Guarding Against Card-Not-Present Fraud

Sylvia Auyeung – Merchant Risk

Nathan Wood – CyberSource

Visa Public

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.

Agenda

- CNP trends
- Key mobile trends
- How prevalent is mobile commerce?
- Is mCommerce riskier than eCommerce?
- What is the right fraud strategy for mCommerce transactions?
- How do you configure your solution to minimize mCommerce fraud?
- Q&A

Visa Public

The amount of data is enormous and growing

VISA

Email users send

204,166,667

messages

Google receives over

2,000,000

search queries

Facebook users share

684,478

posts

Twitter users send over

100,000

tweets

644,444

phishing emails sent

every minute.

Source: www.domo.com, www.phishing.org

Visa Public

What's driving the massive data creation?

In 2015….

4.9 billion
connected devices

In 2020….

25 billion
connected devices

Source: Gartner

Visa Public

Why are we talking about Card Not Present (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

Source: eMarketer July 2015, includes online and mobile ecommerce

Visa Public

Mobile Fraud

Convert more mCommerce orders with less fraud

CyberSource®

U.S. smartphone ownership at highest levels

68% **of U.S. adults have a smartphone, up from 35% in 2011, and tablet computer ownership has edged up to 45% among adults**

Source: "Technology Device Ownership: 2015", PewResearchCenter, October 2015 http://pewrsr.ch/1GyFf76

Visa Public

Mobile made its presence known over the holidays

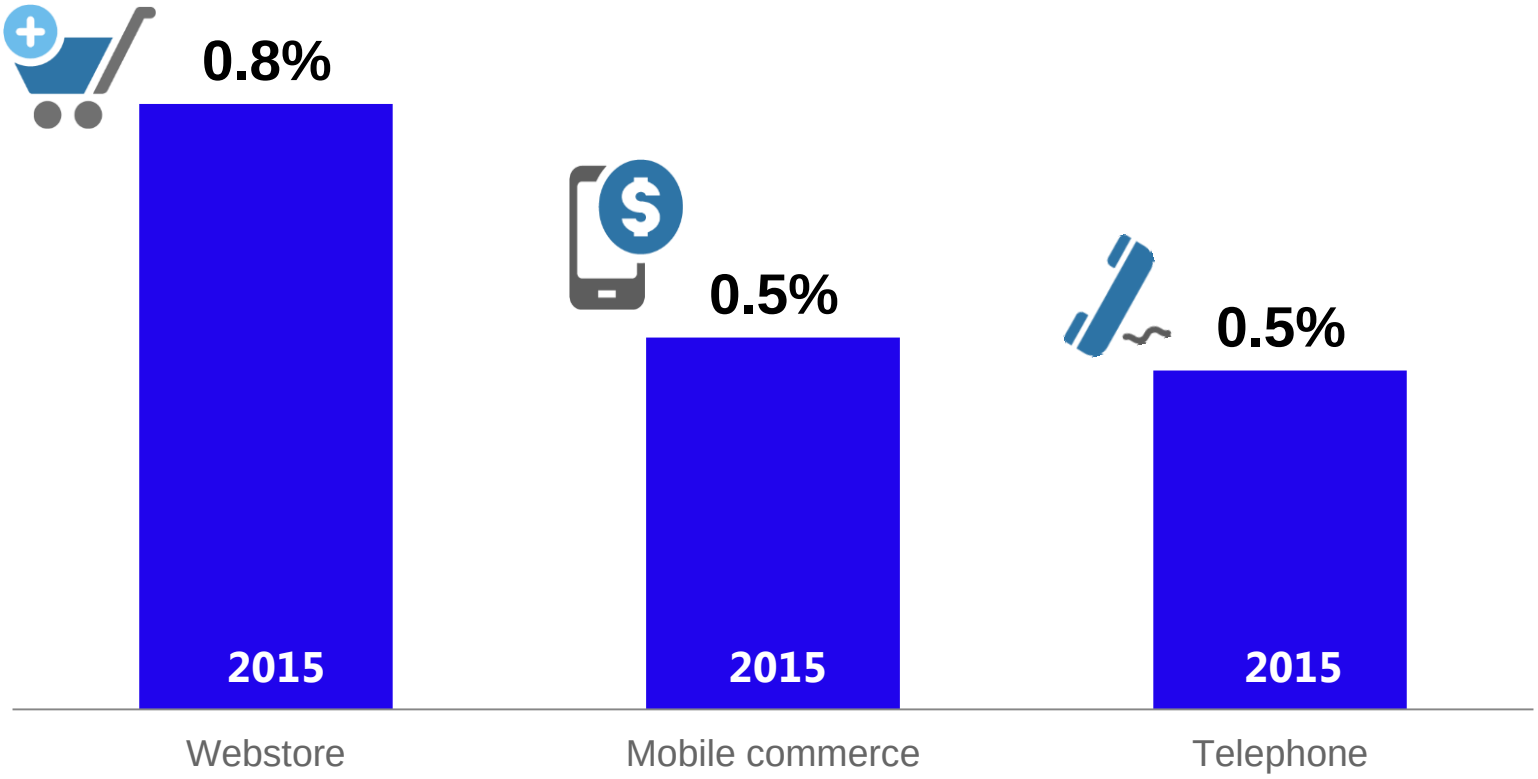
1 in 5 U.S. online holiday purchases made over mobile [1]

44% of smartphone users said they made a purchase from their device, up from 41% a year ago [2]

Source: 1 "Mobile accounts for nearly 1 in 5 online holiday purchases", Internet Retailer, January 8, 2016 http://bit.ly/1Pjyggm
2 ""Survey Shows Rapid Growth in Online Shopping", Wall Street Journal, June 8, 2016 http://on.wsj.com/1PgQjod

