June 2023

Smart Payments Reconciliation by Automatically Detecting and Resolving Anomalies

Nagaraju Shiramshetti

Smart Payments Reconciliation by Automatically Detecting and Resolving Anomalies

ABSTRACT

Online payments can fail for a variety of reasons such as insufficient funds, invalid state of the payment instrument, chargebacks, or one of the involved financial systems being unavailable. Anomalies in payment transactions can result in a loss of money either to a customer or business. Current online payment systems cannot handle such anomalies efficiently and at scale. This disclosure describes techniques to perform smart payments reconciliation by automatically detecting and resolving payment anomalies in online payment transactions. The techniques perform automated early detection of anomalies using artificial intelligence and initiate remedial actions. The described techniques can help improve the accuracy and therefore the reliability of online payment systems by reducing errors in accounting records. The described techniques can help improve the customer experience for online shoppers by making sure that customers are correctly charged or issued an appropriate refund based on purchased or returned items.

KEYWORDS

- Payment reconciliation
- Payment instrument
- Fraudulent customer
- Authorized chargeback
- Unauthorized chargeback
- Payment anomaly
- Online payment
- Insufficient funds
- Vendor risk
- Payment validation
- Transaction fraud
- Anomaly detection

BACKGROUND

Online stores can currently handle online payments via well-established workflows, including item dispatches and where necessary, returns and refunds. The transfer of funds involved in such transactions can fail for a variety of reasons. These can include insufficient funds in the bank account, invalid state of the payment instrument (credit card or debit card), chargebacks, payment profile wipeout, expiration of a payment instrument after using it, a block on a payment instrument (by a financial institution, based on customer request), or one of the involved financial systems being unavailable. Such payment failures or anomalies can result in a loss of money either to a customer or business. Many online payment systems are not able to handle these efficiently and at scale. Early detection of anomalies in payment transactions can help save money for businesses and customers.

DESCRIPTION

This disclosure describes techniques to perform smart payments reconciliation by automatically detecting and resolving payment anomalies.

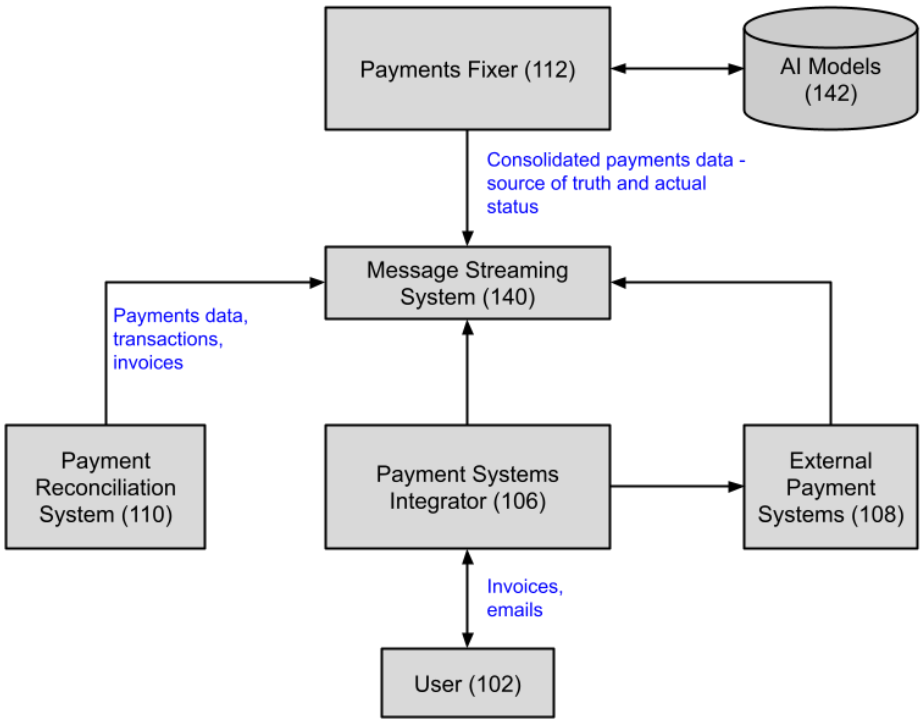

Fig. 1: Architecture diagram

Fig. 1 illustrates an example architecture diagram, per techniques of this disclosure. The architecture includes a payment systems integrator (106), one or more external payment systems (108), a payment reconciliation system (110), and a payments fixer (112) that communicate via a message streaming system (140). The payments fixer may implement artificial intelligence (AI) models (142).

