[May 2023]

Verifi Order Insight – Systematic Dispute Deflection –Merchant FAQ

First-party misuse occurs when cardholders report fraud on authorized transactions knowingly or unknowingly.

To combat the risk and rising occurrences of first party fraud, and to balance the cost of cardholder behavior between issuers and merchants, effective April 2023, Visa is updating dispute rules, which will make a cardholder dispute invalid if specific compelling evidence can be provided to support that the cardholder (or authorized person) participated in the transaction. This rule change is known as "Compelling Evidence 3.0" or "CE3.0". With this change, when a cardholder initiates a fraud-related dispute for a card-not-present transaction, merchants will have two options to take advantage of the rule change.

First, during the pre-dispute phase of the dispute processing, the merchant can leverage Verifi's Order Insight® Systematic Dispute Deflection to respond with qualified transaction data, in real-time, prior to the creation and processing of the dispute within Visa Resolve Online (VROL).

Second, for post-dispute the same required information can be delivered during the pre-arbitration response process via the merchant's acquirer. Benefits to merchants vary depending on whether the pre-dispute or post-dispute process is used.

1. What benefits to the payment ecosystem does this rule change enable?

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.

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.

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

Acquirers:

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

2. What does a merchant need to do to prevent disputes with Systematic Dispute Deflection?

For each CNP fraud dispute raised by the issuer, Visa will search for up to 5 eligible historical transactions between the cardholder and the merchant which do not have fraud activity reported against them. Visa will request qualified transaction data for those purchases via Verifi's Order Insight service.

In early 2023, Verifi launched enhancements to the Verifi API for merchant and reseller partners to allow merchants to take advantage of the rule change at the pre-dispute stage. New and existing merchants who opt to participate in Order Insight will need to integrate to the new API specification.

If an online store wishes to benefit from Systematic Dispute Deflection, and they are already enrolled in Order Insight, they need to:

- Understand the additional data requirements for the new rule and determine if they can capture and provide the required information
- Review their data archival and storage policies (i.e., they need to have the data available in an operational database for up to 365 days)
- Review their IT and infrastructure needs to maintain the response SLA requirements (i.e., implement faster and optimized order search if required)
- Be prepared to make the investment necessary to re-integrate to the new Verifi API specification

3. 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.

4. 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.

5. Do all disputes qualify for the benefits of the Systematic Dispute Deflection?

Only Fraud 10.4 CNP (Other Fraud – Card Absent Environment) disputes qualify.

6. Will Systematic Dispute Deflection benefit a merchant if they are already using Visa Secure/3D Secure?

Both Visa Secure and the compelling evidence rule change target the blocking of inaccurate disputes for dispute condition 10.4. To maximize benefits and reduce fraud ratios, both pre-dispute deflection and Visa Secure can be deployed.

7. Are there any merchant category codes (MCCs) that would be excluded in benefitting from Systematic Dispute Deflection

All MCC's that are supported by VisaNet are eligible to take advantage of the new rules.

8. 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.

9. Why is Systematic Dispute Deflection only available for transactions between the cardholder and same merchant? Fraud prevention companies usually see more historical transactions across different merchants from customers with the same IP, user ID, device ID, email etc. which could be used as evidence as well.

At this time, only those transactions that take place between the same merchant and cardholder in VisaNet can qualify for compelling evidence. Cardholder activity across multiple unrelated businesses cannot be considered.

10. 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.

11. Can the qualifying transaction data for compelling evidence be provided through both Order Insight call center and digital issuer experiences?

Pre-dispute compelling evidence rule processing only occurs in real-time as the issuer is submitting the 10.4 dispute to VROL in the call center. Therefore, call center experience is necessary for rules processing.

12. 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.

13. What impact on fraud and dispute ratios can a merchant expect?

If providing the required data at pre-dispute stage, the merchant's fraud and dispute ratios could be lowered. If the required data is provided with pre-arbitration, resulting in the merchant successfully shifting the dispute liability to the issuer, the merchant's fraud ratio can be lowered, but their dispute ratio will reflect the processed dispute.

14. 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).

15. 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.

16. Do both shipping and BOPIS (buy online pick-up in store orders qualify)?

If the purchase being disputed is a CNP transaction, it is eligible.

17. For merchants with multiple CNP storefronts, can they use all store fronts for the customer history of undisputed orders over 120 days?

If the two CNP storefronts can be identified as the same "merchant" (by an identifier such as descriptor or via Visa's ability to link multiple merchant accounts for the same retailer) then yes, purchases across all the storefronts will be considered eligible for historical transactions.

18. Why can't merchants use biometric auth details as evidence? For example, on Android face-match/fingerprint.

Currently the compelling evidence rules do not consider biometric auth data as part of the response data. This may be considered in the future.

19. 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.

20. Do the benefits of Systematic Dispute Deflection extend to recurring Merchant Initiated Transactions (MIT)?

Yes, Systematic Dispute Deflection applies to 10.4 Fraud disputes on recurring transactions. For subscription merchants processing recurring MIT, the Delivery Address, IP Address, Device ID, Device Fingerprint and Account ID data from the initial Customer Initiated Transaction (CIT) can be provided on the response to the historical, non-disputed transactions.

