Webinar:
Preventing Card-Not-Present Fraud

Gord Jamieson, *Risk Services*
Andrew McGloin, *Risk Services*
David Richey, *Risk & Auth Products*

8 December 2016

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.

Copyright

Forward-looking statements and disclaimer

This presentation may contain forward-looking statements within the meaning of the U.S. Private Securities Litigation Reform Act of 1995. These statements can be identified by the terms “objective,” “goal,” “strategy,” “opportunities,” “continue," “can,” "will,” and other similar references to the future. Examples of such forward-looking statements may include, but are not limited to, statements we make about our corporate strategy and product goals, plans, and objectives. By their nature, forward-looking statements: (i) speak only as of the date they are made, (ii) are neither statements of historical fact nor guarantees of future performance, and (iii) are subject to risks, uncertainties, assumptions, and changes in circumstances that are difficult to predict or quantify. Therefore, actual results could differ materially and adversely from those forward-looking statements for a variety of reasons, including macroeconomic and industry factors such as currency exchange rates, global economic, political, health and other conditions, competitive pressure on customer pricing and in the payments industry generally, and material changes in our customers' performance compared to our estimates; systemic developments such as disruption of our transaction processing systems or the inability to process transactions efficiently, account data breaches involving card data stored by us or third parties, and increased fraudulent and other illegal activity involving our cards; and other factors discussed under the heading "Risk Factors” in our most recent Annual Report on Form 10-K and our most recent Quarterly Reports on Form 10-Q. You should not place undue reliance on such statements. Unless required to do so by law, we do not intend to update or revise any forward-looking statement because of new information or future developments or otherwise.

Studies, survey results, research, recommendations, and opportunity assessments are provided for informational purposes only and should not be relied upon for marketing, legal, regulatory, or other advice. Recommendations and opportunities should be independently evaluated in light of your specific business needs and any applicable laws and regulations. Visa is not responsible for your use of any studies, survey results, research, recommendations, opportunity assessments, or other information, including errors of any kind, or any assumptions or conclusions you might draw from their use. Except where statistically significant differences are specifically noted, survey results should be considered directional only.

Agenda

- E-Commerce Landscape and Fraud Trends
- Visa's CNP strategy
- Effective Merchant Fraud Management Strategy
- Common Flags for CNP Fraud
- Visa Merchant Purchase Inquiry

E-Commerce Landscape and Fraud Trends

Why are we talking about CNP?

$3.5T

GLOBAL ECOMMERCE SALES WILL DOUBLE FROM 2015 TO 2019

$1.7T

Increasing share of total retail spending from 7.3% to 12.4%

Source: eMarketer July 2015, includes online and mobile ecommerce

Challenge: we expect CNP fraud to continue to outpace sales in the channel as markets migrate to EMV Chip

CNP Landscape: Trends and Drivers

Trends

Rapid channel growth

Double digit YoY growth rates for the last 5 years (13% for YE Q2 2016)

Disproportionate fraud relative to channel

CNP accounts for 52% of US domestic total fraud but is only 40% of total sales volume*

New Players, Products & Services

Pay

iTunes

Google

Check out with PayPal

pay

Drivers

Multiple authentication solutions

Proprietary (Fraud Models, Biometrics, Devices) Vs. Industry (3DS, Payment Tokens, EMVCo)

Increased regulatory attention

Regulation: USA, European Banking Authority, India, South Africa, Korea, etc.

Stakeholders want frictionless commerce

Visa Consumer Authentication Service

Verified by VISA

Need to change our *Reliance* on static authentication data

(Three digit Code, Address Verification Service)

Legacy policies and rules

(Chargeback Rules, Acceptance Risk Programs)

Source: EBI, FPB, 04/30/2013

*Based on VisaNet transactions only, includes eCommerce & MOTO for YE June 2016

All brand names and logos are the property of their owners and are used in this presentation for identification purposes only, and do not imply product endorsement.

