Compelling Evidence 3.0 – Merchant FAQ

VERIFI | A Visa Solution

FOR VERIFI MERCHANTS

In January 2024, Visa released an article differentiating requirements for compelling evidence item 10 and the Compelling Evidence remedy rule for dispute condition 10.4 - Other Fraud – Card Absent Environment (commonly referred to as Compelling Evidence 3.0, or CE3.0).

This article outlines required data elements and transaction requirements for:

- Compelling Evidence Item 10, or applicable disputes under condition code 10.4
- Compelling Evidence Remedy Rule.

Visa has seen an increase in the number of inquiries regarding the difference between Compelling Evidence item 10 and the Compelling Evidence remedy rule. The following table provides clarity:

	REQUIRED DATA ELEMENTS	TRANSACTION REQUIREMENTS
Compelling Evidence Item 10	Three or more of the following had been used in an undisputed transaction: • Customer account/login ID • Delivery address • Device ID/device fingerprint • Email address • IP address • Telephone number	One transaction any time period
*Compelling Evidence Remedy Rule	At least two of the following are the same in the disputed/undisputed historical transactions: • Customer account/login ID • Delivery address • Device ID/device fingerprint • IP address One of two must be Device ID or IP address.	Two non-fraud reported transactions between 120-365 days prior to the dispute processing date

*Evidence that qualifies for the Compelling Evidence remedy rule is the same for either the pre-dispute or post-dispute stage.

What are the data elements that should be supplied for Cardholder-initiated Transactions (CIT)?
Merchants should be sourcing the data elements of IP address, device ID/fingerprint, account log-in ID and shipping address from the consumers' data in the CIT and should be the data elements of the consumer and not the merchant. The data elements for CITs should not be sourced from the account set-up or the creation of the card on file information unless it occurred during the financial transaction.

Does CE3.0 work for recurring Merchant-initiated Transactions (MIT)?
Yes, CE3.0 is available for recurring transactions. For subscription merchants processing recurring MITs, the Cardholder's IP address from the initial cardholder-initiated transaction (CIT) can be populated for the subsequent MIT used to establish a historical footprint, if the subsequent MIT was non-disputed and meets all other qualification criteria being used as evidence of a historic, non-disputed transaction.

Can log-in/account ID be the customer's phone or email?
Yes, if that is the credential the customer used to authenticate to the merchant's E-commerce site for the transaction. If the cardholder established a credential that is not their phone or email, such as a user ID, then that credential should be provided to Visa.

If the cardholder used guest checkout for the transaction, can the cardholder's authenticated email or phone number be provided as the log-in/account ID?
No, a guest checkout allows the cardholder to purchase without logging into or creating an account. As an account is nonexistent, an email or phone number cannot be used to represent this data.

Next Page >

Can the shipping address be a store location? What about PO box address or office address?
No, for online purchase the pick-up in store, there is no shipping address since it has been picked up at the merchant location. For delivery to PO boxes or offices, those are valid if that is the consumer's location, not the merchant's.

What elements of the shipping address are required?
Full shipping address of the cardholder is required. Street address, city, state/province (if applicable), postal code and country. If postal code is not applicable for your region, enter xxxxxxxxx (9 "X"s) in the postal code field.

What are the requirements for Device ID?
A device ID must be a unique identifier for the device that is accessible by the cardholder.

Can you provide suggestions on how to generate a device fingerprint?
Multiple attributes can make up the device fingerprint. For instance, device model, CPU, memory, sensors, unique device IDs, etc.

What values are required for merchandise/service description?
The description must include details that are above and beyond the merchant's name or merchant category code (MCC) and must clearly explain what was purchased, as shown in the following examples:

- Renew subscription ID: 123456789
- Instant access to Diet 30 Day Plan
- Hotel stay downtown in Asheville, US checking in on 2023-07-23
- Online dating subscription
- Premium video game package for 90 days
- Transfer to wallet 123456789

Is it valid if the transaction or transactions being used for the historical footprint were eventually credited back to the cardholder (i.e., merchandise return)?
Yes. Because the intent of compelling evidence is to show the cardholder had an existing relationship and participated in previous undisputed transactions using the same key identifying fields. The goods/services being returned and credited have no bearing on the validity of these identifying fields.