An online store (not shown) communicates with the payment systems integrator to initiate a payment checkout transaction when a customer initiates a purchase using a valid payment instrument, or to initiate charges/refunds based on items being shipped to or returned from a customer. The payment systems integrator provides abstraction application programming interfaces (APIs) that enable the online store to initiate a checkout, and to process charges or refunds. The payment systems integrator communicates with various external payment systems such as digital payment or wallet applications to initiate transactions, charges, or refunds.

The payment reconciliation system collects data posted to the payment systems integrator and the results of transactions from the various external payment systems. The data are consolidated and stored internally based on business, customer, purchase or return transaction.

The payments fixer obtains data from the payments reconciliation system on a continual basis. The data is used to train and generate the AI models. When a discrepancy is discovered in an order for charge or refund, the payments fixer mitigates the discrepancy.

The message streaming system can be implemented using any suitable technology, e.g., using a publish-subscribe (pub-sub) model. The message streaming service receives notifications from online stores and from different external systems.

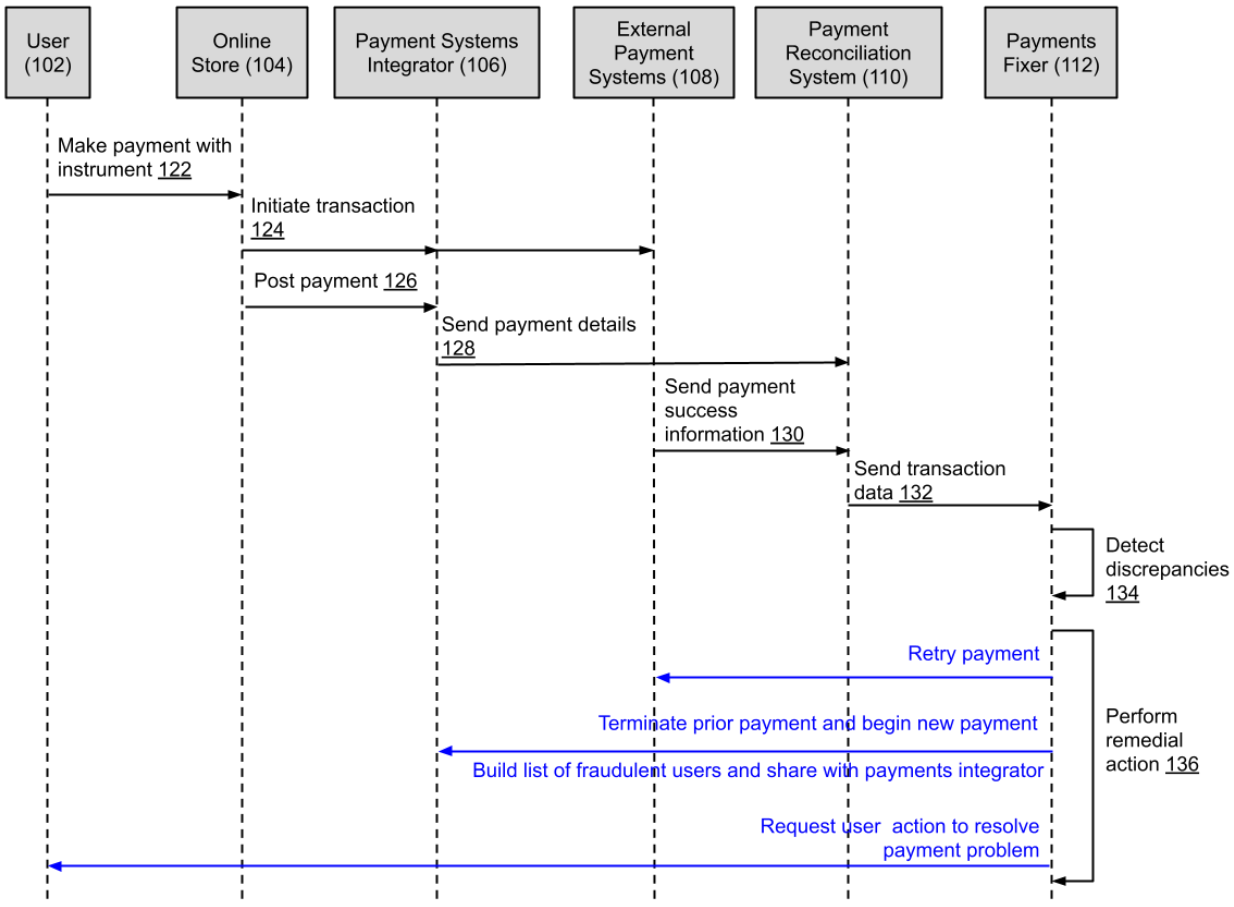

Fig. 2: Smart payments reconciliation by detecting and resolving payment anomalies

Fig. 2 illustrates smart payments reconciliation by automatically detecting and resolving payment anomalies, per techniques of this disclosure. A user (102) makes a purchase from an online store (104). This purchase is made by making an online payment (122) with any suitable online financial instrument. The online store initiates two related steps after the user has made payment. First, the transaction is initiated (124) from the account of the online store by sending a message to the relevant external payments system (108) via a payment systems integrator (106) to ensure that the customer is able to purchase a product. Second, a record of the payment having been initiated by the customer is posted (126) to the payment systems integrator (106).

