Visa Quick Reference Guide for CPP Reporting

Introduction

Issuer Common Point of Purchase (CPP) reporting is critical intelligence to help monitor the security of the payment eco-system. As data compromises continue to emerge, many Visa clients attempt to determine if a CPP exists. To help issuers validate claims of a suspected compromise, Visa partnered with issuers to develop an enhanced CPP form (AP, Canada, CEMEA, LAC, U.S. version | Europe version) for easy reporting to Visa. This report is required in order for an investigation to be considered. The CPP form also helps align a common process that all issuers must adhere to for an investigation to be initiated.

CPP Defined

A Common Point of Purchase (CPP) is determined when clients identify a subset of accounts with legitimate cardholder usage, containing a single common merchant identifier prior to fraudulent activity and not associated with a previously reported data compromise event. In their battle to fight counterfeit fraud, Visa clients will attempt to determine if a CPP exists. A CPP is defined as a merchant location, processor or agent/institution where a legitimate card transaction occurred on the affected account prior to fraudulent activity.

To further assist issuers, this new *Visa CPP Quick Reference Guide* provides detailed guidance and descriptions and examples of each of the required data fields necessary for reporting a CPP to Visa. Clients in the Visa AP, Canada, CEMEA, LAC and U.S. regions can find guidelines on the CPP process, the CPP reporting form, this new Quick Reference Guide and other CPP-related resources at VisaOnline.com. Under the "Risk" tab, choose "Fraud Risk Products and Solutions," and then "Common Point of Purchase (CPP)."

Issuers with processes in place to identify potential points of compromise should report any potential compromises to Visa for further investigation as a CPP. Issuer CPP reporting is a critical intelligence source for Visa and a valuable tool to help monitor the security of the payment ecosystem.

Enroll in Visa Online – Secure Platform for Reporting CPPs

To properly report a CPP all entities must have a valid user ID for Visa Online access. To enroll in Visa Online entities must take the following steps:

Step 1	Enroll in Visa Online at VisaOnline.com (or eu.VisaOnline.com for users in the Visa Europe region).
Step 2	Once enrolled in Visa Online, download the CPP reporting form. Users in the AP, Canada, CEMEA, LAC and U.S. regions may access the CPP form on Visa Online by clicking on the "Risk" tab and choosing "Fraud Risk Products and Solutions," and then navigating to the "Common Point of Purchase (CPP)" section. Users in the Europe region may use the search tool to find the document.
Step 3	Complete all of the CPP form fields and include accounts that were legitimately used at the CPP. Note: A single CPP form can be used to submit multiple CPPs to Visa.
Step 4	After completing the CPP form, log in to Visa Online.
Step 5	As a registered VOL user, you have access to a VOL secure email account. To send the CPP form to Visa, entities must use their secure Visa Online email to submit the CPP form securely to Visa. This form must be sent using the secure Visa Online email infrastructure to protect the account data and other data elements within the CPP form. Entities should send the CPP form to the following email addresses based on their geographical locations: • United States – usfraudcontrol@visa.com • Canada – CanadaInvestigations@visa.com • Latin America and Caribbean – LACFraudInvestigations@visa.com • Asia Pacific (AP) and Central and Eastern Europe, Middle East and Africa (CEMEA) – VIFraudControl@visa.com • Europe – Datacomp@visaonline.com

Note: Visa Fraud and Breach Investigations will not accept CPP form submissions by any method other than Visa Online Secure Email. Incomplete forms will not be reviewed.

