Best Practices for Detecting and Reporting a Common Point of Purchase (CPP)

Popuauliuli Kioa, Analyst, VISA, Cyber Investigations
Stoddard Lambertson Director, VISA, Cyber Investigations

24 March 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.

Agenda

- Introduction
- Data Compromise Trends
- Small Merchant Security Initiatives
- Five Steps to Report a Common Point of Purchase (CPP)
- Key Takeaways
- Questions and Answers

Data Compromises

Typical Data Compromise and Counterfeit Cycle

Entry

- Hackers targeting internet-exposed remote access systems as initial intrusion points
- Once in, attackers conduct network reconnaissance using diagnostic tools/techniques to identify systems with access to payment data and isolate specific user accounts
- They create custom attack scripts and tools to further extend access

Card Data Theft

- Payment card data is extracted with specialized, difficult to detect malware
- Malware is named to appear as legitimate security software in some cases
- Stolen card data is encrypted to avoid detection
- In many recent intrusions, traces of attacker activity are removed, including self-deleting malware

Monetization

- Payment data is used to commit fraud, often across countries via coordinated criminal activity
  - Gift cards
  - High-value goods
- Cards carry a typical value of between US$20–US$60 on underground markets

Note: There may be a significant lag between a breach and monetization

Data Compromise Trends

Visa Security Pillars

Remove sensitive data

Devalue Data

Render data useless for criminals, reducing incentive for payment breaches

- **Tokenization**
- **EMV**

Protect Data

Safeguard payment data

- **Encryption**
- **PCI**

Prevent fraud

Harness Data

Identify fraud before it occurs and increase confidence in approving good transactions

- **Risk-Based Authentication**
- **One-time Passcode**
- **Dynamic CVV2**
- **Breach Response**

Empower Consumers

Engage cardholders as an underutilized resource in fighting fraud

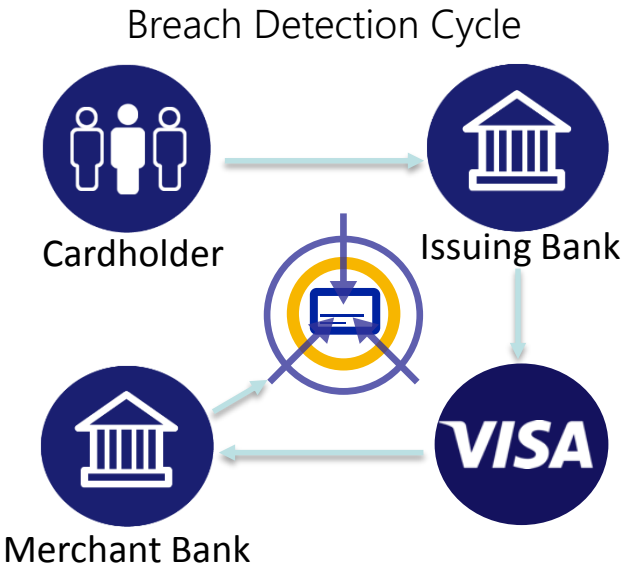
- **Transaction Alerts**
- **Spend Controls**
- **Geolocation**

Transactional Threat Intelligence

Intelligence comes from recognizing fraud patterns, predicting fraud activity

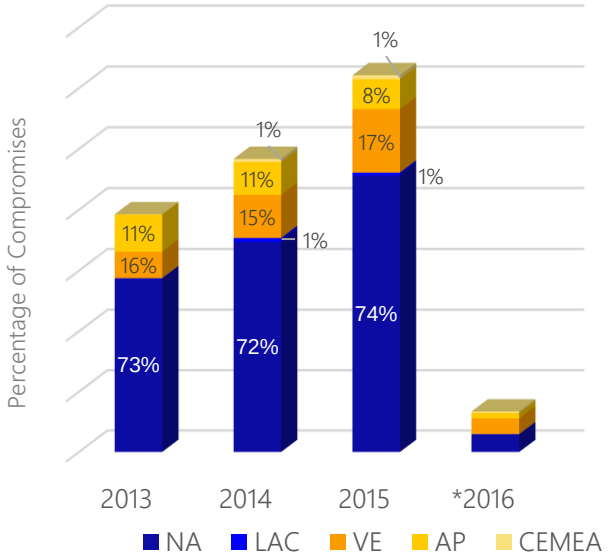
- Cardholders report fraud to their bank
- Banks report fraud to Visa (CPP)
- Visa reports fraud to other banks
- Breach found, stopped

One major limitation: What if there's no fraud?