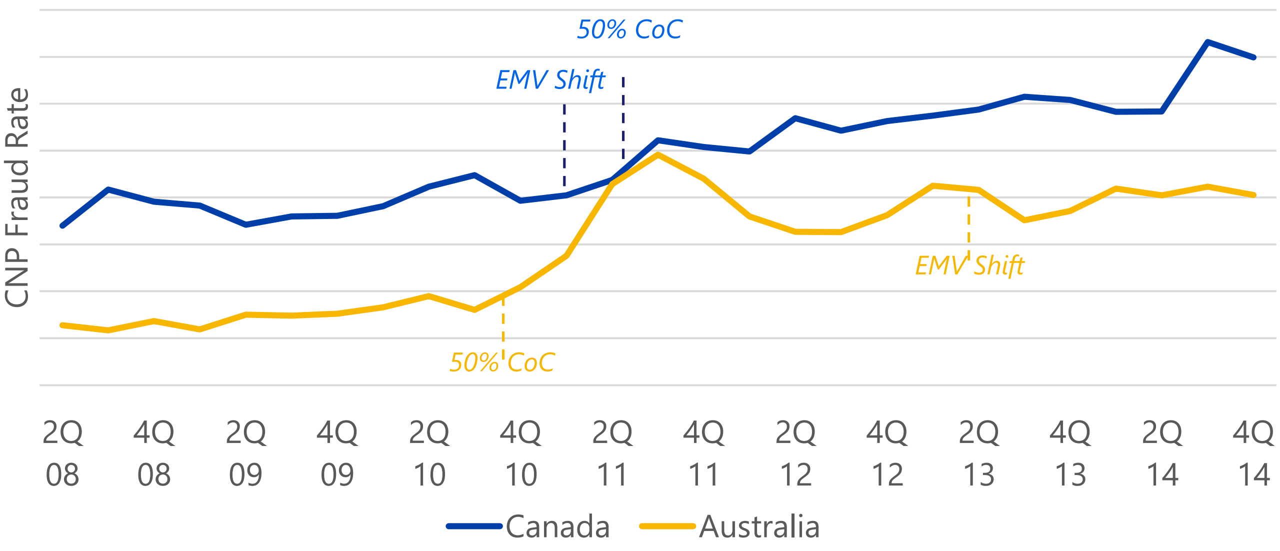
Historic CNP Fraud Rates

US CNP fraud is expected to change similar to experiences in other markets

- When chip-on-chip rates hit a breaking point of approximately 50%, fraudsters shift away from EMV terminals to the CNP channel.

- One year after 50% chip-on-chip, Canada and Australia saw CNP fraud rates increase by 30.1% and 126.1% respectively.

Australian and Canadian CNP Fraud Rates



Visa’s CNP Strategy

VISA

Visa's strategy to address CNP fraud : Smarter security through risk based and dynamic authentication

1.

Devalue Payment Data

Make sensitive data useless through stronger technology

2.

Eliminate Transaction Friction

Improve the exchange of information

3.

Reduce Fraud

Enhance predictive analytics and modeling

Objectives in Addressing Risk

An Interconnected Approach to Balancing Risk, Convenience, and Investment

Devalue Payment Data

Chip Cards

Encryption

Tokens

Reduce Cost of Fraud

Geo-Location

Alerts

Visa Transaction Advisor (VTA)