Visa Public

Overall fraud loss by order channel

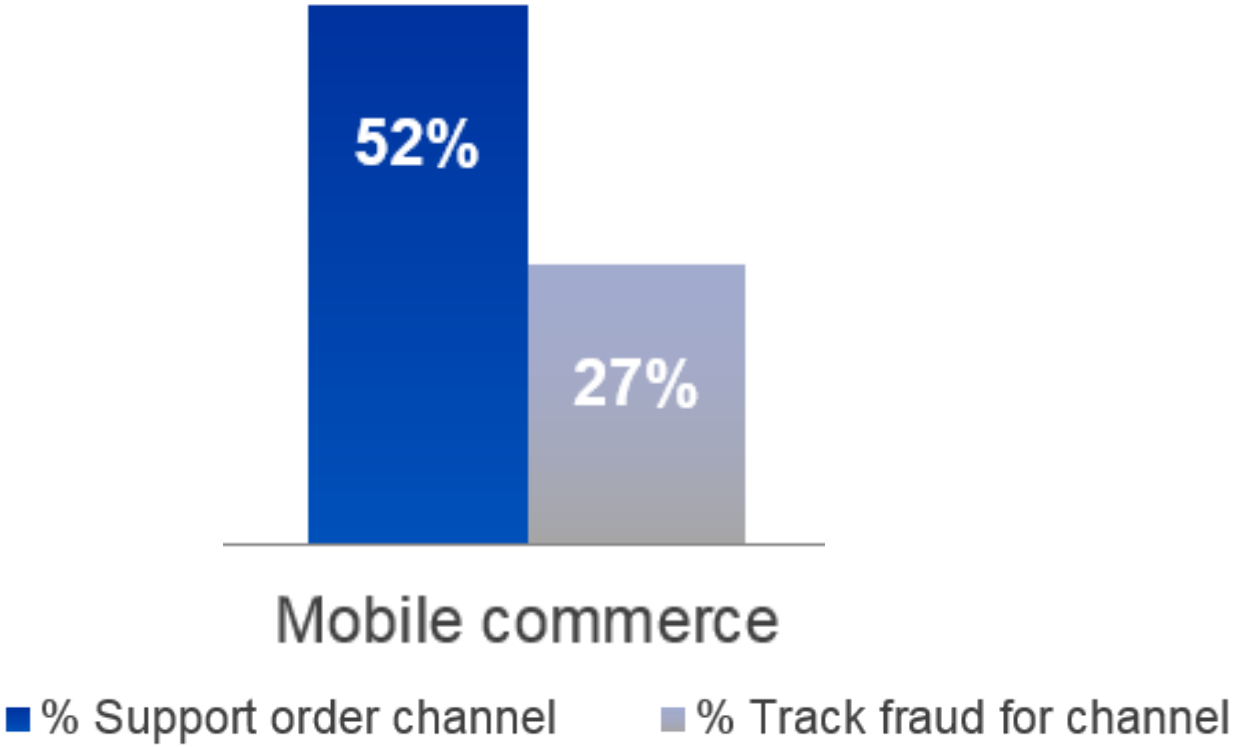


Source: CyberSource Online Fraud Management Benchmark Report, 2016

Visa Public

CyberSource®

Few merchants track mobile fraud



Source: CyberSource Online Fraud Management Benchmark Report, 2016

Visa Public

CyberSource®

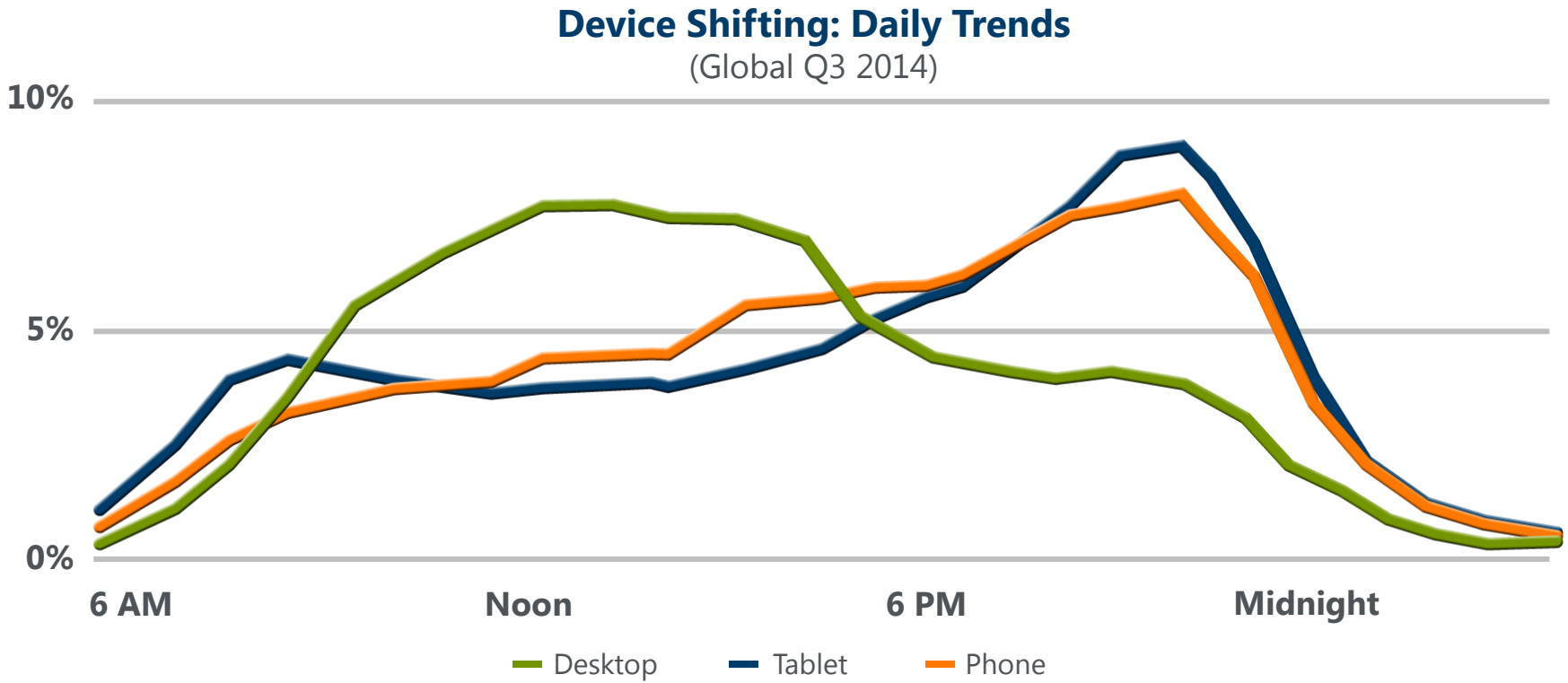
Is mCommerce any riskier?

