

Strategies to Effectively Mitigate Fraud

17 November 2015

Stan Hui, Director – Merchant Risk

Cory Siddens, Senior Director – CyberSource Risk Solutions



VISA

Disclaimer

The information or recommendations contained herein are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. When implementing any new strategy or practice, you should consult with your legal counsel to determine what laws and regulations may apply to your specific circumstances. The actual costs, savings and benefits of any recommendations or programs may vary based upon your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties and assumptions that are difficult to predict or quantify. Assumptions were made by us in light of our experience and our perceptions of historical trends, current conditions and expected future developments and other factors that we believe are appropriate under the circumstance. Recommendations are subject to risks and uncertainties, which may cause actual and future results and trends to differ materially from the assumptions or recommendations. Visa is not responsible for your use of the information contained herein (including errors, omissions, inaccuracy or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use. Visa makes no warranty, express or implied, and explicitly disclaims the warranties of merchantability and fitness for a particular purpose, any warranty of non-infringement of any third party's intellectual property rights, any warranty that the information will meet the requirements of a client, or any warranty that the information is updated and will be error free. To the extent permitted by applicable law, Visa shall not be liable to a client or any third party for any damages under any theory of law, including, without limitation, any special, consequential, incidental or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, even if advised of the possibility of such damages.

Overview



Overview

- Visa's objective is to educate acquirers and merchants of fraud and chargeback issues which may arise during the holiday shopping season
 - Retailers may realize significant increase in holiday sales from October to January with corresponding fraud and chargebacks increases in October to March
 - Merchants have an opportunity to optimize consumer experience and reduce false-declines while minimizing fraud losses
- Criminals take advantage of the holiday season to maximize use of stolen payment card data
 - Most criminal syndicates are knowledgeable of issuer authorization practices, acquirer acceptance practices, and merchant store policies and procedures
- Acquirers and their merchants should carefully tune their security and fraud prevention tools to screen out risky transactions
 - Avoid shutting off security tools
 - It's better to avoid potential disputes (fraud or chargeback) than try to manage it in the back office

Targeted Industries and Products

- Key Sales Channels Covered:
 - Card Not Present – eCommerce, MO/TO, and Recurring Payments
- Targeted Industries and Products:
 - Gift cards
 - Funds transfers
 - Electronics including phones, tablets, video game systems and software
 - High-end and luxury goods
 - Jewelry
 - Airlines, travel agents, concert ticket distributors
 - Other fungible goods such as popular toys, cell phone minutes, etc.

Why are we talking about CNP?

\$3.5T

GLOBAL ECOMMERCE SALES WILL
DOUBLE FROM 2015 TO 2019

\$1.7T



Challenge: Optimize authorization and fraud management practices to maximize the growth of ecommerce and digital payments

Card Not Present Retailers eCommerce, MO/TO, and Continuity Merchants



Card Not Present Fraud: Identifying Potential Red Flags

- Transactions from “unusual” IP addresses
 - Some online retailers have received fraudulent transactions from a foreign country thousands of miles away
- Shipping and billing addresses mismatch
 - In some cases, ship to and billing addresses are separated by significant distances
- Unusual transaction activity from new customers
 - Very large total spend spread across multiple transactions
 - In some cases, these transactions occur in a short period of time (e.g., couple of days)
 - “Rush” or “overnight” shipping
 - Orders made up of “big-ticket” items
 - A holistic review of the account’s purchasing pattern will reveal any unusual activity



Card Not Present Fraud: Addressing Red Flags

- Adopt a KYC “Know Your Customers” mentality and assess how customers access your website
 - Use “strong” and unique passwords with customers (e.g., letters, numbers, special characters, upper and lower cases) to prevent account takeover attacks
 - Analyze customer data:
 - Review any unusual or out of pattern purchases; Are customer purchases consistent with past history (e.g., ticket size, transaction velocity)
 - Verify customer email addresses and obtain secondary contact info (e.g., cell phone)
 - Validate any unusual activity with the customer via email, text message, or direct call
 - Shipping / Billing addresses - are you shipping to a different location from the customer?
 - Cross reference Internet Protocol (IP) addresses; Is the web domain consistent with where your customer is located?
 - Track how customers make purchases; Phone, tablet, PC, website, mobile app, or call center

Card Not Present Fraud: Addressing Red Flags (cont.)