Device Level Authentication

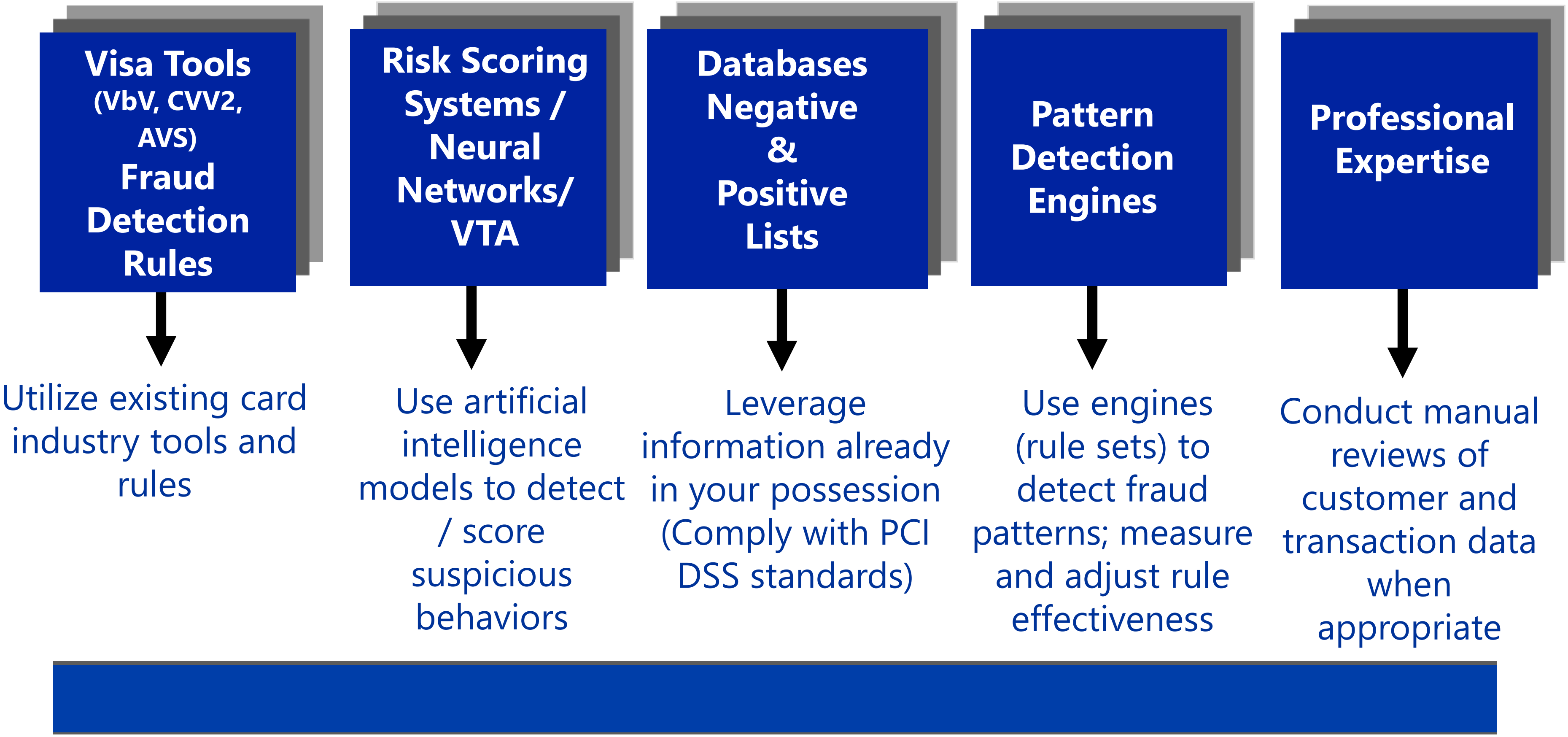
Eliminate Transaction Friction

VCAS

Visa Checkout

Effective Fraud Management Strategy

Effective fraud management requires a layered security strategy



Visa Tools
(VbV, CVV2, AVS)
Fraud Detection Rules

Utilize existing card industry tools and rules

Risk Scoring Systems / Neural Networks/ VTA

Use artificial intelligence models to detect / score suspicious behaviors

Databases Negative & Positive Lists

Leverage information already in your possession (Comply with PCI DSS standards)

Pattern Detection Engines

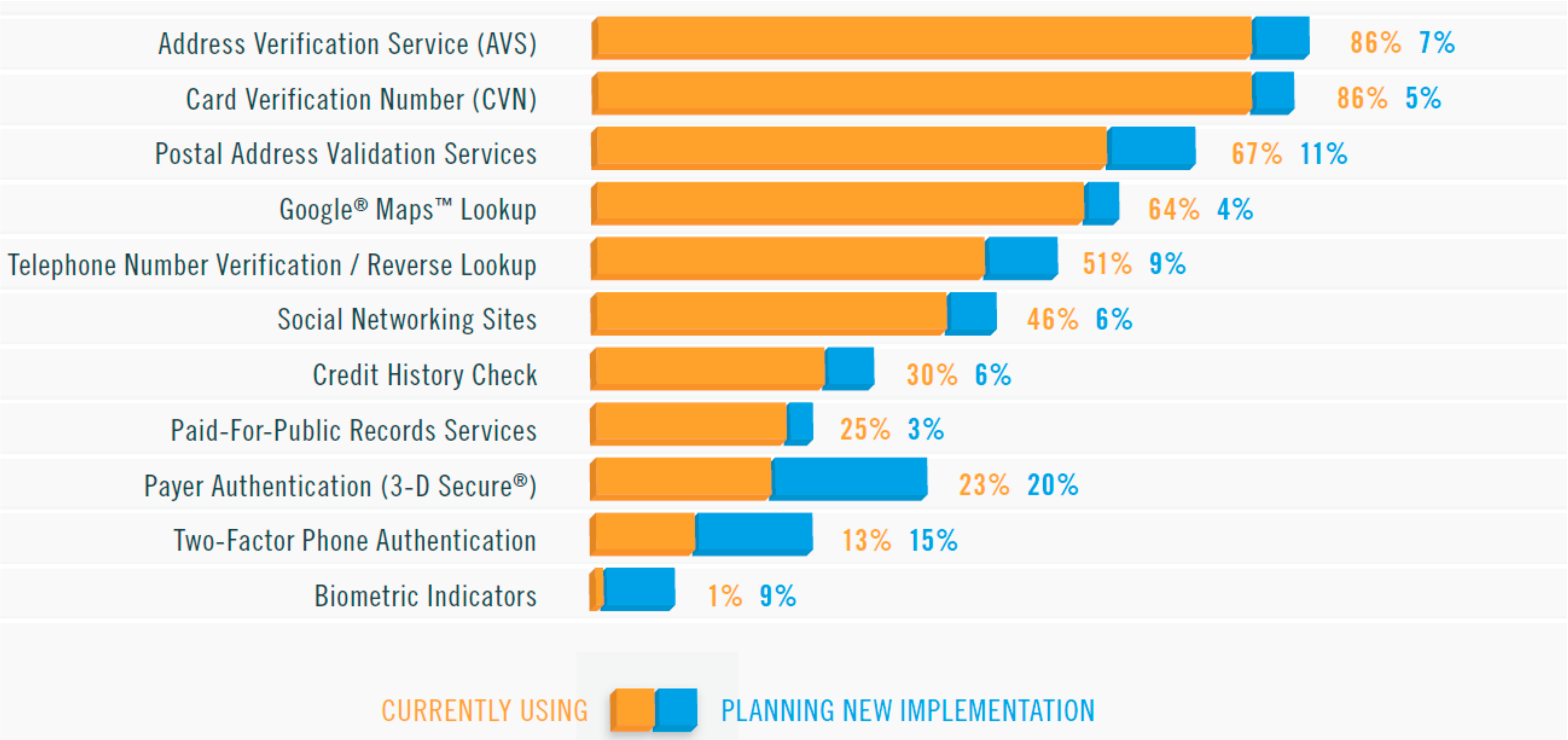
Use engines (rule sets) to detect fraud patterns; measure and adjust rule effectiveness