21. How can Systematic Dispute Deflection apply to first-time purchases/transactions?

A historical footprint for past purchases is required for transactions to qualify for Systematic Dispute Deflection. Therefore, dispute initiated on a first-time purchase will not qualify for CE3.0 coverage.

22. 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.

23. What format should Device ID be delivered in?

There are standard device ID formats – such as IMEI; however, it is up to the merchant to capture the device ID they think will best identify the device. Merchants should discuss with their acquirer what strategies work best for their purposes. The intent of the requirement is to provide evidence that the same device was used for historical as well as disputed transactions.

24. Can PAN and tokenized transactions be used as historical transactions for the same customer?

For the tokenized transaction being disputed, Visa will identify the underlying PAN and search for any historical transactions linked with that underlying PAN and merchant. The historical transactions will not be limited to only those where the token was used, it will span all transactions for that underlying PAN and merchant.

25. Should email address be used for Account ID?

The Account ID is the value the cardholder provided when they established the relationship with the merchant. This may be an email address or username to uniquely identify and authenticate themselves to the merchant. This value should be recognizable to the cardholder and should not be an internal value on the merchant's system.

26. 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 time frames.

27. 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.

28. 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 merchandize).

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

29. What if VROL is unable to find 5 historical transactions to request pre-dispute compelling evidence?

VROL will search for up to 5 historical transactions to request Compelling Evidence information during pre-dispute processing. A minimum of 2 transactions are required to have the Order Insight information returned for rule considerations. If fewer than 2 transactions are identified by VROL, the dispute will be processed as it is today, and it will not be eligible to be blocked via CE 3.0.

Sellers can always fall back on the post-dispute processing to provide compelling evidence during the pre-arbitration processing via their acquirer.

Note that via the post dispute flow, all historical transactions must be from the same acquirer, historical transactions across multiple acquirers will not be able to be submitted. (Acquirer A can not reference Acquirer B's historical transactions when submitting the information to VROL)

30. Once the seller responds with compelling evidence, will they be notified that the dispute has been blocked?

Visa will notify Verifi after validation of the Compelling Evidence pre-dispute response whether the dispute has been blocked (leveraging a new call type 9 between Visa and Verifi). Verifi will in-turn, send the notification to the seller when the response was sufficient to prevent the dispute to be raised. Verifi will also send notification if the issuer requested a review of the decision and if the review was approved (i.e., the dispute was allowed to be processed). Details of the technical solution spanning API and reporting enhancements will be available in Fall 2022.

31. Can a seller participate in CE 3.0 and RDR?

Yes, a seller can leverage the compelling evidence rule change to share data and attempt to block the issuer from submitting a dispute. If the rule criteria are not met, the dispute can be resolved via the RDR service (when eligible) to allow the merchant to resolve the dispute at the pre-dispute stage.

Note: Merchant must be enrolled in RDR and the transaction must be eligible for dispute to resolve a pre-dispute with Rapid Dispute Resolution. Please contact your Verifi Representative for more information on RDR.

The Order Insight compelling evidence qualification check occurs before RDR processing.

32. 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.

33. 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 reversed.

34. What impact will the new rule have on TC40s?

TC40 is the name of the report that issuing banks send to Visa to report fraudulent transactions as part of its Risk Identification Service. TC40 is a record of all fraud notices – once the dispute is created and fraud is reported, the fraud report can only be reversed if the new rule requirements are met. Dispute ratio will remain as the dispute has already happened.

35. Can a TC40 be triggered earlier than the dispute for a CE3.0 qualified transaction, which blocked the dispute being raised?

It is possible that there could have been a fraud reported earlier than the dispute being raised. In such a situation, there would be a TC40 record that had been sent earlier, and the dispute initiated later. When the CE3.0 process blocks the dispute, the fraud report will be deleted in Visa's system. However, depending on the timing of the reported fraud, the merchant's fraud ratio may or may not be rectified retrospectively post the CE3.0 validation.

36. If merchant's response to the 2-5 historical transaction selected by VROL is invalid, i.e., not able to block the dispute, is there a possibility of VROL sending a new set of historical transactions?

If the response to the historical transactions is invalid, the dispute will be allowed to proceed normally. The merchant will not be sent another set of historical transactions to respond to. Note that the merchant can still leverage CE3.0 coverage in the post dispute phase by providing historical transaction evidence.

37. What is an OCT transaction and would CE3.0 rules for 120 - 365 days historical transaction eligibility apply to these transactions?

A "OCT" (Original Credit Transaction) is 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. As an example, once could use a AFT to fund a card wallet and use subsequent OCTs to pay from the wallet.

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

38. Who will monitor timeouts and other errors encountered during processing of CE3.0 transactions?

VROL will implement a set of monitoring for the integration between Verifi and VROL for conditions such as Verifi response timing out, merchant response failing to meet the CE requirements, etc.

Verifi will also implement monitoring for the integration between Verifi and the merchant, to monitor conditions such as merchant response timing out, Verifi unable to send a transaction inquiry due to system failure, CE inquiry received for an unenrolled merchant, etc. Please see our training deck for the kind of monitoring we will have available.

39. Should the merchant send back all the data elements necessary to support compelling evidence remedy (IP address, device ID, etc.) for every lookup?

Yes, our recommendation is for them to send as much information as possible in the Verifi API 3.0 to ensure they are able to leverage Compelling Evidence remedy to the maximum possible extent.

40. 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.