What is TC40 Data and How Should it be Used?

KEY TAKEAWAY: TC40 data is a good tool for merchants trying to improve internal fraud prevention measures but is often misused as a proactive way to prevent chargebacks.

When a cardholder claims that they didn't buy something, issuers are required to file a TC40 claim for the transaction. An aggregate report including all reported fraud data is then sent out as the System to Avoid Fraud Effectively (SAFE) report for MasterCard transactions and the Risk Identification Service (RIS) Report for Visa transactions. These TC40 messages are first collated and validated by the card brands and made available to acquirers and, in some instances, merchants for protection against future fraud. Internationally, these reports are readily and easily available for merchants. Domestically, the reports are released to merchants at the discretion of the merchant acquirer/processor. Because these can be extremely large data files, many processors cannot provide the report on a consistent or ongoing basis.

The realities of using TC40 data for chargeback prevention

Issuers use TC40 data to measure the risk of fraud at each merchant since they include all validated instances of fraud. Because TC40 data includes more than just chargeback data, it can help merchants evaluate their current overall fraud prevention and risk management strategy as well as take steps to make it more effective.

How data accuracy impacts false positives and true alert cost

Since the file contains more data than just instances of chargebacks, it can be very limiting in how it helps merchants prevent chargebacks. TC40s are only a reflection of claims by cardholders of fraud, not friendly fraud or disputes that arise as a result of customer dissatisfaction or not receiving goods or services. Services that offer chargeback alerts reliant on TC40 data can result in unnecessary or over-refunding on transactions that don't actually turn into chargebacks (false positives).

TC40s also include fraud data that will never turn into chargebacks because issuers opt to process them as write-offs rather than charging them back. These are typically smaller transactions that would cost the issuer more to process as a chargeback than to refund themselves. If a fraud alert were generated based on this type of data included in a TC40 file, it would result in a false positive for the merchant, who would never incur a chargeback from that type of fraudulent transaction. Additionally, aging of this data can cause disputes to be outside of the allowable window for a chargeback to subsequently occur, resulting in additional false positives.

TC40 data within open-loop processes can increase defects

Additionally, these are just reports of fraud and do not stop the chargeback process. That means that merchants are still on the hook for resolving the dispute and sometimes **after** resolving the dispute … resulting in defects because the merchant has refunded the customer, but the dispute has still been processed into a chargeback. This is a particularly painful scenario as merchants end up double refunding (once on their own terms and once per the issuer after the chargeback goes through) and still paying fines, fees and penalties associated with the chargeback.

Defects increase with the use of this data because of how the information is communicated as well as **when**. The timing of TC40 data in particular can pose problems for merchants who use it as the sole source of truth when it comes to chargebacks. Due to the communication flow of information, merchants typically don't receive information until it is too late, leaving a small window of reaction time that creates a "race to the refund," where merchants try to refund the customer before the chargeback processes.

Understanding CDRN's Patented Closed-Loop Difference

KEY TAKEAWAY: Verifi's Cardholder Dispute Resolution Network's™ (CDRN) patented and proprietary closed-loop process stops chargebacks with unmatched quality, avoiding costly false positives, defects and lost revenue.

Verifi's Cardholder Dispute Resolution Network (CDRN) becomes active the moment a customer files a dispute with the issuer. CDRN's patented closed-loop process connects merchants with issuers, routing the dispute data directly from the source for resolution. The chargeback process is stopped, providing the merchant with up to 72 hours to review the dispute and take action. This differs from competitive solutions' open-loop processes where the chargeback dispute process continues in tandem with the alert being filed and typically requires a response within 24 hours. The resulting "race to the refund" can cause defects (chargeback was not stopped) and additional losses from erroneous fulfillment of goods.

Solutions that use open-loop processes can also be hampered with timing delays in receipt of needed data to help merchants effectively resolve disputes before they turn into chargebacks. With CDRN, the merchant is notified of the cardholder dispute in near real time so they can resolve the issue directly with the issuer (process a refund or credit) to stop the dispute from escalating to a chargeback and avoid expensive fines, fees and penalties. Merchants are always in control and have the time and insight needed to determine the legitimacy of the sale and decide to let the dispute advance and fight the chargeback through representment later.

The CDRN Closed-Loop Difference – Unparalleled Protection. Here's Why:

Comprehensive coverage and unmatched accuracy

- CDRN's, patented closed-loop process is directly integrated with top issuers so merchants can be confident that notifications are real customer-initiated disputes and not false positives (disputes that will not become chargebacks). CDRN provides comprehensive coverage that covers BOTH fraud or non-fraud disputes for any card type.
- Other solutions can have false positive rates of 50 percent or more, meaning merchants are paying for alerts that are not really chargebacks and use aged data that leads to defects. Merchants should take false positive and defect rates into account when evaluating true "coverage" rates of these other solutions. The combination of bad data, communication silos and rushed response leads to defects that end up hurting profits and increasing the total cost of the service.

CDRN STOPS the chargeback process

- CDRN stops the chargeback process and gives merchants up to 72 hours to respond to the dispute in the best way for their business, removing the possibility of defects from the equation and ensuring the merchant has time to make the best, informed decision and also stop fulfillment to prevent additional losses.
- Other solutions do not stop the chargeback process and often require the merchant to respond to an alert within 24 hours. Since alerts are often generated from aged data, this leaves merchants in a "race to the refund," which can lead to costly defects or issuing too much credit.

Robust and timely data direct for the source

- CDRN notifications come directly from the source of the dispute – the issuing bank – so merchants can be certain it is a real, customer-initiated dispute.
- Other solutions combine data from several sources through an open-loop workflow, pushing information to merchants in a fragmented way while demanding a response in a shorter time frame. The combination of flawed and aged data, communication silos and rushed response leads to defects and false positives (alerts that won't become chargebacks) that end up increasing the total cost of the service.

Prompt notifications help stop additional losses

- Merchants receive insight into the chargeback in near real time that helps to stop fulfillment of goods or services for fraud reasons, preventing additional losses.
- Open-loop solutions are also hindered by communication delays, leaving only a 24-hour window in which merchants can respond. By that time, it's usually too late to stop shipment of goods or provisioning of services.