- Avoid lowering settings on fraud strategy tools
 - Many merchants that relax setting to maximize holiday sales were identified in Visa's fraud / chargeback monitoring programs
 - Merchants should consider fine tuning the settings on their fraud tools based on projected holiday sales
 - If needed, train staff to review orders and screen out suspicious and potentially fraudulent transactions
 - Use online tools to optimize your current processes (e.g., do online satellite images show the shipping address as a large vacant field?)



Card Not Present Fraud: Addressing Red Flags (cont.)

- It's better to avoid a fraudulent transaction and related chargeback than try to manage it in the back office
- Use the right set of tools for your environment and business line
- In the United States, Card Verification Value 2 (CVV2) and Address Verification Service (AVS) are the minimum set of security tools
- If you're in a line of business which may be targeted by fraudsters (e.g. gift cards, jewelry, money transfer), employ additional security tools to screen out the fraud
 - For acquirers, even if your merchant isn't in one of the targeted lines of business, their website could be used to test account data
- In the end, the right set of security tools will make most merchant websites an unattractive target for fraudsters

Card Not Present: Minimizing Chargebacks

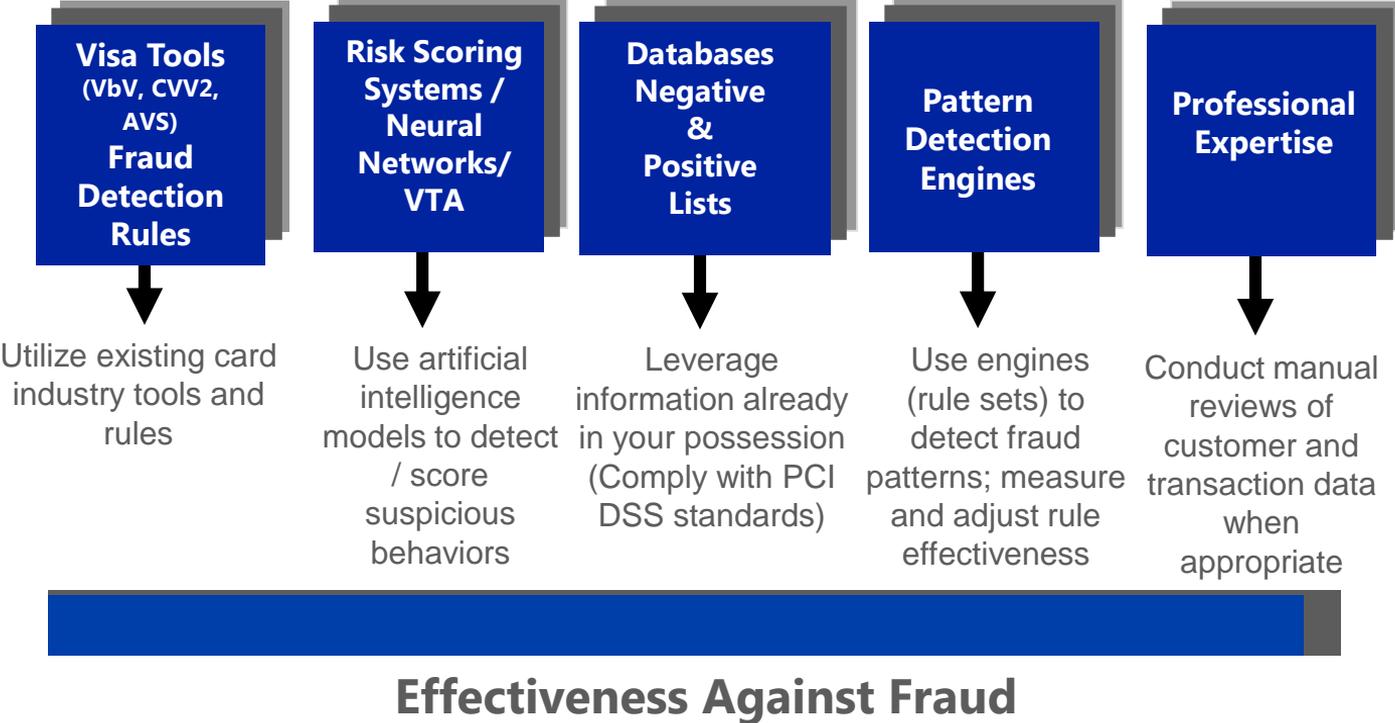
- Will there be product shortages due to increased sales resulting in fulfillment related chargebacks?
- Are the refund and return policies clearly disclosed, prominently displayed to the consumer, and easy to understand? Are they well executed?
 - Some merchants have had significant chargeback issues due to poor customer service practices
- Screen out potentially fraudulent transactions
 - Review any unusual / suspicious transactions manually
 - When in doubt, contact the customer to confirm the order
 - Screen out these potentially fraudulent transactions before requesting an authorization



Card Not Present: Minimizing Chargebacks for Continuity Merchants...