Best Practices for Determining and Reporting a CPP

Issuers with processes in place to identify potential points of compromise should report any potential compromises to Visa for further investigation as a CPP. To assist issuers with their identification and analytics, listed below are some best practices for effective CPP identification:

- Start with similar types of fraud - Card Present vs. Card Not Present (CNP). Note in some regions CNP is under reported and Visa encourages issuers to report both Card Present and CNP fraud schemes
- Fraud transactions should be subsequent to legitimate use at the suspected CPP
- Identify merchants/entities in common with all accounts
- Confirm the legitimate use accounts for detecting the CPP, do not tie to known previous CAMS events
- To ensure entities are detecting recent events, a best practice is to only review legitimate usage for the past 90 – 180 days. As CPP information ages it becomes more difficult to investigate.
- Consider false positives (i.e., commonly-shopped merchants). These popular points of purchase should always be a consideration in detecting a CPP. To help lower false positive rates, consider looking at low usage accounts. Single use accounts, if detected, can further reduce the false positive ratio.

- Do not exclusively rely on social media boards or unconfirmed media reports to drive or steer your decisioning for CPP identification and detection. This may be a tool to use to validate but you should not exclusively rely on such external resources.
- Only report CPPs to Visa with at least 10 accounts, as this helps increase the probability of a correct CPP detection with the higher number of accounts at risk
- Report CPPs in weekly batches to more efficiently manage the submission and intake processes, and use one form to send multiple CPPs
- Do not re-report CPPs unless material changes have occurred, further do not report CPPs on large known public events or events where CAMS has been received unless locations or accounts are new or not previously received.
- The legitimate use accounts must be provided with all CPPs within the second tab of CPP Form. Entities must provide the accounts along with the merchant name and Visa Card Acceptor ID for the merchant. To maintain the integrity of the Accounts and the Card Acceptor ID fields, the columns should be formatted as text.

CPP Data Requirements Fields and Examples

The CPP form consists of the following data fields:

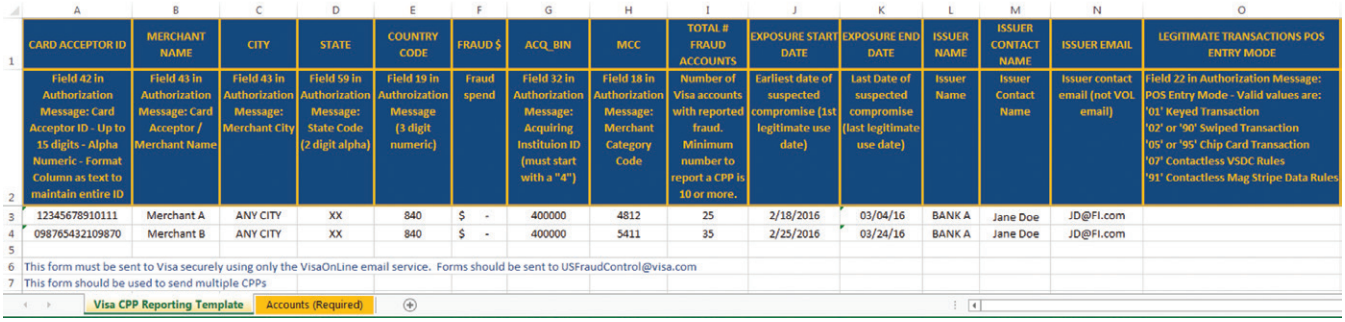
Data Field	Data Field Description	Data Field Overview and Best Practices
CARD ACCEPTOR ID	Field 42 in Authorization Message: Card Acceptor ID - Up to 15 digits - Alpha Numeric	Card Acceptor IDs may begin and end with zeros or letters. Format Column as text in the reporting form to maintain the entire unaltered ID. The full unaltered contents of the Card Acceptor ID must be provided without truncation or modification for Visa to process the CPP.
ENTITY NAME	Field 43 in Authorization Message: Card acceptor/ Merchant/Entity Name	Entity name should be reported exactly as it is found in Field 43 of the Authorization Message
CITY	Field 43 in Authorization Message: Merchant/Entity City	Entity city/location should be reported exactly as it is found in Field 43 of the Authorization Message
STATE	Field 59 in Authorization Message: State Code (2 digit numeric)	Note: For US and Canada two digit alpha state codes are accepted. Field 59 is a national-use field to identify an intra-country geographical location. Visa uses this field to describe the location of a customer transaction within the country of the card acceptor. The card acceptor country is identified in Field 19—Acquiring institution Country Code. Refer to the Visa Technical Specifications for further details.
Country Code	Field 19 Acquiring Institution Country Code (3 digit numeric)	Field 19 contains a three digit numeric code that identifies the country of the acquiring institution for the merchant or ATM. Refer to the Visa Technical Specifications for further details on the valid values for Field 19 "Country and Currency Codes".
FRAUD $	Fraud spend – Approved	This field should be reported in US dollars and should only be for actual fraud dollars that were approved. Do not include fraud losses that were avoided or declined.

