Common Point-of-Purchase Analysis

1.1 Definition/Description

Common point-of-purchase (CPP) analysis is a technique that helps determine the source of a card breach and, with that, indicates the likelihood that specific cards have been compromised. This helps issuers decide which cards need to be canceled and re-issued.

When investigating cards flagged with fraudulent activity or when researching compromised cards being sold or handled in an illicit fashion (e.g., through dark web activity), issuers may analyze authorization history on these cards to triangulate a common point where the cards were used and subsequently compromised.

A CPP happens only after cards have been identified as compromised or an incident has been reported. Using CPP analysis does not prevent all losses related to a breach; instead, it allows affected issuers to mitigate additional fraud related to that breach.

1.2 Applicability

Channel	Applicable?	Use Case	Applicable?	Stakeholder	Applicable?
In-app [merchant app]	NA	Customer onboarding	NA	Merchants	NA
Mobile browser	NA	Authentication (onboarding)	NA	Issuers	Yes: internal
Desktop/laptop computer	NA	Authentication (transaction)	NA	Issuer processors	Yes: for clients
Phone	NA	Authorization	NA	Wallet/online payment providers	NA
		Post-authorization review	NA	Acquirer processors	Yes: for clients

1.3 Technical Features/How the Technique Works

When fraud is reported or a card is suspected of being compromised, an issuer flags the card and the places where the card was previously used. Repeating this process on multiple cards may show common points of purchase—merchants—where the cards were likely compromised. This allows an issuer to identify additional cards used at those merchants that may also be compromised, even though they have not yet experienced fraud, and take appropriate action.

Large issuers have the staff and transaction volume to do CPP analysis for themselves. Smaller issuers typically do not.

Vendors aggregate volume from many issuers to flag CPPs and potentially breached portfolios.

1.4 Risks Associated with Technique

A card issuer using results from a CPP analysis must make its own decision about which cards to cancel and re-issue. Each cancellation and reissuance has a direct cost, and may have an indirect cost—e.g., cardholders may reduce spend if a card has been cancelled and re-issued due to suspected fraud.

1.5 Customer Impact/Level of Friction

This technique initially has no impact on customers if the cardholder’s card is unaffected.

1.6 Implementation Considerations

Issuers and vendors implementing a successful CPP analysis program will need access to authorization/transaction history for their card populations. Additionally, issuers and vendors may employ various research methods to identify compromised cards online and on the dark web.

1.7 Maturity

The practice of CPP analysis has been present and active with issuer for over 10 years.

1.8 Applicable Industry Standards

This technique has no applicable industry standards.

1.9 Publicly Available Statistics on Implementations and Use

Statistics are not available for this technique.

1.10 Further Reading

https://finance.uw.edu/ps/sites/default/files/Fraud%20Prevention%20Best%20Practices.pdf

https://www.sas.com/en_us/insights/articles/risk-fraud/common-point-of-purchase.html