- Memberships and subscriptions are common holiday purchases
- Acquirers should review their continuity merchants (e.g. memberships, subscriptions, etc.) business practices:
 - Are there clear and easy to understand terms and conditions in the merchants disclosures?
 - Are all of the charges and future charges clearly defined with amounts and dates?
 - Do the continuity merchants reach out to their customers before renewing the membership or subscription?
 - Is there enough lead time to process cancellations and refunds?

Effective Fraud Management Requires a Layered Security Strategy



Fraud Detection Engines Key Components

1. **IP Tracking:** This has many purposes, for example - not accepting sales from similar IP's without reviewing the details, geo tracking for known "High Risk" hot spots.
2. **Velocity Checking:** Account number, IP Address, number of transactions etc.
3. **BIN and BIN Country verification checks:** What is the Issuer BIN country? Does this verification raise concern?
4. **BIN Tracking and Customer Performance tracking:** Review for anomalies and follow-up requirements.
5. **Use of "Positive-List" and "Negative-List":** Track and check sales and recurring payments against previous reported fraud / chargebacks, refunds, IPs, emails, good customer data etc. The goal is to reduce fraud as a percentage of sales while minimizing the impact of this effort.

Fraud Detection Engines Key Components (cont.)

- 6. Shipping:** Ship to billing address. Variances should be scrutinized and further risk assessment made.
- 7. Email confirmation:** Consider cancelling or refunding orders if e-mail verification bounces back.
- 8. Email Domain verifications:** Ensure domains and IP's are to major ISP's (Caution should be exercised for those customers using free emails) .
- 9. Balancing:** Systems should be capable of tracking refunds requested to refunds processed.
- 10. E-mail/SMS reminders:** For recurring transactions, it is a best practice to send the consumer reminder several days before a recurring transaction is initiated.

A decorative graphic consisting of three horizontal bars of varying lengths and shades of blue, positioned in the upper right quadrant of the slide.