Data Field	Data Field Description	Data Field Overview and Best Practices
ACQ_BIN	Field 32 in Authorization Message: Acquiring Institution Identification Code	This code identifies the financial institution acting as the acquirer of record for the transaction. The acquirer is the client or system user that signed the merchant, installed the ATM or unattended cardholder-activated environment, or dispensed cash. The ID can be a Visa BIN or another code that identifies the financial institution. Visa BINs are usually 6 digits and typically begin with a 4.
MCC	Field 18 in Authorization Message: Merchant Category Code (MCC)	Field 18 contains a 4 digit numeric code describing the merchant's type of business product or service, also known as the merchant category code (MCC). These codes are based on the Merchant Classification Code Guideline available from the Bank Card Division of the ABA.
TOTAL # FRAUD ACCOUNTS	Number of Visa accounts with reported fraud	For Visa to prioritize and process CPPs, reporting entities must report a minimum of 10 or more unique accounts with fraud when reporting a CPP. Visa will allow for CPP reporting with less than 10 accounts for cross border scenarios and when there is limited domestic Visa processing. Entities should not continue to report CPPs based on number of account changing/increasing. If there is a material increase in the number of accounts entities should provide an updated CPP report to Visa with only the new affected count of accounts. Note the Visa accounts should not be associated with other known compromise events. Entities should exclude any accounts that are deemed to be associated with previous accounts identified in other compromises which may have been communicated via CAMS to issuers.
EXPOSURE START DATE	Earliest date of suspected compromise (1st legitimate use date) Format mm/dd/yyyy	The earliest date of suspected compromise (1st legitimate use date) is determined when clients identify a subset of accounts with legitimate cardholder usage, containing a single common merchant identifier prior to fraudulent activity and not associated with a previously reported data compromise events. This exposure start date should be the earliest legitimate use date. The format must be in a MM/DD/YYYY format.
EXPOSURE END DATE	Last Date of suspected compromise (last legitimate use date) Format mm/dd/yyyy	The last date of suspected compromise can be referred to as the last legitimate use date. Entities may re-report a CPP if there is a material change in the window of exposure for a CPP and the last legitimate use date continues to expand. An active fraud investigation can take approximately 30 to 90 days on average to contain and close; however, larger investigations may take longer. The format must be in a mm/dd/yyyy.
SUBMITTER INSTITUTION NAME	Name Of Company/Institution	In some cases, Visa may need to contact the reporting CPP entity for additional details to assist with an investigation. Further, Visa requires this information to properly attribute the CPP to the correct reporting institution.
SUBMITTER CONTACT NAME	Name of contact at submitting organization	Visa may need to contact the reporting CPP entity for further details.
CONTACT EMAIL	Email of contact at submitting organization (not VOL email)	Visa may need to contact the reporting CPP entity for further details. Entities must provide their normal business email and should not provide their Visa Online email in this field.

Data Field	Data Field Description	Data Field Overview and Best Practices
LEGITIMATE TRANSACTIONS POS ENTRY MODE	Field 22 in Authorization Message: Point-Of-Service Entry Mode Code: 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	Field 22 contains the Point-of-Service Entry Mode Code that indicates the method used to enter the account number. To understand the data elements at risk and to help focus the investigation on what acceptance channel may be impacted it is critical for issuers to provide how the account was entered by the merchant. Accounts can be key entered, mag stripe read, chip read and contactless.
LIST OF VISA ACCOUNTS (part 2 of form)	Visa Accounts used during the legitimate use data ranges. Format as text to maintain account numbers.	These accounts must be provided on the second tab of the CPP Reporting Form. The Merchant Name, the Card Acceptor ID and the associated accounts must be provided for the CPP to be processed by Visa. Visa accounts are critical for the Acquirer and their merchant/agent to conduct a thorough investigation. Both the Card Acceptor ID and the Visa Accounts must be formatted as text to maintain their integrity.

