

## Technical Bulletin

### Duplicate Charges and How To Handle Them

CP-TECH-08:14  
November 12, 2008

A “duplicate charge” refers to a shopper being charged twice on an electronic payments card for the same purchase. There can be many possible reasons (including checker error and running a transaction twice) but there are two primary reasons that duplicate charges occur.

#### PRIMARY CAUSES OF DUPLICATE CHARGES

It is technically possible – but unusual – to have double charges outside of these two scenarios.

- The most common cause is that the POS time-out is set *shorter* than the payments system time-out interval.
  - With a slow transaction, the POS tells the checker the transaction failed at the end of the short POS time-out window. The clerk will typically retry.
  - But meanwhile, the payment system’s window is longer and thinks the transaction is still alive – and if its approval arrives inside this longer window, the payment system will log it as a success and won’t generate a time-out reversal (TOR).
  - The cashier didn’t see this approval of the original transaction so the retry is sending a second identical transaction to the processor for the same ticket. The result is two approvals and no TORs – the shopper is charged twice.
- A second reason can be the transaction and its TOR arriving in quick succession at the processor.
  - When clearing an off-line stand-in queue, the “parent” transaction and its TOR might be sent almost simultaneously.
  - The processor won’t have the parent transaction approved and complete before receiving the TOR, and will naturally reject the TOR.
  - Or, the original transaction might go to one of the processor’s circuits while the TOR goes to another point in the processor’s “cloud” – and a different host or data center location. Processors usually synchronize their multiple data centers in seconds or less, but if the transaction goes to one host location and the TOR goes to a different one, the TOR will again be rejected since the original transaction hasn’t been seen yet.
  - The reason this happens is because of new rules enforced by processors that require the payments system to send TORs *immediately* even though they can’t really be handled.
  - Using off-line stand-in will limit the damage to a maximum of just one duplicate (since with off-line stand-in there will be a maximum of one TOR to wrongly deny) while without off-line stand-in there can be multiple retries, therefore multiple TORs therefore multiple duplicates. Please see more detail about this issue in the example starting on Page 4 of this bulletin.

This document and information are supplied to StoreNext Retail Technologies personnel and third parties to assist them in doing business with StoreNext. They are not to be used or distributed for any other purpose.

StoreNext Retail Technologies LLC endeavors to ensure that the information in this document is correct and fairly stated, but does not accept liability for any error or omission.

## HOW TO HANDLE A DUPLICATE CHARGE

If there are double charges, how do you sort them out?

1. First, if there is a situation where significant numbers of double charges are possible, including many off-line transactions, StoreNext and MTXEPS will do everything in our power to clear them prior to a processor's end-of-day – this way, they'll cancel out harmlessly without bridging multiple days. Connected Payments enables Support to undo most or many of the duplicates, since multiple transactions with the identical date/time stamp are unquestionably duplicated charges, and there is also likely to be a denied TOR which let the duplicate stand.
2. StoreNext normally provides a customer-by-customer list of “suspect transactions” to the dealers for retailers who might have been affected by several duplicate transactions. This is a list of transactions that *look* like duplicates – for example, they would have the same card with the same amount but slightly differing time stamps. There is no way to be 100% sure that these are duplicates without first checking these transactions against the POS transactions in the POS Electronic Journal.
  - For example, there could be two transactions for the identical amount on the same card, but the two transactions were five minutes apart. There was no TOR on the first transaction. Is this a duplicate? Answer: the store can't be sure unless they check the POS EJ. The EJ could show that only one order took place, meaning the two electronic payments transactions were duplicates. But on the other hand, the EJ could show that there were two similar tickets separated by a few minutes: for example, a shopper bought a limit-one promotion, then went back through the line and repeated the purchase to get the same promotion a second time.
3. Another source for finding duplicate transaction “suspects” is the Connected Payments Settlement Report. This report compares the processor's report of settled transactions to what Connected Payments has logged.
  - For example, if the processor settlement report shows 100 Visa transactions for a total of \$5,000 but the store reporting shows just 99 Visa transactions for \$4,979, you can be pretty sure that somewhere there's a duplicate Visa transaction for \$21. This one will be very easy to track down on the POS journal. Once you get past two or three transactions, however, it gets much more difficult to find the exact amounts that add up.
  - One word of caution – most processors have a “filtering” system that searches for duplicate transactions and automatically reverses them internally. However, this process normally takes place *after* the settlement report is produced. So, even if the settlement report indicates a duplicate, it's quite possible that the processor has by then found it too and reversed it out.
  - Also regarding the timing, transactions may or may not hit shoppers' accounts before the store knows about it. For example, a duplicate occurs on Monday and the store discovers it on Tuesday. A shopper checking their credit card account on line may see a double charge on Tuesday, but by Wednesday the processor may have already reversed it out. So just because the shopper sees the duplicate doesn't mean the error will actually stick on their account, even without action from the store.