	No	Yes
Customer/ preventions	• Omni present • Personal identification number (PIN) lock prevents access and usage • GPS to quickly locate and deactivate • Biometrics (Siri)	• Easier to steal • Customer apathy • New threats: Rogue apps, malware, "smishing" • Man-in-the-middle subverts SMS verification
Merchant/ mitigations	• New data elements to determine identity • Mobile network security more secure than WiFi • New validation methods (short message service (SMS))	• Variable internet protocol (IP) addresses and "diluted" digital fingerprint • App "fatigue" and privacy considerations • New customer behavior/norms/history

Visa Public

Device preferences throughout the day

Traditional fraud strategies need to be "tuned"



Source: OOYALA Global Video Index, Q3 2014 http://bit.ly/1KxEVkb

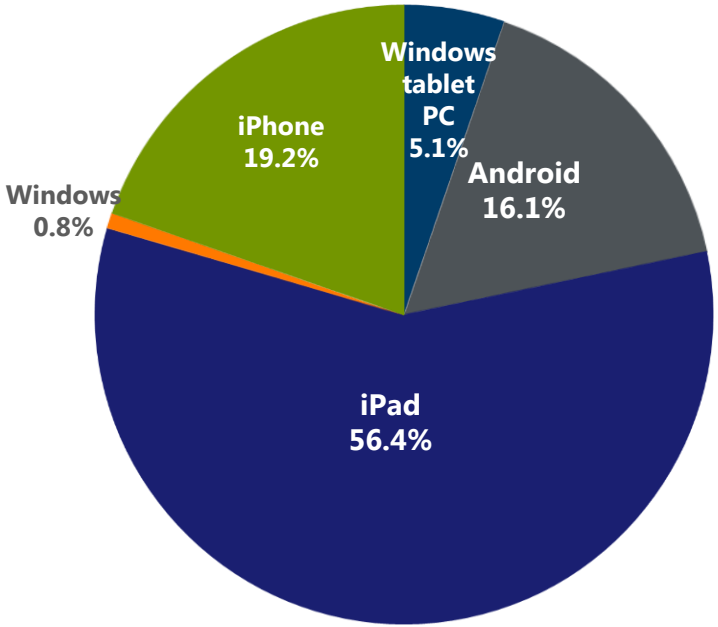
Visa Public

CyberSource®

What is a “mobile” transaction?

All devices are not created equal

Percentage of volume by device type



Fraud “pressure” by device type (fraud chargebacks + cancels)

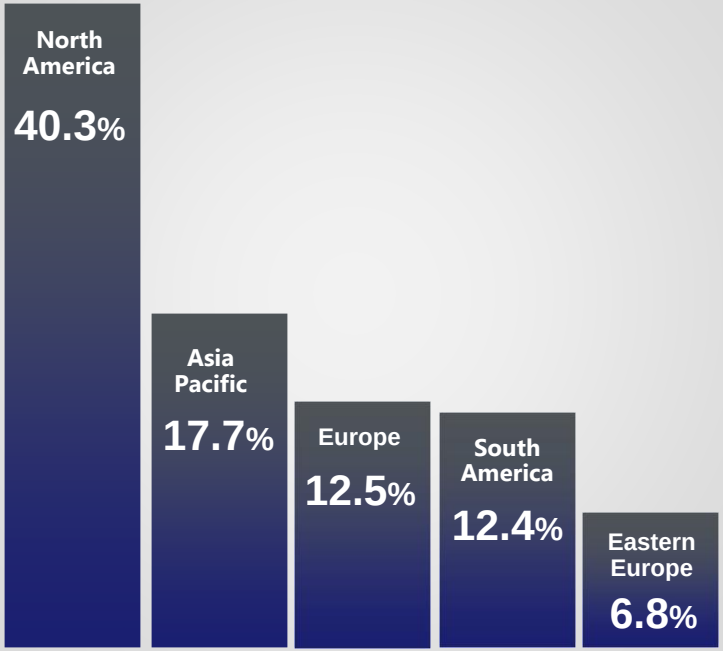
Source: Decision Manager, January – June 2015 Global credit card transactions for transactions where the device was identified

Visa Public

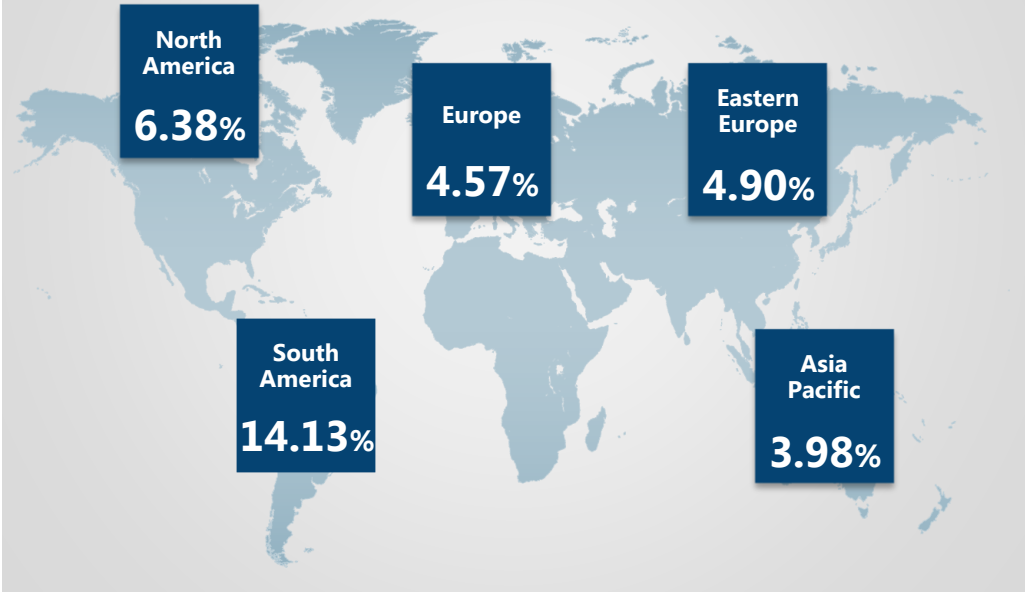
CyberSource®

Global view of mobile rates

Mobile volume as a % of total



Fraud "pressure" rates by revenue



Source: Decision Manager, January – June 2015, mobile phones only, Global credit card transactions