Global CAMS Distribution

CAMS Alerts Distributed by Region



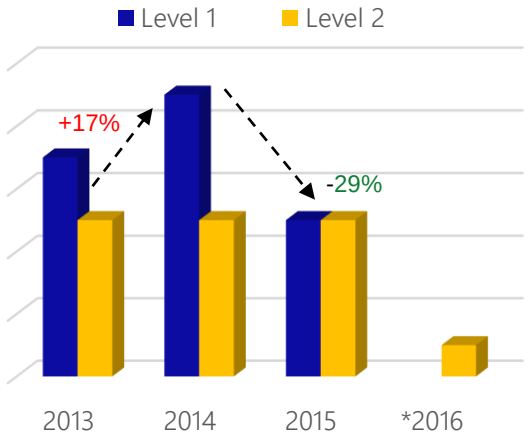
*2016 year-to-date through February

- In 2015, total CAMS alerts increased to the highest level in 3 years
- Because of the sheer magnitude of the number of small merchants worldwide and especially in the United States, Level 4 merchants or small merchants make up the majority of reported compromises
- Investigations revealed cyber criminals exploiting inadequate controls to gain unauthorized access to the POS systems of small level 4 merchants and then ultimately to their payment card data

Global Fraud and Breach Investigation Trends

Breach Events by Merchant Level

Merchant / Entity size	Entity Type	2013	2014	2015	2016*
		%	%	%	%
	Level 1	1%	1%	<1%	0%
	Level 2	1%	1%	<1%	1%
	Level 3	4%	4%	4%	7%
	Level 4	**92%**	**93%**	**93%**	**91%**
Agent		1%	1%	2%	0%
Other		<1%	0%	0%	0%
Total		**100%**	**100%**	**100%**	**100%**



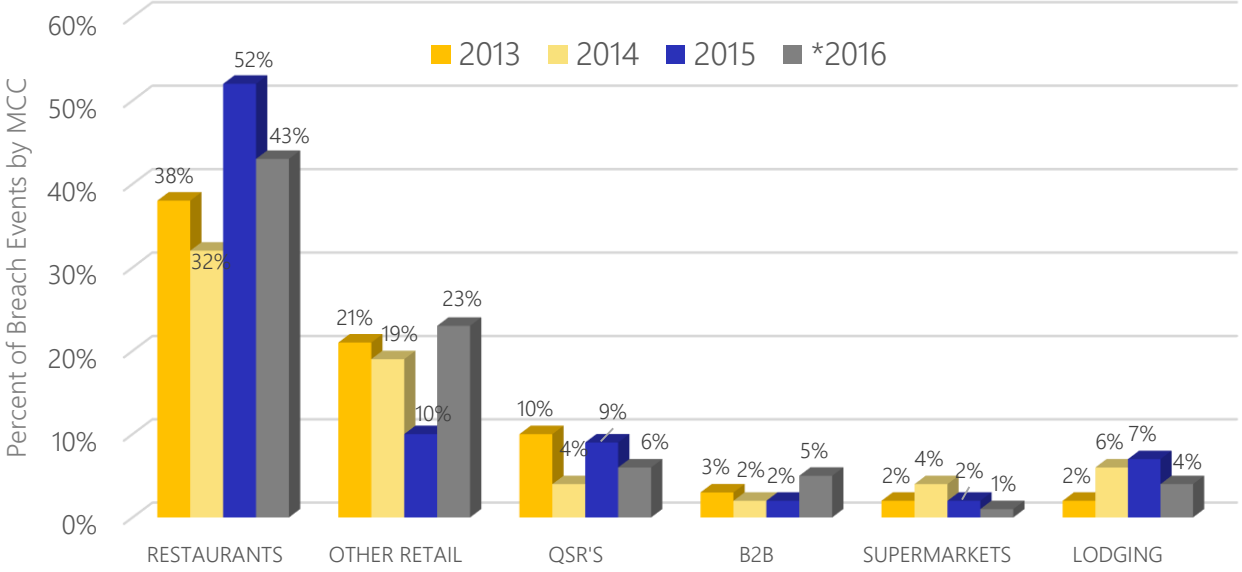
- As a proportion of the total number of breach events, L4s remain the vast majority of compromise cases (93% in 2014-2015)
- Almost half of the at-risk accounts distributed in 2015 were attributed to L4 merchants
- Level 4 merchants outnumber L1s in the U.S.