4. Once the store knows which transactions on the “suspect list” are really duplicates, the next step is to reconcile these with the processor.
  - Do take it to the processor! It is *not* a good idea to go to a terminal or virtual terminal and issue a credit if the shopper calls complaining of a duplicate, even if it’s clearly a duplicate according to the POS EJ. This is especially true if only a day or two has passed since the original charge.
  - Why? Because the processor may have already put the reversal wheels in motion. If so, now the shopper will get *two* credits, one from the processor and one from the store, leaving the retailer empty-handed.
  - It is very common for processors to reverse duplicate charge on stores’ accounts several days before the shoppers’ accounts show these credits. So make sure that shoppers know they are usually the last to see confirmations.
5. The fastest and best way to reconcile duplicates with the processor is to use the processor’s on-line settlement database (for example, First Data’s Client Line). In fact, if the store calls the processor’s account representative, this will be exactly the same data and reports the rep uses to look up the same information.
  - The store may find that the processor has reversed the duplicated transaction already, even though the original settlement report indicated the duplicate. If so, all is well and the store can advise the shopper that their account will – or soon will be – credited.
6. However, the store may see that the duplicate transaction has withstood the processor’s filter and still stands. At this point, you have a situation where the store’s EJ has confirmed that there was only one true ticket but the processor records have consistently shown two or more payments with the same card, time and amount.
  - These are the cases where the store’s processor account representative needs to be called and requested to fix the duplicate.
  - When the duplicate has been agreed by the processor’s account representative, the reversal will show on the processor reporting. (For example this will show as an Internal Reversal (“IRV”) on First Data Client Line.)
7. Once retailers see the IRV (or a similar confirmation from other processors), they can be confident in notifying the shopper that their credit will appear in the next few days.
  - Caution: commitment by the processor is not equal to the correction being visible to the shopper’s bank. The processor will back you up with the shopper, but be careful since the processor may or may not have handed the duplicate’s reversal off to the acquiring bank yet. So if the shopper calls Visa to check, it may not be visible on their account yet.
  - If the reversal is *not* provided on the processor’s transaction reporting, you can be pretty sure that there hasn’t been any conclusive motion yet from the processor. In this case, the processor hasn’t taken the necessary steps yet. The store should check again and remind the processor account rep that the necessary correction is still open.



## A TRICKY CASE IN POINT

- A shopper buys \$35 in groceries and tenders with MasterCard credit.
- Either the network, Internet, Connected Payments or the processor is down and the charge does not go through.
- The transaction times out and the clerk informs the shopper to try the transaction again.
- The shopper pulls out \$35 in cash, pays and leaves.
- Two days later, the shopper comes back angry – they just checked their on-line statement, which says the shopper’s card was billed \$35 besides the receipt proving they paid \$35 in cash.
  - Could the store have headed this off proactively?
  - Possibly. By checking the Connected Payments settlement report, they may have seen that it shows \$35 more in MasterCard credit than the store shows on the end-of-day accounting. Then checking the EJ, they would have seen that the order was actually paid in cash.
  - The store could then contact the shopper – but only if they have a way of knowing who the shopper is via, for example, by a loyalty card attached to the transaction in the EJ.
  - If the store notices the settlement report problem, the store may get this fixed with the processor or at least have it in motion before the shopper notices and calls in.
- But what happened here to cause the duplicate charge in the first place?
  - The payment system attempted the credit transaction, but it didn’t go through and timed out.
  - When it timed out, the system generated a time-out reversal. This is because it knows there’s a authorization request out there that will eventually hit the processor, and this request needs to be reversed.
  - When communications was restored, the transaction and the TOR hit the processor in quick succession. But there hadn’t been time for the original “parent” transaction to be fully logged at the processor when the TOR arrived (as little as a fraction of a second later). With no parent transaction to reference yet, the TOR was an “orphan” and denied.
    - At this point, you’re about to ask why OpenEPS doesn’t just hold back sending the TORs for a few minutes – giving the original charge requests time to be logged – and *then* send the TORs. This way, the processor will have the needed parent transactions and so the TORs won’t be denied.
    - Sorry - don’t bother with an ER on this one. Systems *used* to be able to work this way, but not any more.
    - Explanation: new security mandates outside our control.
    - What?
    - Here goes: a thief could buy a gift card with a credit card, activate it and often with an accomplice, use a copy thereof immediately at the current or another store. But before leaving, the original clerk is asked to void / reverse / credit the transaction: the thief pays nothing for a gift card that’s now already been used. There are several variations on this scam, but it only works if there’s a significant gap between the original transaction and the reversal.



- Until recently, OpenEPS delayed sending TORs at least two minutes after the original transaction to give the processor ample time to get the parent transaction logged. But processors and gift card companies know that if credits are sent instantaneously, this minimizes the time gap available for the gift card thieves. You can guess the ending of this story: it's now mandatory for payment systems to send all credits immediately - very unfortunately including TORs.
  - And the result is that the parent transaction and the TOR can arrive at the processor in bang-bang fashion either if there have been processing delays or the transaction and TOR are coming from off-line stand-in.
  - Using off-line stand-in is actually an advantage since a maximum of only *one* TOR will be generated per transaction. On a store-and-forward transaction, the payments system must time-out the original parent, reverse it with the TOR, and then create an identical transaction and approve it back to the POS. That's just one TOR.
  - But without off-line stand-in, there may be multiple retries to get the transaction approved. Although this will always create one more authorization request than there are TORs, the processor may deny more than one of the TORs, causing double, triple etc. charges.
  - *Note: MTXEPS has been working with the processors to find a way to circumvent this problem with the hope of putting a change into production soon.*
- Back to the story: so the shopper's account was mistakenly charged, even though the shopper paid cash.
  - The Connected Payments reports and the settlement reports will show (1) the parent transaction, (2) the TOR and (3) the TOR denial.
  - With this information brought to their attention, the processor account reps will provide the manual/internal reversal for the transaction and credit the shopper. Usually, the Connected Payments and/or settlement reports will be sufficient, but the POS EJ should cinch any disagreement.

To Your Success,




---

Anthony van Seveiter