What benefits to the payment ecosystem does this rule change enable?
Benefits to merchants participating via Order Insight during pre-dispute processing:

- Helps reduce fraud and dispute ratios
- Helps reduce revenue lost to disputes
- Helps reduce overall dispute processing expenses
- Drives network value for merchants
- For multi-acquired merchants, transactions acquired by any acquirer can be provided as historical transactions

Benefits to merchants participating via post-dispute pre-arbitration:

- Helps reduce fraud ratios, not dispute ratio (important distinction)
- Helps reduce revenue lost to disputes
- Drives network value for merchants. Merchants using VisaNet for payment processing benefit from these services to help protect their revenue
- For multi-acquired merchants, the merchant is limited to the historical transactions acquired by the acquirer for the disputed transaction

Issuers:

- Helps avoid card reissuance costs (for pre-dispute deflection only)
- Helps increase issuer risk model performance with more accuracy
- Provides issuers with more data on their cardholder behavior
- Empowers issuers with data to potentially challenge cardholders and reverses provisional credits on disputed transactions

Next Page >

Acquirers:

- Delivers accurate data and compliance program identifications
- Creates opportunities for acquirers to assist in solving the friendly fraud problem

How many fraud disputes are estimated to qualify for the new rules?
Results will vary by merchant and may be driven by their business model. Merchants that see high-frequency purchases from cardholders or use recurring billing methods are more likely to benefit from the rule change. Merchants must collect the data required by the rule change, so it is important to evaluate what data is collected and stored on purchases.

Will all issuers and merchants participate? Can they opt in or opt out?
The rule will be effective globally and apply to all Visa issuers. All Visa transactions processed using VisaNet will be eligible. Merchants can choose to leverage both pre-dispute and post-dispute capabilities to maximize benefits, or simply use one or the other. However, they must be integrated with Verifi through the Order Insight integration for pre-dispute benefit.

How does this affect transactions using pre-paid cards?
If there are historical undisputed and non-fraud disputed transactions associated with the PAN greater than 120 days, and the data points for the transaction match the historical transactions, the new rule can be leveraged.

Can a transaction that had a prior non-fraud dispute be considered as a historical transaction?
Yes, if a prior transaction has a non-fraud dispute it qualifies as a historical transaction. ONLY prior transactions that DO NOT have any fraud activity (TC40) are eligible. Note: Fraud Disputes reported under codes C and D will not be classed as a fraud dispute.

FRAUD CODE	CODE NAME	CODE DESCRIPTION
C	Merchant Misrepresentation	Fraud resulting from a merchant deliberately misleading the account holder. Examples may include: • A merchant fraudulently selling items that are not as they seem or sub-standard. • Charging more than anticipated or for a longer term. • Charging for a service that the consumer can get for free through another channel for the purpose of conducting fraudulent activity, etc.
D	Manipulation of Account Holder	Fraud resulting from a merchant manipulating an account holder into completing what they believe to be a legitimate transaction. This fraud type has been added to support Visa Direct and European PSD2 regulations. Examples may include: • Account holder manipulated into sending funds to a fraudulent beneficiary when the sender believes they will gain fictitious riches or help an individual.

Next Page >

Is there any guidance on what period the merchant should search for historical transactions?
For participating merchants in pre-dispute, Visa will identify prior eligible transactions, and the merchant will receive API requests to provide order details for these transactions which will be used to evaluate whether the dispute is eligible for CE3.0 coverage. To maximize the benefits, merchants must ensure order data is available for up to 365 days after the original payment was processed.

Merchants should work with their acquirers to identify the best transactions to supply as compelling evidence in the post-dispute and pre-arbitration process that meet the requirements for qualifying transaction data as outlined in the CE3.0 rule.

How can annual subscription merchants benefit if the limit on previous transactions is 365 days?
If the merchant does not have multiple transactions for the cardholder within a 365-day time, then the rule will not be supported in either the pre-dispute or post-dispute processing. Note however, that subscription disputes are often classified as "Cancelled Recurring", rather than "Other Fraud – Card Absent Environment" (10.4).

For digital goods merchants, are there any alternative data points that could be considered in lieu of delivery address?
Delivery address would not apply for digital goods merchants; but the rule allows for other applicable fields such as IP address, Device ID, Device fingerprint, and/or Account ID values to qualify instead.

If the merchant is not supplying physical goods, can the billing address be used?
No, if merchandise is not shipped, the delivery address cannot be replaced with billing address. The other 3 data elements would be available for use to meet the requirement.

