit cards and thus raise questions regarding order integrity.

- Neural Net Risk Detection Model/Risk Score: Commercial models that utilize statistical modeling to assess purchase patterns and behaviors to deliver a risk score.
- Global Purchase Velocity : Measures the frequency of purchase activity across multiple merchants.

#### 4. Purchase Device Tracing

This category of detectors assesses whether the attributes of the purchasing device are consistent with that of a “good” or “fraudulent” purchaser, including the following:

- Device Fingerprinting & Profiling: Derives a “digital fingerprint” of the device used for order placement. This fingerprint can then be used in conjunction with other order attributes to detect abnormalities (same device, different identities, etc.). Some technologies can also determine the nature of activity arising from that device, such as firewall scanning, SPAM distribution, etc., all of which would be consistent with botnet behavior and thus carry a higher suspicion of fraud.
- IP Geolocation: Assesses the consistency between the geographic location of the IP address and address/billing information provided with the order. This includes the ability to detect anonymizers.

While many of these detectors can be applied similarly for the U.S. and Canadian markets, some must be interpreted differently, or applied with more or less weight. The following discusses notable differences in application.

#### Canadian Market: Unique Factors and Conditions

#### Tuning your practices for the Canadian market

Up to now, we have been discussing best practices that more or less hold true in many places around the world – further proof that fraud knows no borders. Let us now look at some factors and conditions unique to Canada, that influence how you apply and tune these practices. First, two detectors that deserve your attention.

- Delivery Address Verification: The Canadian postal code system offers even greater reliability when testing for address consistency (9-digit number/letter code). If postal code referencing is not among your current tests, you should apply this element as a part of your screening profile when assessing Canadian orders.

CyberSource’s “Online Fraud Report” indicates 78% of merchants in the U.S. and Canada employ a delivery address verification check for inbound orders to confirm the deliverability of the address provided. The check can also be used effectively in conjunction with IP Geolocation tests to validate purchaser device and address location consistency.

- **Payer Authentication:** This general term incorporates cardholder verification programs such as Verified by Visa®. These programs enjoy broad acceptance in Canada (considerably higher than in the U.S.), deliver greater fraud protection for your customers, and can bring you significant chargeback protection. Because the programs enjoy strong support in Canada, Canadian consumers are accustomed to seeing this step during the checkout process. We strongly recommend you employ these programs as a part of your fraud management toolkit.

## Differences in Interpreting Detector Results

- **IP Inconsistencies can mean Different Things in Canada than they do in the U.S.:** Seeing an IP address from a different country than the delivery address on the order can raise a red flag in the U.S.; not necessarily so in Canada. One of the country's largest Internet service providers frequently resolves to a Chicago-based IP address. Canadian consumers can, in fact, be purchasing from Canada, but display an out-of-country IP address, so a greater tolerance for cross-border ordering is advised to avoid wrongly turning away good orders. That can also be true for orders originating in rural, isolated environments. The common connection strategy in those areas is via satellite. Satellite connections are typically viewed with suspicion south of the border because they are harder to trace (and thus a vehicle used by fraudsters). Denying satellite-based orders from some areas in Canada can mean you are turning away a significant percentage of your likely shoppers.
- **“Foreign” Cards Aren’t Necessarily So:** It is not uncommon for Canadians to use payment cards issued outside of Canada, whether those cards are from France, the U.K., or the Caribbean. Wholesale rejection of orders made on foreign-issued cards can seriously impede legitimate business opportunities.
- **Address Challenges May Cause False Positives:** Canada is a prosperous country that happens to occupy a northerly spot on the globe. It is not uncommon for residents to have more than one address—at least one located in a warmer environment. Indiscriminate rejection of cards because the ship-to address is outside of Canada can cause unnecessary loss of online revenue and insults to customers.

## E-commerce Fraud in Canada – A-Two Rule Summary

- **Rule #1:** Understand that linguistic and cultural similarities aside, Canada and the U.S. are not the same country. Many Canadian payment practices, including address verification, reliance on payer authentication programs, IP addresses, use of foreign-issued cards, etc., are radically different than practices in the U.S. Doing business in Canada and using U.S.-based rules can set your e-commerce sales back significantly.
- **Rule #2:** Learn your way into Canadian e-commerce through pre-production testing. It is important to work with a fraud management system that will allow you to passively analyze the impact of fraud screening rules on sales activity before you impact real orders. Review more than you have done in past environments to learn, all over again, what a good order looks like...then automate.

---

## Implications

- **Financial:** Failure to efficiently manage fraud can cause loss of revenue opportunity (rejecting valid orders), unnecessary revenue loss, and unnecessary sales overhead (manual order review). All of these concerns can be mitigated with proper fraud-management tools.
- **Strategic:** Management may view international order acceptance as carrying an unacceptable level of fraud risk, and thus choose not to enter (or pull out after a short period of time). With the proper tools, this need not be an issue.
- **Consumer:** The inability to manage fraud effectively can result in higher prices (passing on the cost of loss to consumers). It also results in poor customer experience (i.e., delayed shipment of goods due to unnecessary order review, or cumbersome checkout processes that create extra navigation or checkout steps). Proper tools and rules can maximize fraud management transparency and thus improve customer experience.

## Checklist

Some of the elements your company will need to consider as it establishes the fraud management and security systems include the following:

Review of Items	Key Elements	Cross-border Emphasis Required
<b>Global Validation Services</b>		
■ Telephone Number Validation	■	■
■ Delivery Address Verification	■	■
■ U.S. Export Compliance/DPL Lists	■	■
■ Payer Authentication Services	■	■
■ AVS/CVV Services	■	■
<b>Single Merchant Purchase History</b>		
■ Single Merchant Purchase Velocity	■	■
■ Negative and Positive Lists	■	■
■ Other Customer data	■	■
<b>Multiple Merchant Purchase History</b>		
■ Identity Morphing Detection	■	■
■ Neutral Net Risk Detection Model/ Risk Score	■	■
■ Global Purchase Velocity	■	■
<b>Purchasing Device Tracing</b>		
■ Device Fingerprinting and Profiling	■	■
■ IP Geolocation	■	■
<b>Canadian Specific Practices</b>		
■ Delivery Address Verification	■	■
■ Payer Authentication	■	■

## About the Author

**Paul Brock** is a Senior Fraud Analyst at CyberSource Corporation. He has more than 20 years of technology consulting experience, delivering improved risk management performance to the online operations of Fortune 1000 companies across a variety of industries. Paul provides extended best practices consulting and education to large-scale online merchants and leads consulting teams in the delivery of innovative credit card and electronic payment processing solutions.

Prior to joining CyberSource, Paul led business intelligence teams and implementation projects at SGI, Compaq, IBM Global Services, and EDS. Paul earned his BBA in Accounting from the University of Texas in Austin in 1989.