Professional Expertise

Conduct manual reviews of customer and transaction data when appropriate

Effectiveness Against Fraud

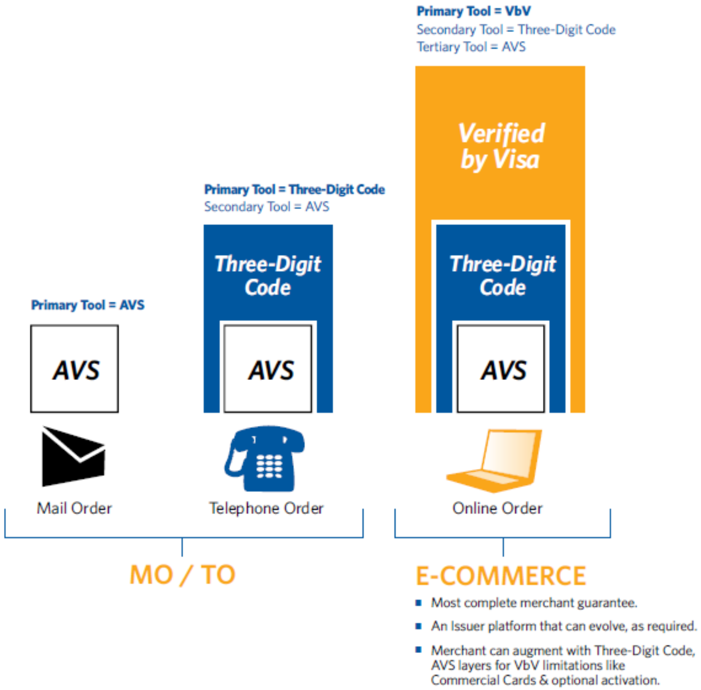
Automated Screening: most adopted fraud tool



Source: CyberSource Online Fraud Management Benchmark Report, 2016 http://forms.cybersource.com/LP=1248

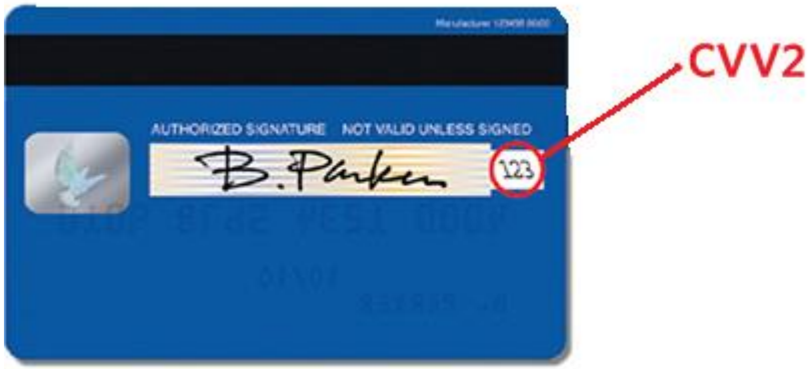
Card Not Present Fraud Tools

Whether you conduct your business by mail order, phone or over the Internet, Visa offers layers of protection.


Primary Tool = VbV
Secondary Tool = Three-Digit Code
Tertiary Tool = AVS
Verified by Visa
Primary Tool = Three-Digit Code
Secondary Tool = AVS
Three-Digit Code
Three-Digit Code
Primary Tool = AVS
AVS
AVS
AVS
Mail Order
Telephone Order
Online Order
MO / TO
E-COMMERCE
Most complete merchant guarantee.
An Issuer platform that can evolve, as required.
Merchant can augment with Three-Digit Code, AVS layers for VbV limitations like Commercial Cards & optional activation.

- Merchants who support CNP transactions can reduce their exposure to fraudulent transactions through an effective combination of Visa tools and acceptance procedures
- Use the CVV2 and AVS response codes correctly
- Consider additional checks or screening for ‘no match’ responses

Card Verification Value 2 (CVV2)



- The Card Verification Value 2 (CVV2)* is a three-digit security number printed on the back of Visa cards to help validate that a customer is in possession of the card at the time of an order.

- These numbers are used to help merchants validate that the customer has a genuine card in his or her possession during an Internet or Telephone Order transaction

Studies show that merchants who include CVV2 validation in their authorization procedures for card-absent transactions can reduce their fraud-related chargebacks, and should use CVV2 as a fraud reduction tool.

Address Verification Service (AVS)

- Use AVS to verify the cardholder billing address
  - Confirm the order information
  - Ask the customer for the billing address (street address and/or postal code) for the card being used

- Evaluate the AVS response code and take appropriate action based on all transaction characteristics and any other verification information received with the authorization (i.e., expiration date, CVV2, etc.).

- Do not accept any transaction that has been declined, regardless of the AVS response.