CyberSource Risk Management Solutions

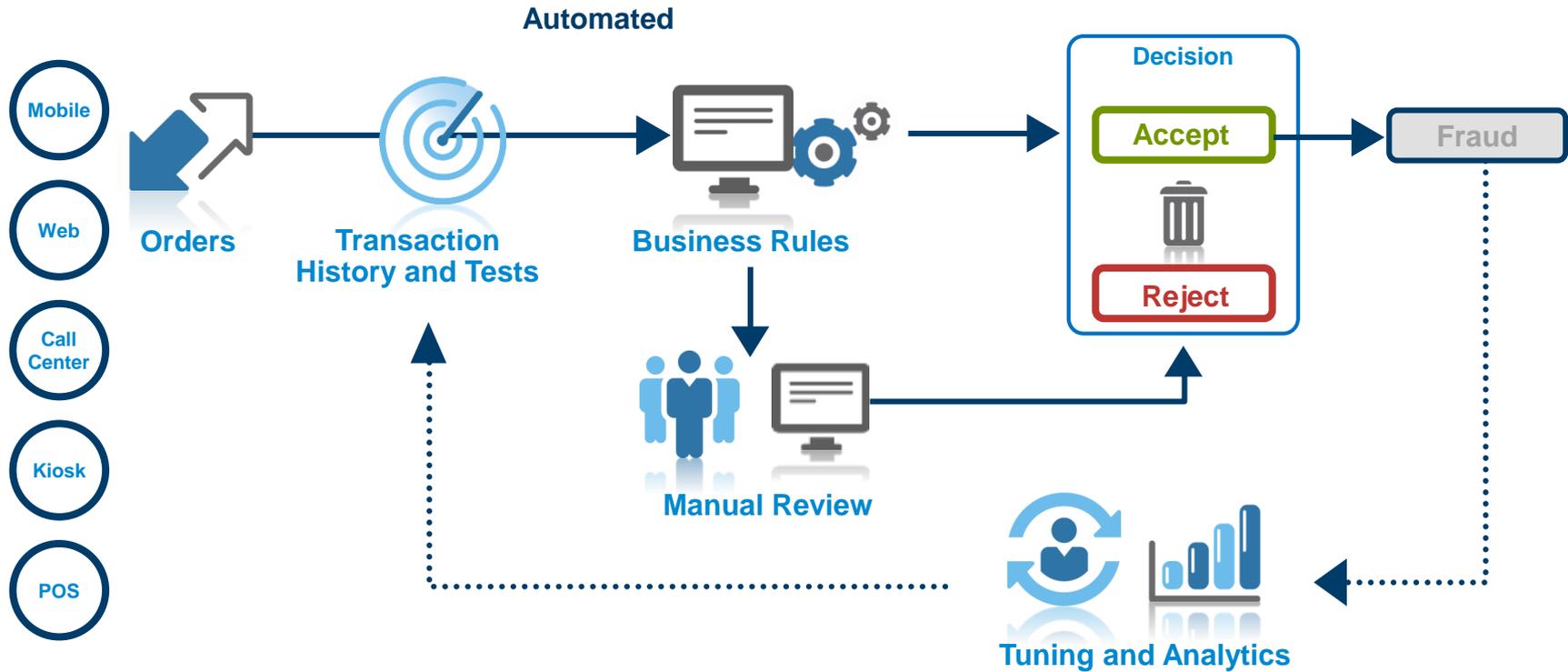
Cory Siddens

Sr. Director

Product Management

CyberSource®

Fraud management process



CyberSource Decision Manager

1



Detection Radar

- Proven risk model
- Detection insights from over 68 billion Visa and CyberSource trans
- Global multi-merchant data
- 260+ detection tests
- Device finger-print analysis

2



Rules Engine

- Flexible rule building
- Change rules instantly
- Use our risk score or customize your own

3



Case Management System

- One console with all necessary data sources to make decision
- Manage review queue priorities and team assignments

4



Tuning and Analytics

- Real-time reporting suite: financial, operations, review team analysis
- Fine tune with passive testing without impacting operations

Transaction history

- Purchase velocity
- Shipping method data
- Bad customer list
- Good customer list

3rd-party data sources



Popular detection tests

- Phone data
- Address validation
- Device fingerprint
- Packet signature inspection
- IP geolocation data

More data
improves
accuracy

WORLD'S LARGEST
**FRAUD
DETECTION
RADAR**

CyberSource®

Service checks

- Card # / address match (AVS)
- Card verification number
- Valid account number

VISA

- Billing/shipping histories
- Email address histories

- Name histories
- Phone histories

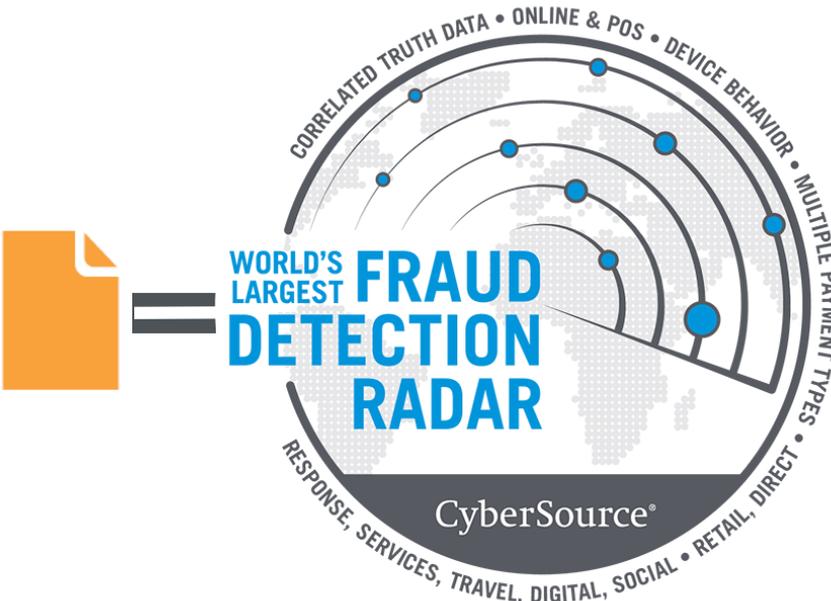
- Online/mobile
- Online (POS)

- BIN checks
- Chargebacks and more...