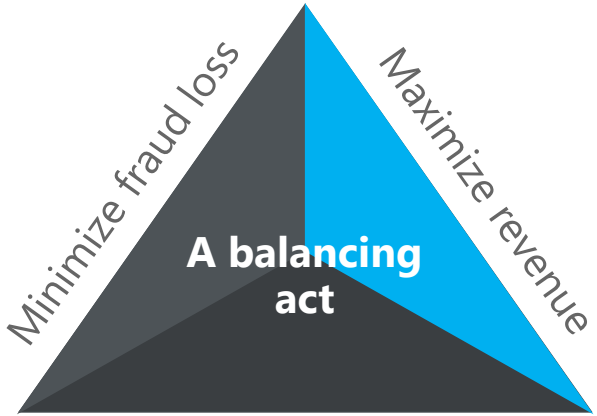
Visa Public

CyberSource®

Fraud management is a balancing act, including mobile

Accurate detection

- Reduce fraud rate
- Help minimize chargebacks



Positive customer experience

- Reduce false positives
- Increase acceptance rates
- Lower review rates

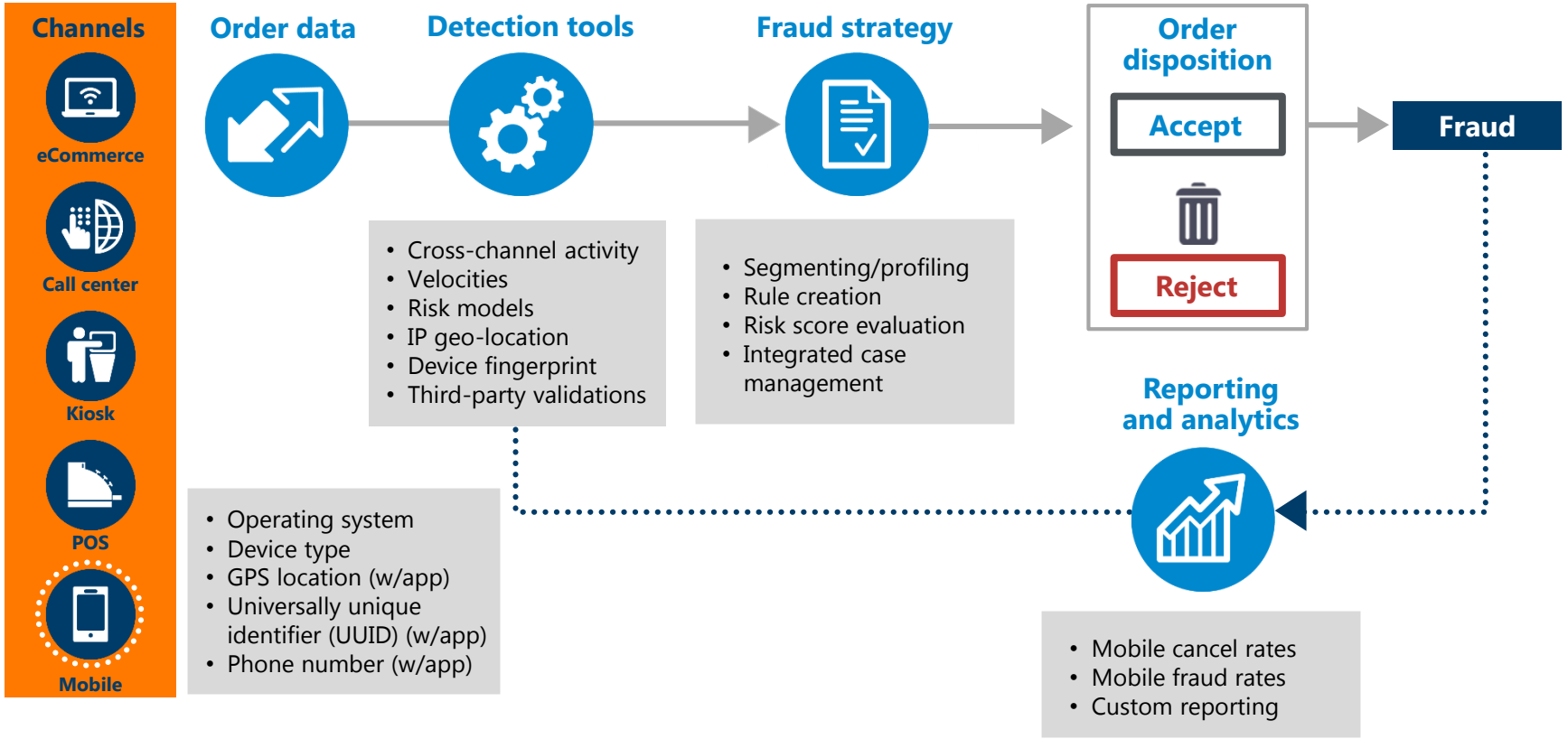
Efficiency

- Maximize automated decisioning
- Streamline review process

Visa Public

CyberSource®

Managing mobile fraud on your platform



Visa Public

CyberSource®

Strategy #1 - Mobile data

Traditional mobile browser vs. "apps"

	Browser	Apps

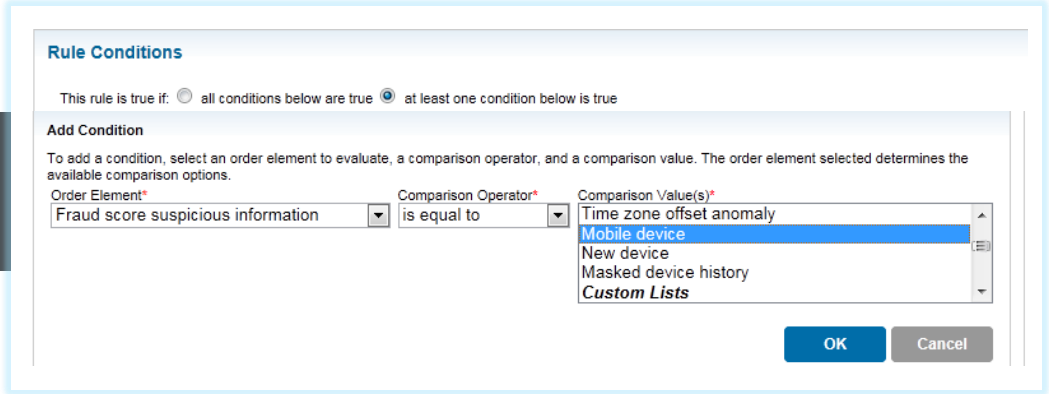
Pros	• New data elements
	  – Operating system (e.g., Windows, iOS)
	  – Device type (e.g., iPhone 4.0, Kindle)
	• Advancements in HTML5
	• Easier server-side updates
	• Does not require download
		• A more robust mobile experience
		• Great for repeat purchases (accounts)
		• Ideal for certain verticals (travel)
		• Collect more customized data
		  – Download ID
		  – UUID
		  – Phone numbers
		  – Install ID