- Fewer level 1 and 2 breaches in 2015
- U.S. Level 1/Level 2 entities comprised 53% of the total accounts distributed for 2015 – related to large hotel and restaurant events.
- Threat actors are targeting smaller interconnected merchants in large numbers

*2016 year-to-date through February

Global Data Compromises

Breach Trends by Merchant Category Code (MCC)



- Restaurant segments are increasing at a faster rate because they fall in the small business or hospitality industry that are serviced by Integrator Resellers (IR)
- Quick service restaurants, supermarkets, and lodging make up the other top MCCs

Source: Compromised Account Management System (CAMS); data is for Visa Inc. only and represents breach events for which a CAMS was sent.

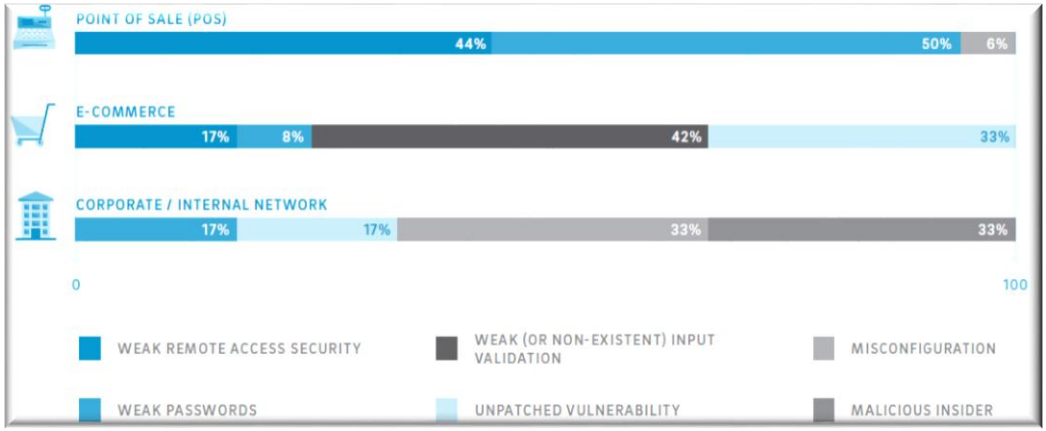
*2016 year-to-date through February

Small Merchant Security Initiatives

Majority of Compromises Occur at Small Merchants

- Untrained integrators that deploy weak remote access configurations are the most common reason for small merchant compromises
- Common attack vector: web-based and direct remote access services used by POS Integrators and Resellers

According to Trustwave Global Security Report 2015, 94% of POS compromises are related to weak remote access security and weak or default passwords



Visa Small Merchant Security Program

QIR and PCI DSS Validation Requirements*

Effective Date	Requirement
March 31, 2016	Acquirers must communicate to Level 4 merchants that beginning January 31, 2017, they must use PCI-certified Qualified Integrators and Resellers for point-of-sale application and terminal installation and integration
January 31, 2017	Acquirers must ensure that Level 4 merchants using third parties for POS application and terminal installation and integration engage only PCI QIR professionals
January 31, 2017	Acquirers must ensure that Level 4 merchants annually validate PCI DSS compliance or participate in the Technology Innovation Program

*Single-use terminals without Internet connectivity are excluded from these requirements.