IP addresses are often dynamic, and customers are changing their devices from time to time. How are merchants supposed to match that?
Recognizing that this information can change across transactions, Visa is searching for up to 5 historical transactions for the merchant to respond. Matching data across 2 of those transactions is required to meet the rule conditions. If a merchant is unable to provide the IP address as a reliable data element to match across multiple transactions, they should use other data elements such as device ID, device fingerprint or account ID.

How will the merchant decide which two transactions to choose for the post-dispute response?
For post-dispute pre-arbitration responses, the merchant will identify prior transactions based on rule criteria. The merchant should work with their acquirer to get up-to-date fraud data to ensure they are only responding with orders that have not been disputed as fraud. Merchants that do not get fraud data from their acquirer can leverage Verifi's INFORM solution to receive fraud reports to ensure the transactions the merchant selects have not been reported as fraud or disputed as fraud. If the merchant has multiple eligible transactions to be returned for post-dispute compelling evidence rules, it is advised they choose from the most recent transactions that meet the rule timeframes.

If a cardholder continues to deny that they made the purchase after the merchant has submitted all the data that proves the purchase is legitimate, will this be an automatic pre-arbitration loss to the issuer?
If the merchant provided all the required data elements in the pre-arbitration stage, the issuer will be liable for the transaction, if they accept the liability. Issuers have the option to deny the liability shift if they have enough evidence to support their claim. However, the issuer should carefully evaluate this option, as the acquirer can go to arbitration and if Visa determines that the evidence provided by the issuer is not sufficient, issuer will not only lose the case, but also will pay for the cost of arbitration. Hence issuers are strongly advised to assess the relationship with the cardholder to determine whether to hold the cardholder liable or accept the loss.

Can an issuer file a fraud dispute, get blocked by the Compelling Evidence, then re-submit the dispute under a non-fraud dispute reason code?
Yes, it is possible that a cardholder can report a fraud, and if the fraud gets rejected, the cardholder may submit a consumer (or any other non-fraud) dispute, if it is within the dispute timeframe.

A valid use case for this: the cardholders was unable to recognize a transaction (thereby claiming fraud), then recognizing it and raising a consumer dispute (e.g., non receipt of merchandise).

Next Page >

However, the reverse is not valid, i.e., once a cardholder raises a consumer dispute and is rejected, it cannot again be claimed as fraud.

Issuers usually provide provisional credit to the cardholder before the fraud dispute submission is initiated. Will they need to reverse the provisional credit?
Issuer procedures vary. In the event the dispute is blocked by the Compelling Evidence supplied by the seller, the issuer may choose to reverse the provisional credit and reject the cardholder's claim of fraud and discuss/review the Order Insight data returned by the seller or allow it to become permanent and write off the funds as a financial loss.

What if the issuer reports fraud for a transaction but it is not disputed? Does this rule change allow the reported fraud to be reversed?
No, the Compelling Evidence rule only triggers once the issuer files a fraud dispute. If the cardholder does not initiate the dispute, the fraud report will not be reversed because it does not qualify for rule protection. If the fraud dispute is blocked by the Compelling Evidence rules processing, the fraud report will also be deleted.

What is an OCT transaction and would CE3.0 rules for 120 - 365 days historical transaction eligibility apply to these transactions?
An "OCT" (Original Credit Transaction) is a Visanet transaction used to "push" funds to a card-based account (such as to pay a cardholder to their card account). An "AFT" (Account Funding Transaction) is a Visanet transaction used to draw or "pull" funds from a card account to fund an OCT to a different account.

The 120-365 day rule is valid for the AFT but the OCTs can be between 0 - 365 days.

What format should Device ID and Device Fingerprint be delivered in?
There are standard device ID formats – such as IMEI, MAC ID, UUID, etc. It is up to the merchant to capture the device ID that they think is most appropriate for them to identify the device. Our API specifications dictate that the device ID should not be more than 32 characters.

Device fingerprint does not have a "standard" definition or format. The merchant may choose from a set of fields such as:

- IP address
- Http request headers
- Plugins or fonts installed in the device
- Battery information
- OS and its version#
- VPN and browser information, etc.

Verifi/Visa has not released a guidance for this other than that Device Fingerprint should not be more than 45 characters.

The merchant may choose whichever fields makes the best sense. We suggest the merchants discuss with their network and hardware experts and come up with the suitable strategy that works for them. They may use a third-party provider or use their own algorithm by combining hardware, browser or software data elements. The intent of the requirement is to provide evidence that the same device was used for the historical as well as disputed transactions.

For any additional questions related to the new compelling evidence rule, please reach out to your Verifi Representative.