Cons	• Variable IP geo-location (WiFi limited) • True device fingerprint (locked iOS) • Browser strings can be spoofed	• Proliferation of apps • More expensive to update and coordinate • Update fatigue • Privacy concerns

Visa Public

Strategy #2 - Identifying mobile device in your fraud management system

1 **Select "mobile device" identifier**



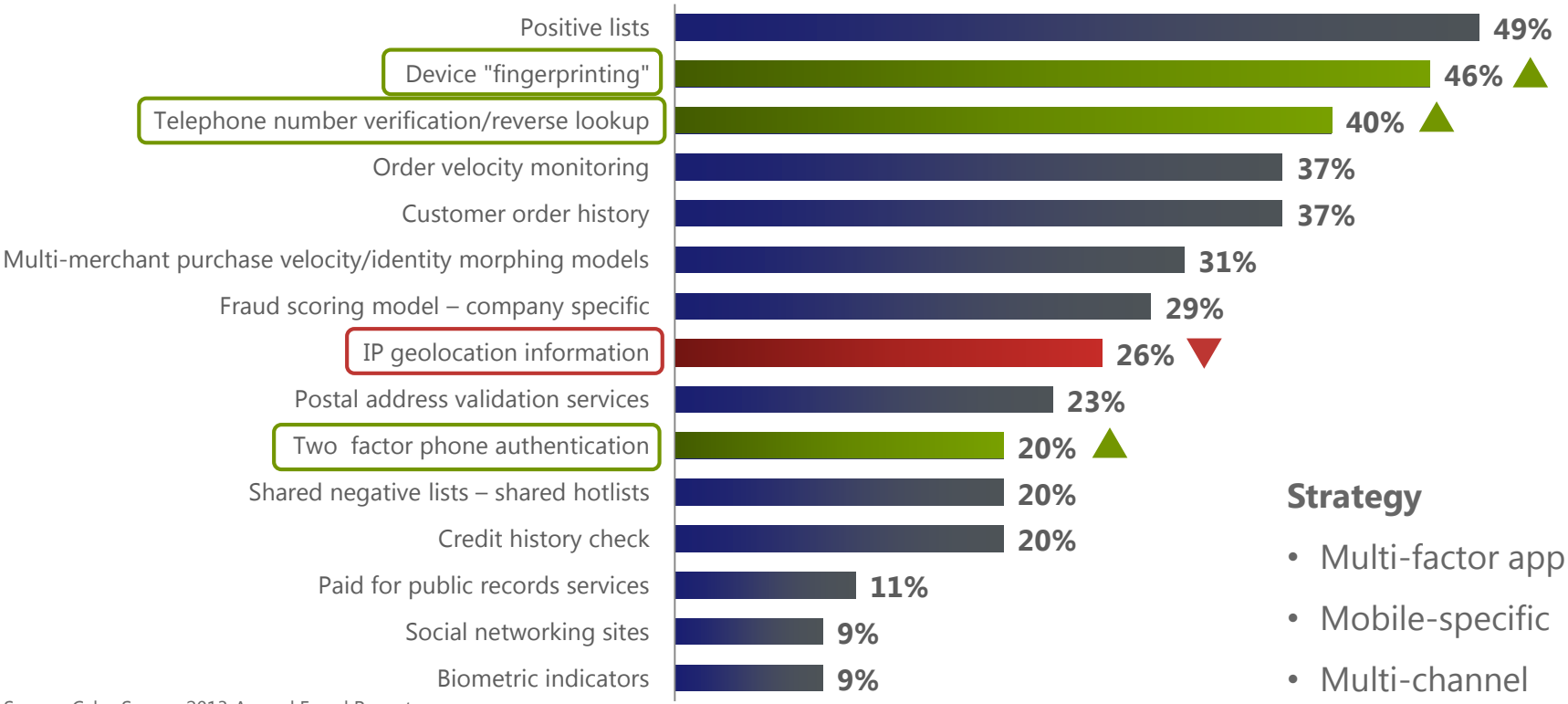
2 **Create custom data**

Visa Public

CyberSource®

Strategy #3 - Tool usage

Merchants tracking mobile fraud



Source: CyberSource 2013 Annual Fraud Report

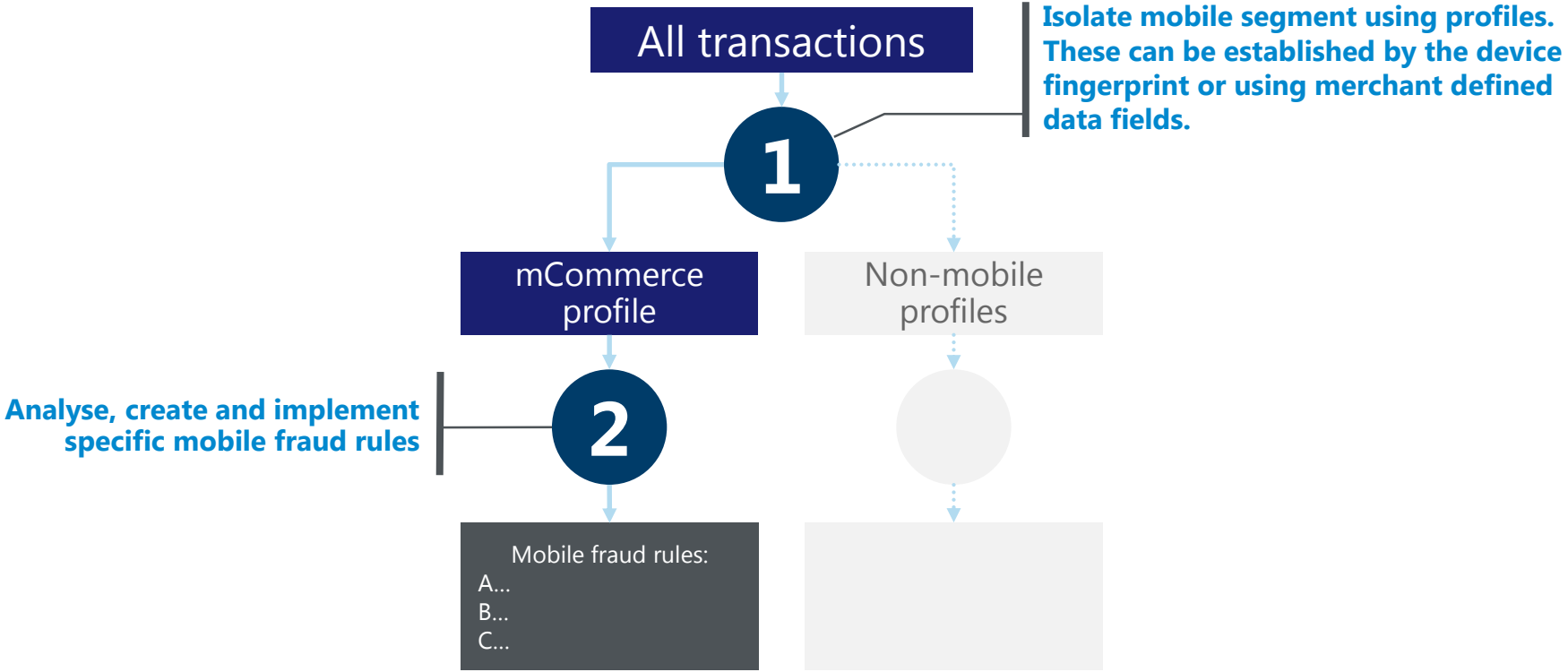
Strategy

- Multi-factor approach
- Mobile-specific
- Multi-channel

Visa Public

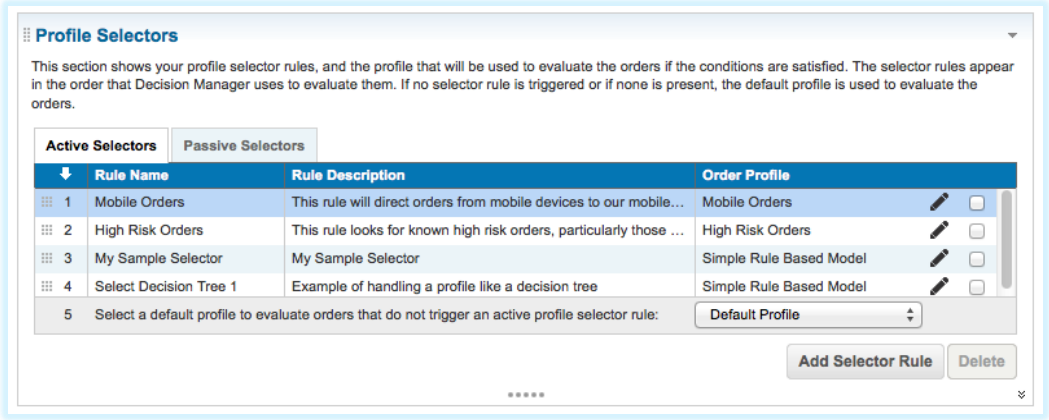
CyberSource®

Strategy #4 - Mobile fraud strategy



Visa Public

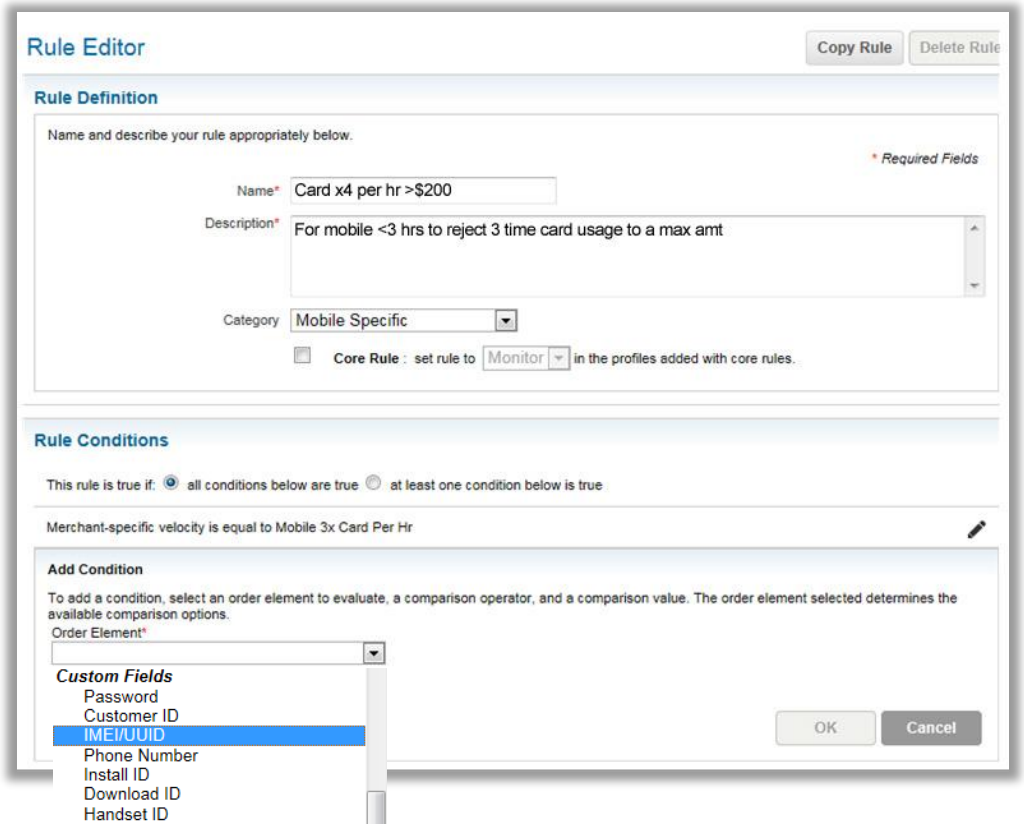
Strategy #4 - Mobile fraud strategy



Visa Public

CyberSource®

Strategy #4 - Mobile fraud strategy

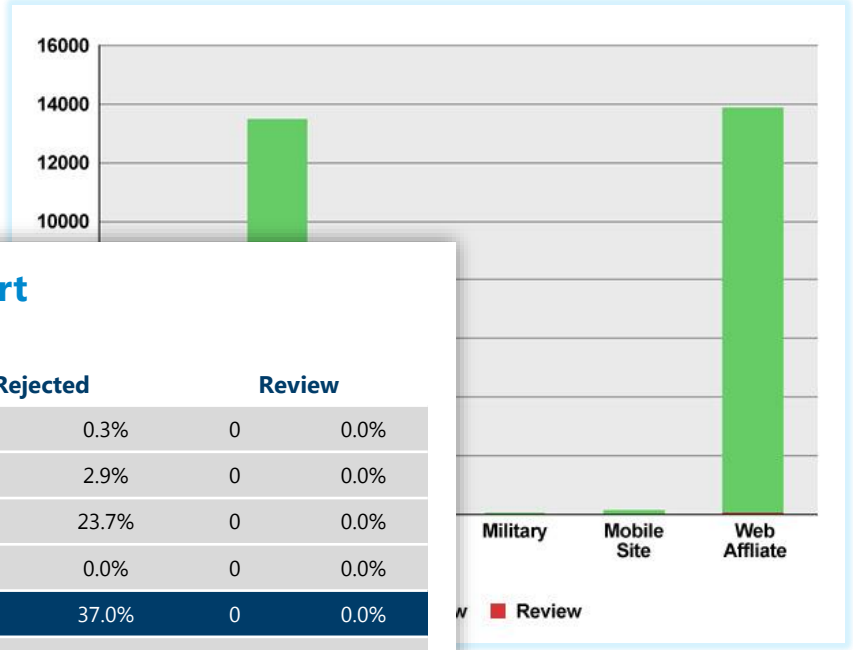


Visa Public

Strategy #5 - Mobile reporting

Profile reports

Summary comparison of profiles



Profile performance comparison report

Results: Date: March 01, 2013 – March 31, 2013 | Merchant(s)