Improving CNP with enhanced data exchange

Enhancing risk-based analytics

Additional data points available

Improving the checkout experience

No step up authentication and more integrated into the purchase environment

Expanding data exchange

In-app and non-payment related uses
(i.e., account provisioning)

3D Secure improvements

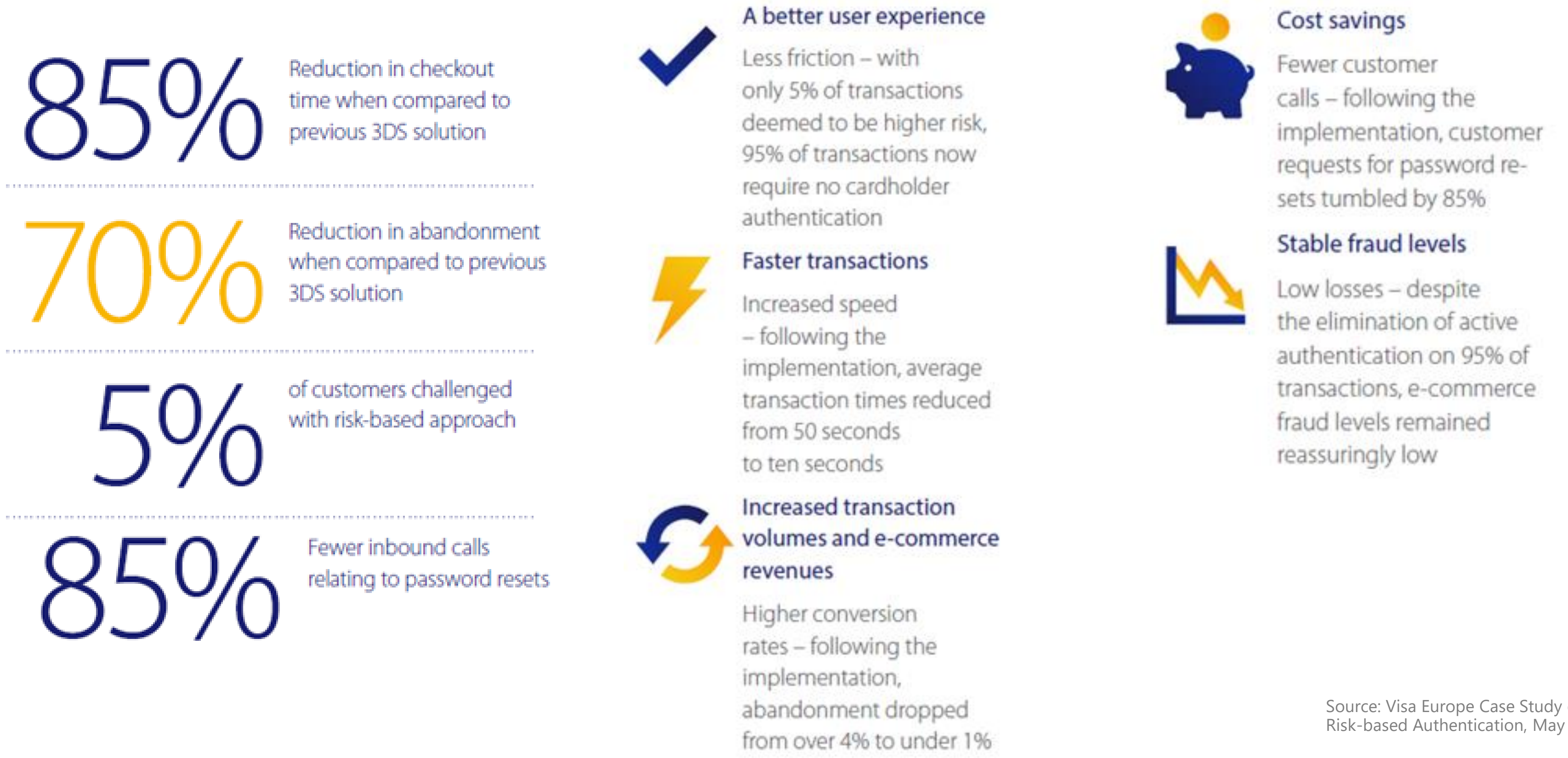
3DS 2.0 protocol enhances issuer risk-based authentication capabilities and improves the user experience across multiple form factors and use cases

Improved User Experience	3-D Secure 1.0	3-D Secure 2.0
▪ Capable of integration with the merchant experience	✓ limited	✓ expanded
▪ Removal of Activation During Shopping		✓
▪ Reduce the number of messages required		✓

Flexible Device and Channel Support	3-D Secure 1.0	3-D Secure 2.0
▪ Browser-based authentication support	✓	✓
▪ Mobile/application-based authentication support		✓
▪ Digital Wallet, Non-payment-based authentication		✓

More Data for Authentication and Security	3-D Secure 1.0	3-D Secure 2.0
▪ Payment-related data	✓ limited	✓ expanded
▪ Non-payment related data		✓
▪ Support for new and future authentication methods		✓

The Benefits of Risk-based Authentication



85% Reduction in checkout time when compared to previous 3DS solution

70% Reduction in abandonment when compared to previous 3DS solution

5% of customers challenged with risk-based approach

85% Fewer inbound calls relating to password resets

A better user experience

Less friction – with only 5% of transactions deemed to be higher risk, 95% of transactions now require no cardholder authentication

Faster transactions

Increased speed – following the implementation, average transaction times reduced from 50 seconds to ten seconds

Increased transaction volumes and e-commerce revenues

Higher conversion rates – following the implementation, abandonment dropped from over 4% to under 1%

Cost savings

Fewer customer calls – following the implementation, customer requests for password re-sets tumbled by 85%

Stable fraud levels

Low losses – despite the elimination of active authentication on 95% of transactions, e-commerce fraud levels remained reassuringly low