Sample CPP Form

Part 1 – CPP Details



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	CARD ACCEPTOR ID	MERCHANT NAME	CITY	STATE	COUNTRY CODE	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)	Field 19 in Authrization Message (3 digit numeric)	Fraud spend	Field 32 in Authorization Message: Acquiring Instituion 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	12345678910111	Merchant A	ANY CITY	XX	840	$ -	400000	4812	25	2/18/2016	03/04/16	BANK A	Jane Doe	JD@FI.com	
4	098765432109870	Merchant B	ANY CITY	XX	840	$ -	400000	5411	35	2/25/2016	03/24/16	BANK A	Jane Doe	JD@FI.com	
5															
6	This form must be sent to Visa securely using only the VisaOnLine email service. Forms should be sent to USFraudControl@visa.com														
7	This form should be used to send multiple CPPs														

Visa CPP Reporting Template | Accounts (Required)

Part 2 – Legitimate Use Visa Accounts

	A	B	C
1	MERCHANT NAME	CARD ACCEPTOR ID - Format Column as text to maintain entire ID	Visa Accounts Provide Visa Accounts that were used during the legitimate use data ranges - Format as text to maintain account numbers
3	Merchant A	12345678910111	4xxxxxxxxxxxxxxx
4	Merchant A	12345678910111	4xxxxxxxxxxxxxxx
5	Merchant A	12345678910111	4xxxxxxxxxxxxxxx
6	Merchant A	12345678910111	4xxxxxxxxxxxxxxx
7	Merchant A	12345678910111	4xxxxxxxxxxxxxxx
8	Merchant A	12345678910111	4xxxxxxxxxxxxxxx
9	Merchant A	12345678910111	4xxxxxxxxxxxxxxx
10	Merchant A	12345678910111	4xxxxxxxxxxxxxxx
11	Merchant B	098765432109870	4xxxxxxxxxxxxxxx
12	Merchant B	098765432109870	4xxxxxxxxxxxxxxx
13	Merchant B	098765432109870	4xxxxxxxxxxxxxxx
14	Merchant B	098765432109870	4xxxxxxxxxxxxxxx
15	Merchant B	098765432109870	4xxxxxxxxxxxxxxx
16	Merchant B	098765432109870	4xxxxxxxxxxxxxxx
17	Merchant B	098765432109870	4xxxxxxxxxxxxxxx
18	Merchant B	098765432109870	4xxxxxxxxxxxxxxx
19	Merchant B	098765432109870	4xxxxxxxxxxxxxxx
20	Merchant B	098765432109870	4xxxxxxxxxxxxxxx
21	Merchant B	098765432109870	4xxxxxxxxxxxxxxx
22	Merchant B	098765432109870	4xxxxxxxxxxxxxxx

Visa CPP Reporting Template | Accounts (Required)

Visa expects attack techniques will continue to evolve, and accurate Issuer CPP reporting will continue to be critical intelligence to help monitor the security of the payment eco-system

For further details on CPP reporting, and other related information refer to the CPP section of Visa Online.

For More Information

U.S.	+1 (650) 432-2978	USFraudControl@visa.com
Canada	+1 (416) 860-3872	CanadaInvestigations@visa.com
Latin America & Caribbean	+1 (305) 328-1593	LACFraudInvestigations@visa.com
Asia Pacific (AP) and Central and Eastern Europe, Middle East and Africa (CEMEA)		VIFraudControl@visa.com
Europe		datacompromise@visa.com