Active profiles	Total transactions		Accepted		Rejected		Review	
Call center	**8,431**	21.2%	**8,402**	99.7%	**29**	0.3%	0	0.0%
Electronic web public	**13,459**	33.8%	**13,075**	97.1%	**384**	2.9%	0	0.0%
Web Canada	**19,77**	5.0%	**1,509**	76.3%	**468**	23.7%	0	0.0%
Military	**18**	0.0%	**18**	100.0%	0	0.0%	0	0.0%
Mobile site	**108**	0.3%	**68**	63.0%	**40**	37.0%	0	0.0%
Web affiliate	**13,878**	34.8%	**13,824**	99.6%	**54**	0.4%	0	0.0%

All rights reserved CyberSource® 2016

Visa Public

CyberSource®

Mobile reporting

Mobile profile detail (continued)

Profile performance comparison report

Results: Date: March 01, 2013 – March 31, 2013 | Merchant(s)

Active profiles	Transactions	Accepted		Force accepted		Rejected		Review		Accepted	Rejected	MAS
Totals	39,845	24,532	61.57%	14,338	35.98%	975	2.45%	0	0.00%	38,870	975	307
Profiles												
Call center	8,431	4,810	12.07%	3,592	9.01%	29	0.70%	0	0.00%	8,402	29	4
Electronic web public	13,459	9,802	24.60%	3,273	8.21%	384	0.96%	0	0.00%	13,075	384	81
Web Canada	1,977	1,488	3.73%	21	0.05%	468	1.17%	0	0.00%	1,509	468	189
Military	18	15	0.04%	3	0.01%	0	0.00%	0	0.00%	18	0	0
▼Mobile Site	108	50	0.13%	18	0.05%	40	0.10%	0	0.00%	68	40	29