Source: Visa Europe Case Study on Risk-based Authentication, May 2016

Risk Scoring and Neural Networks

Helps minimize fraud losses, maximize revenue and minimize operational costs

- Allows businesses to customize rules and models to your specific business, across all sales channels, including web, mobile, call center, and kiosks
- Confidently quantify fraud strategies in real time prior to activating in the live production environment
- Quickly test various ‘what-if’ rules profiles against historical data rather than wait months to understand the impact of any fraud changes

Number of third-party vendors that can provide such services to merchants such as:

- CyberSource
- Kount
- Acertify

Using a Positive Database

Build a comprehensive database of “positive-list” customers

- Encourage use of customer registration programs
  - Promote rewards programs for customers that ‘sign in’
  - Creates opportunity to increase customer satisfaction
- Limit or reduce fraud screening for regular ‘positive list’ customers to avoid unnecessary delays / expenses
- Securely store all data in compliance with PCI Data Security Standards*
  - Avoid storing data that is no longer required

* The laws relevant to the definition, collection, storage and use of personal information may vary by jurisdiction and should be completed in accordance with applicable law. Card account numbers and other sensitive elements must be handled in accordance with the PCI DSS and, if stored truncated or encrypted.

Using a Negative Database

Utilize a negative database to reduce the impact of fraudulent transactions

- Maintain key attributes of previously identified fraudulent transactions
- Include data from fraud and chargeback reports
- Flag transactions for further review or ‘decline’ where appropriate
- Consider at least the minimum following attributes:

1. IP Address
2. Cardholder Name
3. E-mail Address
4. Phone Number
5. Shipping Address

* The laws relevant to the definition, collection, storage and use of personal information may vary by jurisdiction and should be completed in accordance with applicable law. Card account numbers and other sensitive elements must be handled in accordance with the PCI DSS and, if stored truncated or encrypted.

Professional Expertise

- Establish a formal fraud control function
- Perform internal fraud screening
- Establish procedures for responding to suspicious transactions and dollar thresholds
- Track fraud control performance and adjust fraud tools
- Train your employees to have a thorough understanding of fraud risk, chargebacks, rules and your risk management policies and procedures.
- Work with your acquirer to ensure you are using all the necessary tools

Common Red Flags for Card Not Present Fraud

Common ‘Red Flags’ for Card Not Present (CNP) Fraud

Product / Order Flags

- Larger-than-normal orders
- Multiple orders for the same product
- Multiple cards used for a single purchase
- Orders for products readily convertible to cash (gift cards)
- Orders made up of “big-ticket” items

Delivery Flags

- Customer requests “rush” or “overnight” delivery
- Single card used with multiple shipping addresses
- Delivery to an international address
- Billing address different than shipping address

Customer Flags

- Orders have different names, addresses, and card numbers, but from a single IP address
- Internet addresses at free e-mail services
- Multiple transactions on a single card over a short time period
- First time customer and the order does not fit the “average” customer purchase pattern

What You Should Know About CNP Fraud

There is no “silver bullet” to effectively managing CNP fraud

- Fraudsters take full advantage of the anonymity of the Internet
- An authorization is not proof that the true cardholder is making the purchase. More is needed to detect fraud.
- Effective fraud management requires a layered security strategy
- Continuously track and analyze fraud trends. Modify risk controls and acceptance procedures accordingly.
- Regularly measure your performance to ensure your strategy is effective

Fraud can affect an internet merchant’s bottom line – a merchant can be held financially responsible for fraud even if the transaction was approved

Visa Merchant Purchase Inquiry (VMPI)

Solution Overview

Background

Consumer complaints that lead to disputed transactions are reactive today, causing significant overhead and cost for all participants in the payment chain

Current Landscape

- Today, acquirers/merchants are *reacting* to financial claims filed by cardholders/issuers
- 45 days to provide compelling evidence to support existing charge
- Limited ways to encourage “proactive” contact by issuers, acquirers or merchants
- Impact can be severe for cardholder experience and consumer confidence