VISA

VISA SECURITY ALERT

June 2015

CYBERCRIMINALS TARGETING POINT OF SALE INTEGRATORS

Distribution: Value-Added POS Resellers, Merchant Service Providers, Point of Sale Providers, Acquirers, Merchants
Who should read this: Information Security managers and staff, IT Support Providers

Summary

To promote the security and integrity of the payment system, Visa periodically prepares informative materials related to securing cardholder data and protecting the payment industry. To ensure continued preparedness for new and emerging cyber security vulnerabilities, please review this urgent Security Alert.

Visa has observed a considerable increase in malicious remote access activity associated with unauthorized access to merchant Point-of-Sale (POS) environments via POS integrators. POS integrators are businesses that resell, install, configure, and maintain POS software and hardware for many different types of merchants. POS integrators often provide IT support and ongoing maintenance over remote network connections, many of which are established through third-party providers of remote desktop access. Properly secured, these connections pose little risk to merchants. Recently, however, cyber criminals have exploited inadequate security controls to

Five Steps to Report a Common Point of Purchase (CPP)

Common Point of Purchase Process Flow

Goal is to Contain Compromises Quickly and Mitigate Issuer Losses by Sending At-risk Accounts via Proactive Compromised Account Management System (CAMS) Alerts

Visa Investigations

- Receive Suspected Common Point of Purchase (CPP) Reports
- Visa validates Merchant / Agent and Acquirer information
- Fraud Incident Tracking Case Created / Updated
- Visa sends CPP details to Acquirer to investigate
- Visa sends At-Risk accounts to Issuers for CPPs reported by 2 or more issuers

Acquirer Bank Investigations

- Acquirer receives CPP report from Visa
- Acquirer begins investigation & containment process
- Acquirer has 10 days to contain breach
- Once contained acquirer validates merchant is compliant
- Acquirer reports to Visa that case is contained and merchant / agent is compliant

Best Practices: Determining and Reporting a Common Point of Purchase

- Start with similar types of fraud - Card present vs. Card Not Present (CNP)
  - CNP is under reported – Visa encourages issuers to report both CP and CNP fraud schemes despite the liability shift and the chargeback rights
- Fraud transactions should be subsequent to legitimate CPP
- Confirm accounts; do not tie to known previous CAMS events
- Review legitimate usage for 90 – 180 days
  - Identify merchants in common with all accounts
  - Consider false positives (i.e., commonly-shopped merchants)
- Do not exclusively rely on social media boards such as FICO to drive or steer your decisioning for CPP reporting
  - It's a good tool to use to validate but you should not exclusively rely on it
- Only report CPPs to Visa with at least 10 accounts
  - Report CPPs in weekly batches
  - Do not re-report CPPs unless material changes

CPP Reporting Overview

Step 1

- Enroll in VisaOnLine (VOL)
  - https://gvol.visaonline.com

Step 2

- Download New Americas CPP Reporting Form

Step 3

- Complete CPP Form and include accounts!