Rules	**Transactions**	**Accepted**		**Force accepted**		**Rejected**		**Review**		**Accepted**	**Rejected**	**MAS**
None												
AVS service is not available												6
Account issued outside of billing country												27
BCountry =/= BIN Country: CA						1	0.93%					1

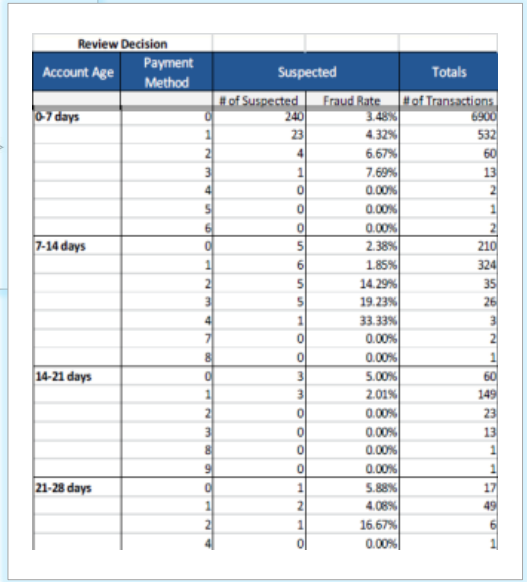
All rights reserved Copyright CyberSource® 2016

Visa Public

CyberSource®

Mobile reporting

Ad hoc analysis



Review Decision

Account Age	Payment Method	Suspected		Totals
		# of Suspected	Fraud Rate	# of Transactions
0-7 days	0	240	3.48%	6900
	1	23	4.32%	532
	2	4	6.67%	60
	3	1	7.69%	13
	4	0	0.00%	2
	5	0	0.00%	1
	6	0	0.00%	2
7-14 days	0	5	2.38%	210
	1	6	1.85%	324
	2	5	14.29%	35
	3	5	19.23%	26
	4	1	33.33%	3
	7	0	0.00%	2
	8	0	0.00%	1
14-21 days	0	3	5.00%	60
	1	3	2.01%	149
	2	0	0.00%	23
	3	0	0.00%	13
	8	0	0.00%	1
	9	0	0.00%	1
21-28 days	0	1	5.88%	17
	1	2	4.08%	49
	2	1	16.67%	6
	4	0	0.00%	1

All rights reserved CyberSource® 2013

Visa Public

CyberSource®

Strategy #5 – Fraud management tools

Device fingerprinting specialized for mobile

- Additional mobile data fields for rule building and reporting
- Support iOS and Android software development kits (SDKs)