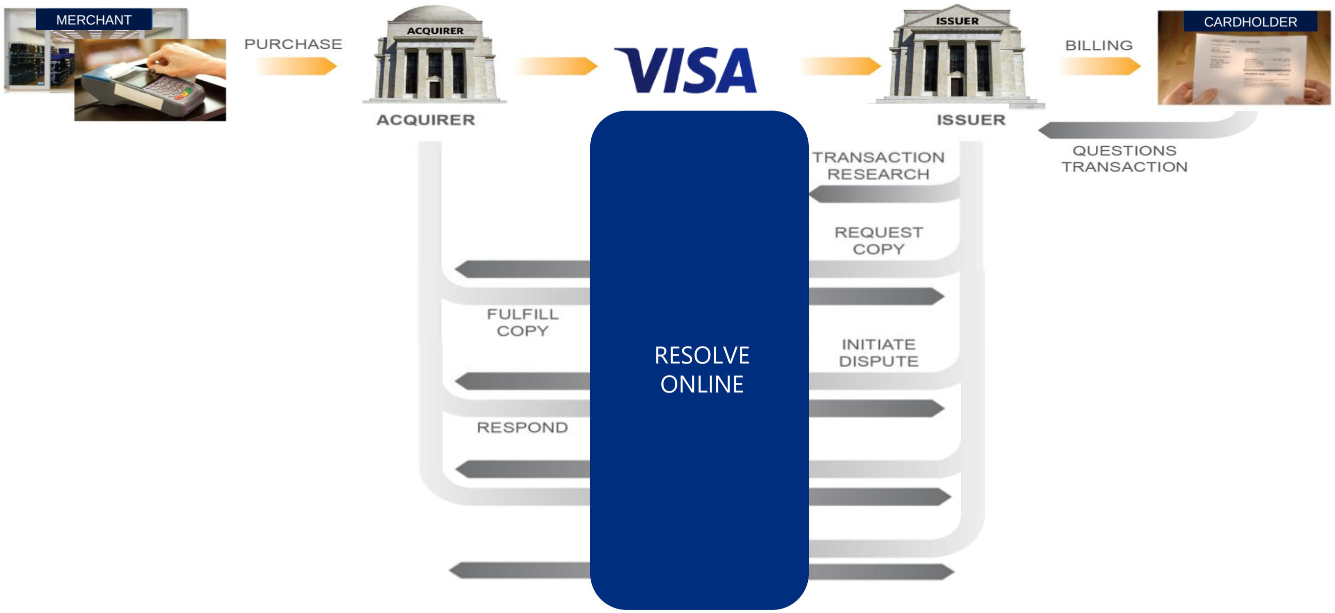
Key Reasons for Consumer Complaints

“I did not make this purchase, it must be fraud.”

“I am not sure if I made this purchase because I don’t recognize it.”

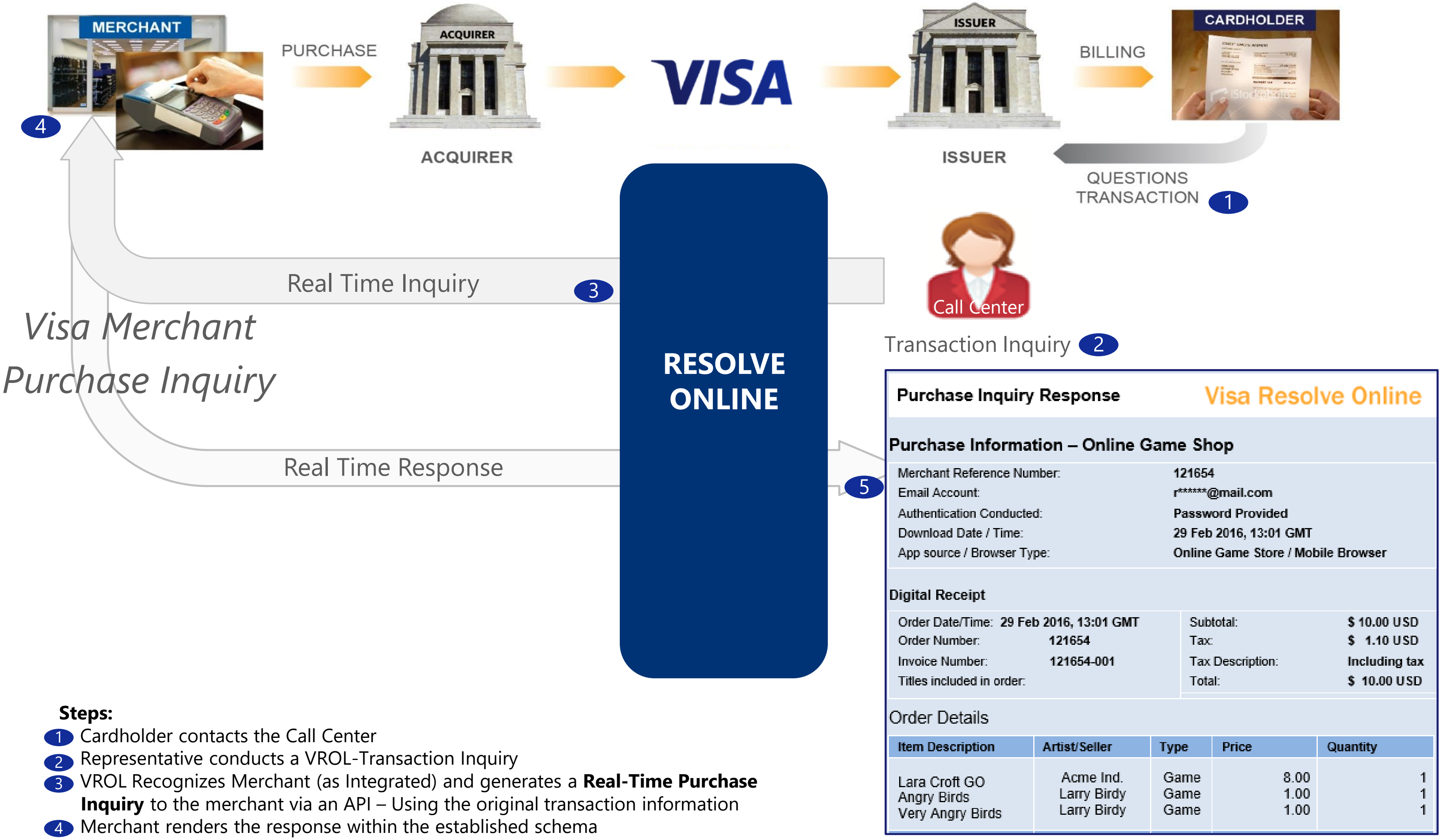
“I made this purchase, but there’s a problem.”