Step 4

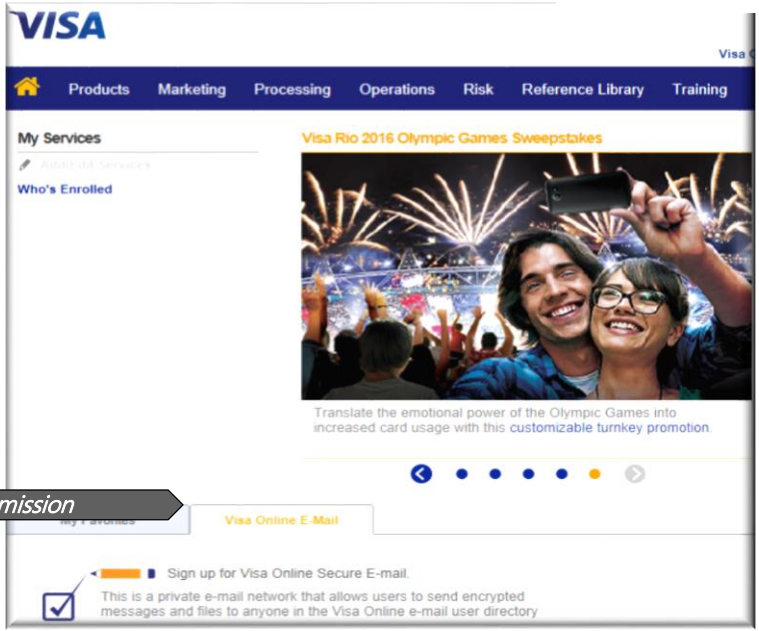
- Log into VOL

Secure E-mail for CPP submission

Step 5

- Send CPP form to Visa using VOL E-mail

Visa Online



VisaOnLine (VOL) – Your Platform for Reporting CPPs

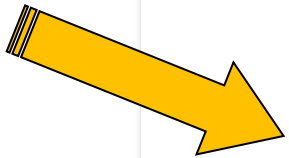
Step 1

- Enroll in VOL

Step 2

- Access the CPP form on VOL:

→ Risk
→ Fraud Risk Products & Solutions
→ Common Point of Purchase (CPP)



Changes to New CPP Reporting Form

Changes to New CPP Reporting Form

Step 3

- Complete CPP Report - Data Fields Defined

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	CARD ACCEPTOR ID	MERCHANT NAME	CITY	STATE	FRAUD $	ACQ_BIN	MCC	TOTAL # FRAUD ACCOUNTS	EXPOSURE START DATE	EXPOSURE END DATE	ISSUER NAME	ISSUER CONTACT NAME	ISSUER EMAIL	LEGITIMATE TRANSACTIONS POS ENTRY MODE
2	Field 42 in Authorization Message: Card Acceptor ID - Up to 15 digits - Alpha Numeric - Format Column as text to maintain entire ID	Field 43 in Authorization Message: Card Acceptor/Merchant Name	Field 43 in Authorization Message: Merchant City	Field 59 in Authorization Message: State Code (2 digit alpha)	Fraud spend	Field 32 in Authorization Message: Acquiring Institution ID (must start with a "4")	Field 18 in Authorization Message: Merchant Category Code	Number of Visa accounts with reported fraud. Minimum number to report a CPP is 10 or more.	Earliest date of suspected compromise (1st legitimate use date)	Last Date of suspected compromise (last legitimate use date)	Issuer Name	Issuer Contact Name	Issuer contact email (not VOL email)	Field 22 in Authorization Message: POS Entry Mode - Valid values are: '01' Keyed Transaction '02' or '90' Swiped Transaction '05' or '95' Chip Card Transaction '07' Contactless VSDC Rules '91' Contactless Mag Stripe Data Rules
3	123456789123456	Merchant A	ANY CITY	XX	$ -	400000	4812	25	2/18/2016	03/04/16	BANK A	Jane Doe	JD@FI.com	90
4	098765432109870	Merchant B	ANY CITY	XX	$ -	400000	5411	35	2/25/2016	03/24/16	BANK A	Jane Doe	JD@FI.com	01

Visa CPP Reporting Template | Accounts (Required)

Note: The Card Acceptor ID fields must be formatted as TEXT to maintain the exact formatting

Changes to New CPP Reporting Form

(Step 3 cont.)

- Accounts Must Be Provided With All CPPs
- Second tab of CPP Form - Provide Visa accounts associated with each merchant name reported
- Use only two columns to report multiple merchants and associated accounts
- Account column must be formatted as TEXT to properly maintain the account numbers