Data for authentication

- IP address
- Browser fingerprint data
- Location ID
- Dynamic ID
- Persistent ID
- Device fingerprint
  - 1,000+ inputs

Data for security and fraud

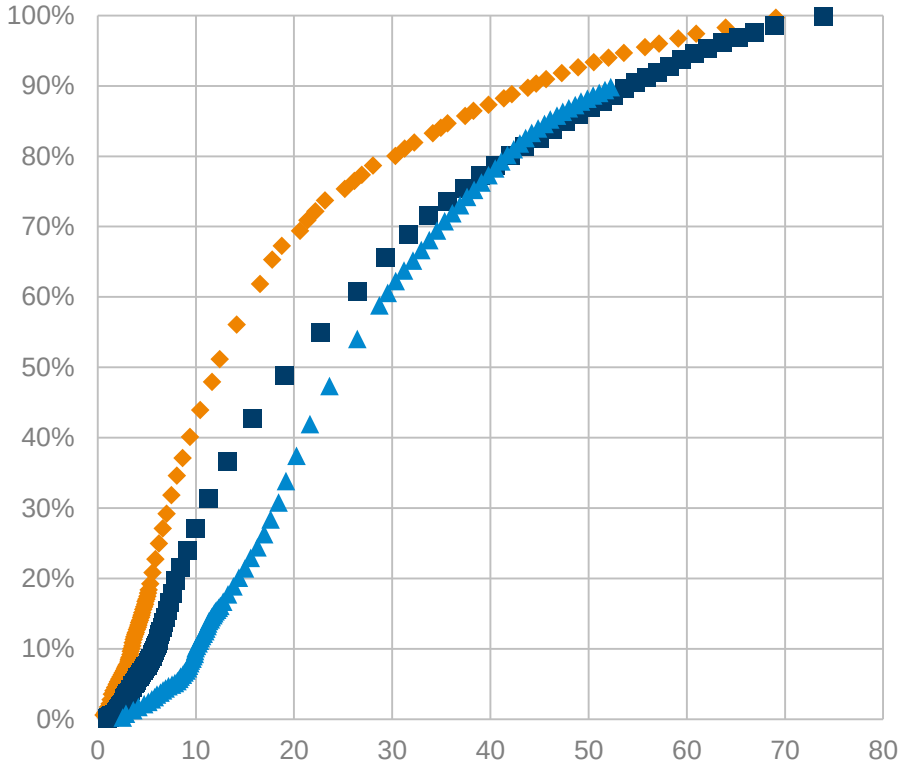
- Root detection
- Crime ware detect
- Malware detect
- Location anomaly
- Device languages

Visa Public

Fraud management tools

Mobile risk models for greater accuracy

- Built specifically for mobile channel using historical transaction data
- Requires sufficient transaction information and “truth” data
- Will further segment into additional regions/verticals as warranted



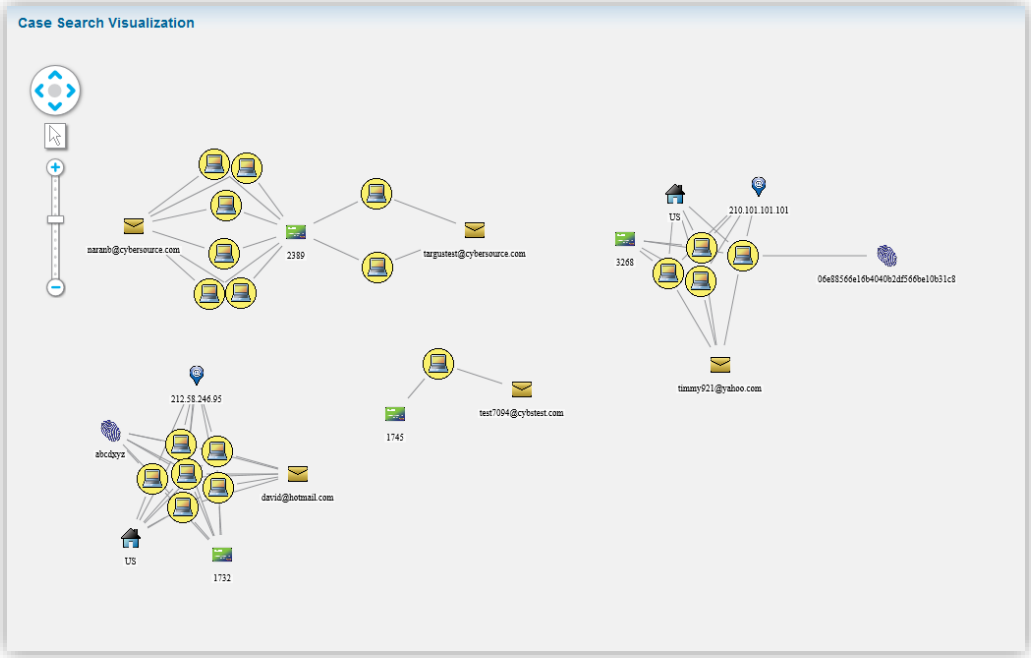
Visa Public

CyberSource®

Fraud management tools

Visual Link Analysis for Case Management

- Find common data linkages across transactions (including mobile device fingerprints)
- Drill down each linkage to transaction level detail
- Select multiple transactions with click through disposition from visual map



Visa Public

CyberSource®

Summary

- Rapid mCommerce growth but also increasing mobile fraud “pressure”
- Supplement traditional fraud-prevention data points, tools, and rules for mobile
- Tune fraud strategies specifically for mCommerce
- Incorporate mobile as part of overall cross-channel monitoring
- Remain flexible and vigilant to anticipate fraud behavior

Visa Public

Resources

Upcoming Webinars – Training page on www.visa.com/cisp

- September 28, 2016: Effectively Managing Account Data Breaches

Visa Data Security Website – www.visa.com/cisp

- Alerts, Bulletins
- Best Practices, White Papers
- Webinar Presentations

PCI Security Standards Council Website – www.pcissc.org

- Data Security Standards – PCI DSS, PA-DSS, P2PE, and PTS
- Programs – QSA, ASV, PA-QSA, PFI, ISA, PCIP, and QIR
- Fact Sheets – ATM Security, Mobile Payments Acceptance, Tokenization, Cloud Computing, and many more…

Questions?

Visa Public