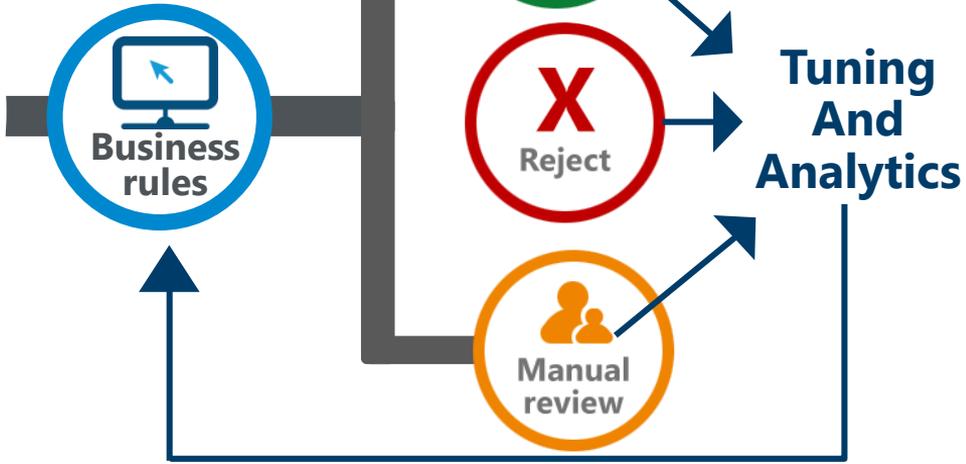
CyberSource®

All brand names and logos are the property of their respective owners and the above-mentioned reference does not imply product endorsement or affiliation with Visa

Improved accuracy increases automation



Increases fraud pattern visibility
200X



Compares with insights from over...

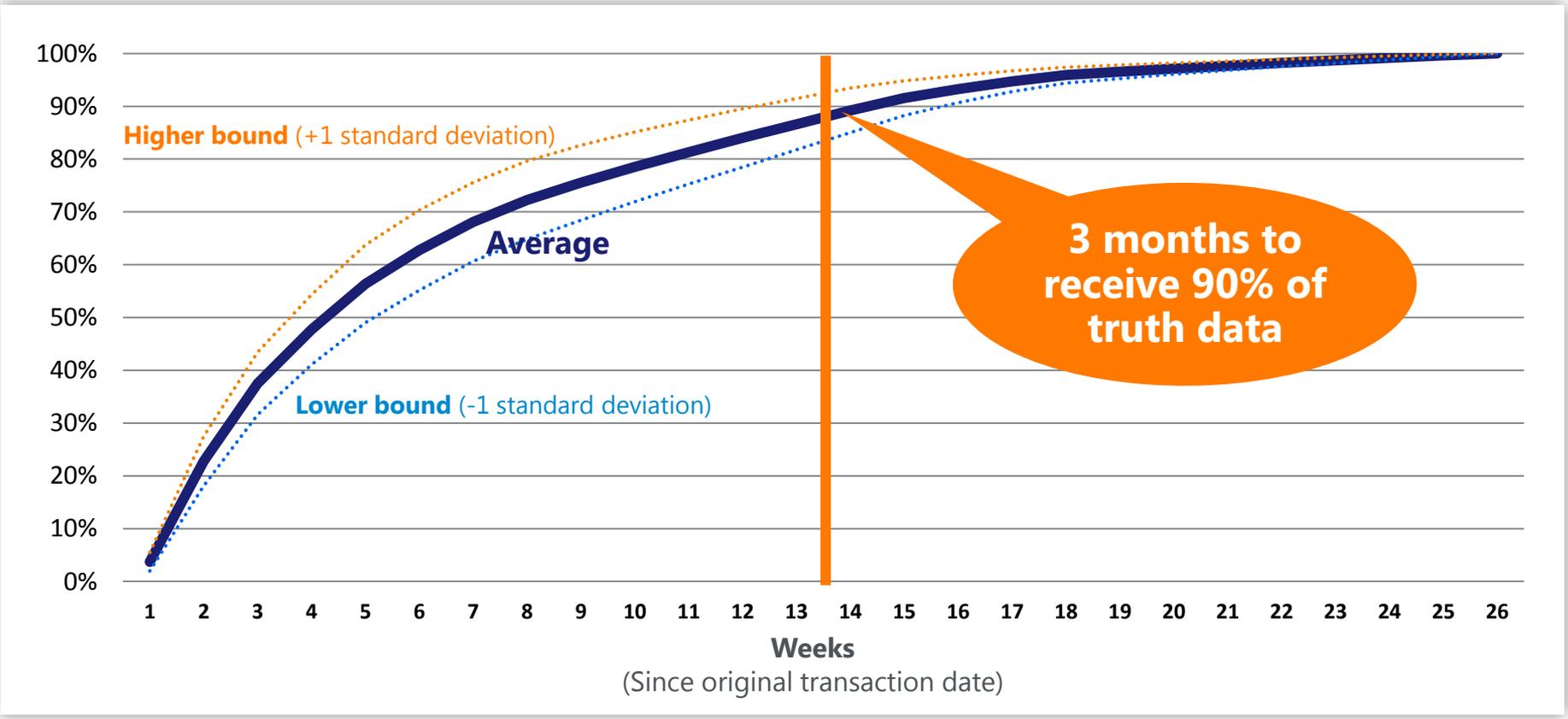
68B
annual Visa and CyberSource transactions worldwide