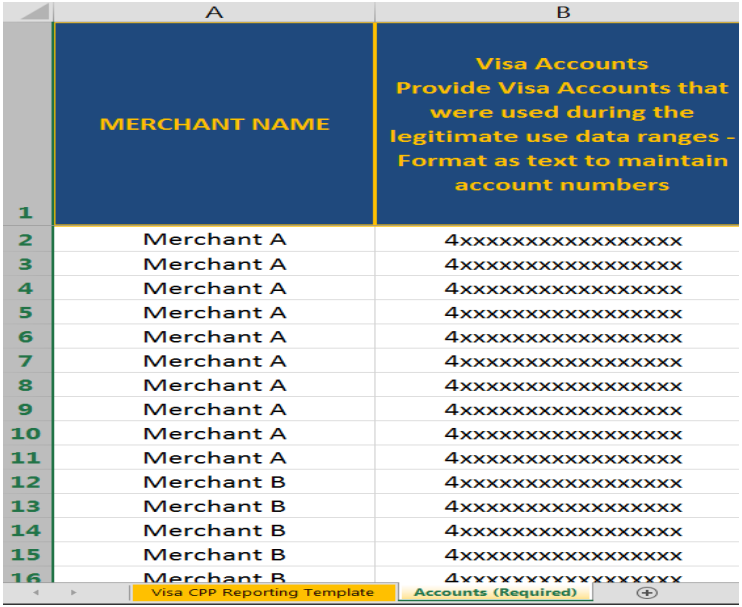
Step 4

- Log into VisaOnLine (VOL)

Step 5

- Send CPP form to usfraudcontrol@visa.com only using secure VOL E-mail

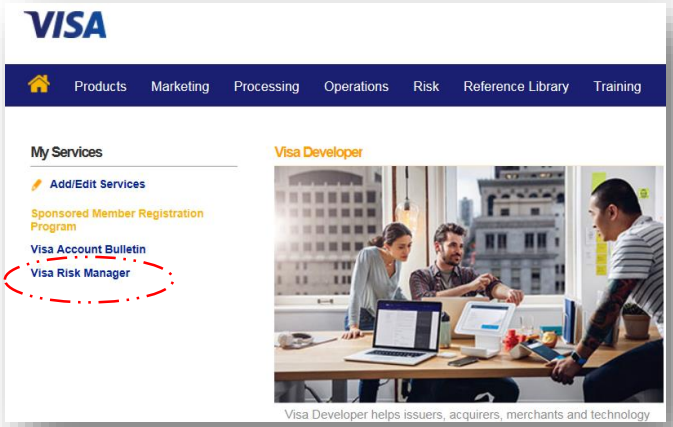
Note: New form goes into effect April 30, 2016



	A	B
1	MERCHANT NAME	Visa Accounts Provide Visa Accounts that were used during the legitimate use data ranges - Format as text to maintain account numbers
2	Merchant A	4xxxxxxxxxxxxxxx
3	Merchant A	4xxxxxxxxxxxxxxx
4	Merchant A	4xxxxxxxxxxxxxxx
5	Merchant A	4xxxxxxxxxxxxxxx
6	Merchant A	4xxxxxxxxxxxxxxx
7	Merchant A	4xxxxxxxxxxxxxxx
8	Merchant A	4xxxxxxxxxxxxxxx
9	Merchant A	4xxxxxxxxxxxxxxx
10	Merchant A	4xxxxxxxxxxxxxxx
11	Merchant A	4xxxxxxxxxxxxxxx
12	Merchant B	4xxxxxxxxxxxxxxx
13	Merchant B	4xxxxxxxxxxxxxxx
14	Merchant B	4xxxxxxxxxxxxxxx
15	Merchant B	4xxxxxxxxxxxxxxx
16	Merchant B	4xxxxxxxxxxxxxxx

Visa CPP Reporting Template | Accounts (Required)

Compromised Account Management System (CAMS) Overview



- Compromised Account Management System (CAMS) notifies financial institutions when their accounts are at risk due to a compromise and provides critical information such as:
  - At-risk Accounts
  - Expiration Dates
  - Data Elements Involved
- Visa CAMS provides important updates on compromised accounts to subscribers as soon as it becomes available
- Best practices of analyzing CAMS data to their fraudulent accounts – not known in CAMS then provide CPP with new details
- Visa CAMS alerts now contain merchant name when they have gone public for large events

Account Compromise Response Strategies

Before
(identifying a data compromise)

- Consider Issuing EMV Cards!
- Analyze fraud patterns on "at risk" accounts, test fraud mitigation rules
- Report CPPs to Visa

During
(preventing fraud once a compromise is confirmed)