The payment systems integrator in turn sends (128) the payment details to the payment reconciliation system (110). The payments reconciliation system obtains the relevant payment data posted to the payments system integrator by the online store. It also obtains relevant results of related transactions from various external payments systems. The payments reconciliation system then consolidates and stores these internally based on identifiers: business, customer, purchase or return, transaction. Payments data in this case can refer to information about the invoice, the purchase order or the refund order, items purchased, purchase amount, and tax details. When a payment is successfully made, the external payments system sends (130) this information to the payment reconciliation system. The payment reconciliation system then passes on all relevant information pertaining to the transaction data (132) to the payments fixer (112).

The payments fixer obtains data from the payments reconciliation system on a continual basis. This data is fed as input to an artificial intelligence (AI) model that is trained to detect discrepancies (134) in online transactions on an ongoing basis. The model can be trained based on user-permitted prior transaction data. When an anomaly is detected, remedial actions are performed (136) by the payments fixer.

Remedial actions include a variety of actions. For example, one of the remedial actions is to retry payment. The retry time for a charge or a refund can be determined by the customer, geography, instrument type, and other relevant factors. Retrying is done with caution since it invalidates the instrument, which can make it impossible to recover the money in the future. Further, card networks impose strict limits on retries and levy hefty fines for exceeding such limits. The platform application programming interface (API) contract specifies that a payment systems integrator should not retry and allow maximization of the use of the network limits. Another action is to terminate the prior transaction with the original payment system and begin a new one with a different payment system. It provides an option for automatic refunds to customer instruments that were stolen and used by fraudulent customers. In this case, the loss is accepted to prevent chargebacks with penalties from banks and to provide a positive customer experience.

The payments fixer can also request the customer who initiated the online purchase to resolve payment problems with their instrument. Customers may be able to do so by revalidating the initial payment method, or trying a new payment method. When a customer revalidates the payment, the payments fixer receives a notification from the external payment systems and automatically makes a charge or refund decision. Further, based on detected data discrepancies, the payments fixer can build a list of potentially fraudulent customers to avoid charge failures. Charge failure can occur due to various factors such as: lack of a valid instrument on the account for the system to make a charge (e.g., customers can close payment profiles, or remove an instrument); insufficient funds in the account; a control on the account requested by the customer blocks the action (e.g., “vendor denied”); a customer can call the bank and chargeback the money by raising a dispute that the item was not received, or that the charge is unauthorized.

Fraudulent customers can be identified using various factors such as payment profile Identification, user identification, shipping and/or delivery addresses, instruments or payment signature, etc. The list can be shared with the payment systems integrator to take additional actions, e.g., prevent such customers from creating new orders, require additional payment authentication, etc.

Example transaction

Table 1 shows an example of a transaction.

OrderId	Product Code	Description	Pre Tax	Tax Amount	Total Amount	Currency	Transaction State	Transaction State (External System)
Order-7457	12345	Smartphone (Unlocked)	899	79.79	978.79	USD	Succeeded	Succeeded
Order-7457	12346	Customer appeasement	-150	-13.32	-163.32	USD	Succeeded	Succeeded
Order-7457	10001	Warranty Care	199	17.67	216.67	USD	Succeeded	Succeeded
Order-7457	10001	Refund	-199	-17.67	-216.67	USD	Succeeded	Pending
Order-7457	12346	Refund	150	13.32	163.32	USD	Succeeded	Pending
Order-7457	12345	Refund	-899	-79.79	-978.79	USD	Succeeded	Pending

The described techniques can help improve the accuracy and therefore the reliability of online payment systems by reducing errors in accounting records. A payments fixer as described

herein can also help to ensure that a business complies with all applicable regulations. This can help in avoiding fines and penalties and can protect businesses from financial losses. The described techniques can also help improve the customer experience for online shoppers by making sure that customers are correctly charged or issued an appropriate refund based on purchased or returned items.

CONCLUSION

This disclosure describes techniques to perform smart payments reconciliation by automatically detecting and resolving payment anomalies in online payment transactions. The techniques perform automated early detection of anomalies using artificial intelligence and initiate remedial actions. The described techniques can help improve the accuracy and therefore the reliability of online payment systems by reducing errors in accounting records. The described techniques can help improve the customer experience for online shoppers by making sure that customers are correctly charged or issued an appropriate refund based on purchased or returned items.