260
real-time correlation tests

VTA
Merchant Risk Score

*Source: CyberSource North America Merchants Fraud Benchmark Report 2015

Cumulative chargeback percentage rate



Note: This graph is illustrative of the chargeback rates typically seen by CyberSource across its merchant base over a 26 week time frame.

Strategy tuning

Current state

3-month lag time

Results

Current strategy



Impact unknown

Impact?

New strategy



Sequential

Impact?

Next strategy



Decision Manager Replay



**Transaction history
including all data
elements from
order session**



Strategy Test A

Strategy Test B

Strategy Test C

Strategy Test D

Strategy Test n...

Activate best

Allows comparing before/after and triggered rules

Before Replay

Current strategy	GRAND Total	Accept	Reviewer Accept	Review	Reviewer Reject	Reject
		\$798,823.76	\$425,148.18 (53.22%)	\$55,436.14 (6.94%)	\$82,573.33 (10.34%)	\$27,721.54 (3.47%)

After Replay

New strategy		Accept'	Review'	Reject'	Accept	Reviewer Accept	Review	Reviewer Reject	Reject
			\$483,672.16 (+13.77%)	\$155,788.78 (+88.67%)	\$159,362.82 (-23.36%)	<u>\$390,215.17</u> (-8.22%)	<u>\$24,434.93</u> (+44.08%)	<u>\$33,633.32</u> (+40.73%)	<u>\$9,511.83</u> (+34.31%)
				<u>\$30,695.04</u> (+7.22%)	<u>\$30,695.21</u> (+55.37%)	<u>\$44,817.01</u> (-45.72%)	<u>\$17,058.72</u> (+61.54%)	<u>\$32,522.80</u> (+15.64%)	
				<u>\$4,237.97</u> (+1.00%)	<u>\$306.00</u> (+0.55%)	<u>\$4,123.00</u> (+4.99%)	<u>\$1,150.99</u> (+4.15%)	<u>\$149,544.86</u> (-28.08%)	

Show in parenthesis

- % Change (before vs. after)
- % of total before
- Transaction amount (US\$)
- Change in transaction count
- % of total after
- Fraud count

Note: This data is illustrative of an order disposition for a mid-sized merchant typically seen by CyberSource across its merchant base

Account Takeover Protection

- Keep customer accounts safe and protect against the fraudulent use of account-on-file payments
- Identify fraud at account creation and login, and monitor for suspicious account changes
- Decision to Accept, Reject or Challenge
- Enables you to monitor activity to enhance the security of your customer accounts

CyberSource Decision Manager helps bring balance to your business...

Services



**Payment
Fraud
Protection**



**Account
Takeover
Protection**

3-D

***Rules-Based
Payer
Authentication***

Tools



**Case
management**



**Core rules
engine**



**Tuning
and analytics**



Decision Manager Platform

CyberSource®

...helping your business gain efficiencies
and optimize profits



How to get started

- Ask if your organization is optimized
- Are you operating with a balanced view
- What's your fraud pattern visibility
- Are you reducing friction
- What's your tuning frequency
- How accurate is your forecasting



CyberSource®

To Learn More Visit

cybersource.com/products/fraud_management/

CyberSource®

Visa E-Commerce Merchants' Guide to Risk Management

Merchant Resource Library

<https://usa.visa.com/support/merchant/library.html>

Direct link

<https://usa.visa.com/dam/VCOM/download/merchants/visa-risk-management-guide-ecommerce.pdf>



Questions?