Existing Dispute Process Flow



Visa Merchant Purchase Inquiry – Digital Goods

Merchants are able to satisfy the cardholder queries through providing information at the point of escalation to the Issuer



Purchase Inquiry Response Visa Resolve Online

Purchase Information – Online Game Shop

Merchant Reference Number:	121654
Email Account:	r******@mail.com
Authentication Conducted:	Password Provided
Download Date / Time:	29 Feb 2016, 13:01 GMT
App source / Browser Type:	Online Game Store / Mobile Browser

Digital Receipt

Order Date/Time:	29 Feb 2016, 13:01 GMT	Subtotal:	$ 10.00 USD
Order Number:	121654	Tax:	$ 1.10 USD
Invoice Number:	121654-001	Tax Description:	Including tax
Titles included in order:		Total:	$ 10.00 USD

Order Details

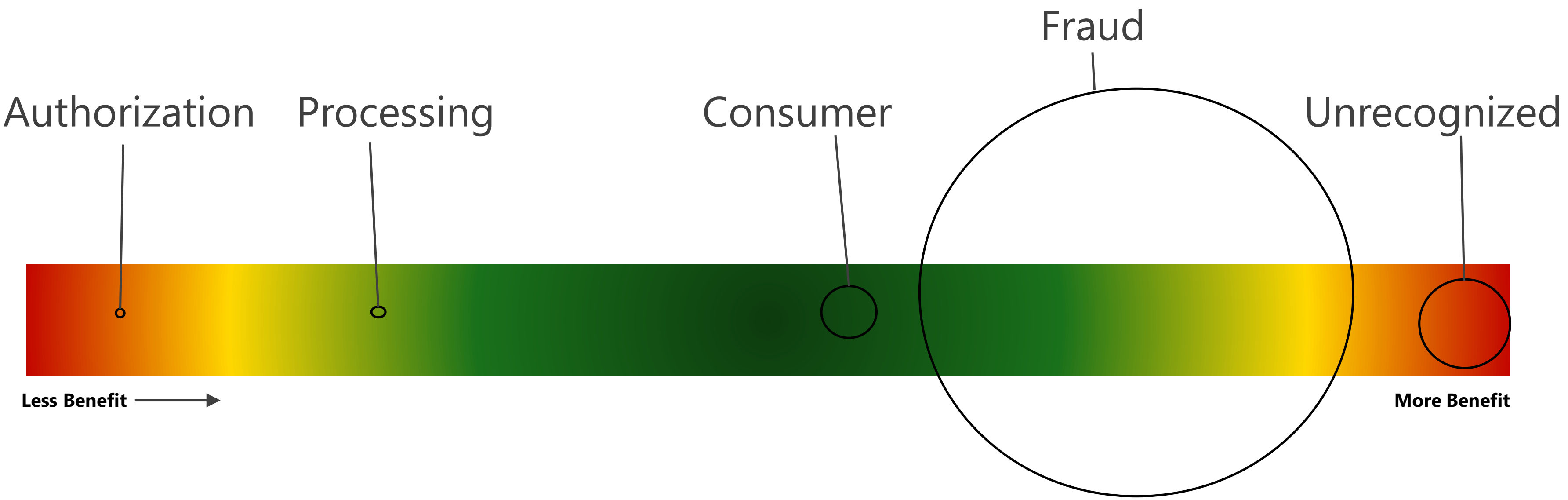
Item Description	Artist/Seller	Type	Price	Quantity
Lara Croft GO	Acme Ind.	Game	8.00	1
Angry Birds	Larry Birdy	Game	1.00	1
Very Angry Birds	Larry Birdy	Game	1.00	1

Steps:

1. Cardholder contacts the Call Center
2. Representative conducts a VROL-Transaction Inquiry
3. VROL Recognizes Merchant (as Integrated) and generates a **Real-Time Purchase Inquiry** to the merchant via an API – Using the original transaction information
4. Merchant renders the response within the established schema
5. Response is provided to the Issuer user, intercepting the potential dispute

Opportunity by Category

- There is significant opportunity due to the nature of disputes by their category, in order to avoid claims at the forefront of the dispute process, reducing costs and financial exposure for all transaction participants



"I shouldn't have been charged. I was declined at the POS."

"I made this purchase but the transaction amount is incorrect."

"The product I ordered is not working"

"I did not make this purchase."

"I need more information because I don't recognize this purchase."

Upcoming Events and Resources

Upcoming Webinars
https://visa.com/cisp

Visa Data Security
https://visa.com/cisp

PCI Security Standards Council Website
https://pcissc.org

Speaker contact information:

- Andrew McGloin - amcgloin@visa.com
- Gord Jamieson – GJamieso@visa.com
- David Richey – drichey@visa.com
- Michelle Levin – milevin@visa.com

Questions