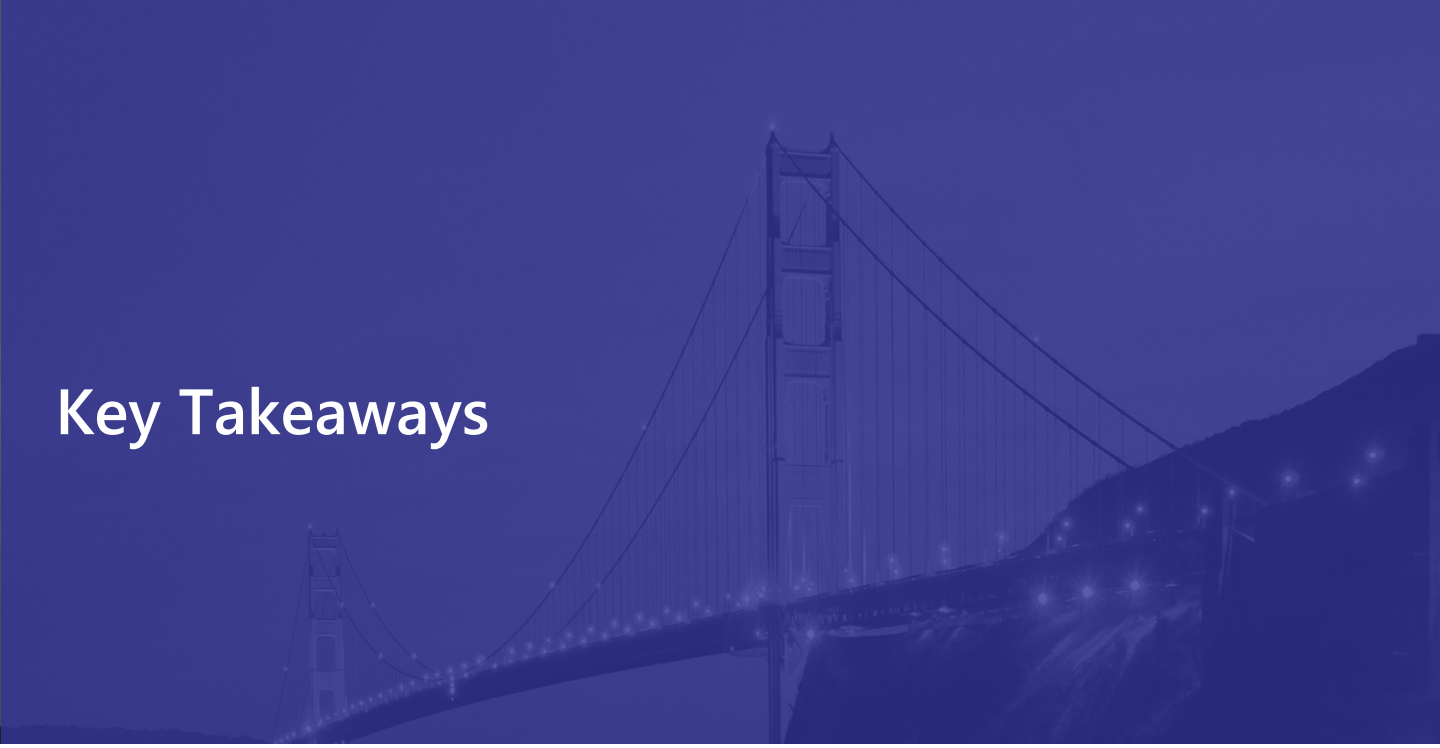
- Download accounts from CAMS
- Flag impacted accounts and monitor activity
- Leverage Visa Advanced Authorization (VAA)
- Align fraud controls to type of data exposed

After
(on-going, monitoring)

- Adjust fraud rules based on how fraud is trending
- Report fraud to Visa using Visa's Fraud Reporting System
- Consider reissuance strategy as applicable

Note: Best Practices for Issuers on VOL CPP Site

Key Takeaways



Conclusion and Recap: The Benefits of CPP Reporting

1. We expect attack techniques to evolve along with security
2. Issuer CPP Reporting is critical intelligence to help monitor the security of the payment eco-system
   - Visa encourages Issuers to increase Card Not Present CPP reporting
   - CNP fraud has grown globally as the channel has grown, regardless of EMV
3. New CPP form with accounts will help Acquirers more quickly to investigate and contain events
4. Never send CPP forms (which must have Accounts!) through regular email. Always use your secure Visa OnLine Email for CPP submissions.

Questions and Answers