Gateway Bulletin GB-2014-06 Action Recommended
Gateway Advisory: Partial Payment Flag

October 17, 2014

Overview

The purpose of this bulletin is to describe the Partial Payment flag and best practices around balancing activity on and off the ledger. Gateways are encouraged to implement best practices and understand the Partial Payment flag to mitigate errors that can result in fraud if undetected. The tfPartialPayment flag is set by the sender to specify a payment where the beneficiary can receive less than the specified amount.

Background

Payments are normally made by specifying how much to deliver to the beneficiary and the maximum amount the originator is willing to spend. For normal payments, the payment only succeeds if the full amount specified to be delivered can be delivered. The sender is responsible for paying all transfer fees and currency conversion costs. The Ripple marketplace sets the rates used to convert the currency.

However, there are other common payment cases where it is appropriate for the receiver of the funds to pay all fees. In fact, with most consumer credit/debit card payments, the receiver (merchant) pays transaction fees. The customer is quoted a price by the merchant. The customer's account is debited exactly the quoted amount but the amount credited to the merchant's account is out of the consumer's control.

A *"partial payment"* is the terminology that Ripple uses to describe a payment transaction that specifies that *less than* the originally specified transaction amount is permitted to be delivered.

Sometimes, funds are sent to the wrong the address or must be returned for some other reason. In this case the beneficiary (the person returning the funds) needs to return all received funds, but is not responsible for paying fees or currency conversion costs above the amount received.

The partial payment feature frees gateways from the obligation of paying a fee in order to return an unsolicited payment. This protects gateways against accounts configuring their accounts to receive funds *and* fees from the gateways for unsolicited funds. For a return payment, the sender specifies the payment is a "partial payment" (a term that has specific meaning within the Ripple protocol). **A partial payment may deliver significantly less than the specified payment amount**.

Partial payments are a feature. Without this feature returning funds would be extremely cumbersome, perhaps requiring multiple attempts at guessing the market rate and making smaller payments to return as much as possible to the sender.

Technical Application
Improperly crediting incoming payments in core accounting systems could lead to theft. Attackers can exploit these errors and withdraw funds from a gateway. To correctly credit incoming payments, receiving systems must do the following:

For applications interfacing directly with rippled or ripple-lib
1) Only consider incoming payments with the result "tesSUCCESS"

2) If the incoming payment has a "meta.DeliveredAmount" field, use it to determine the delivered amount of the incoming payment.

3) Otherwise, if the incoming payment does NOT have the "meta.DeliveredAmount" field, use the "Amount" field to determine the delivered amount of the incoming payment.

For applications interfacing directly with Ripple REST
Ripple REST applications should use the "destination_balance_changes" field (NOT "destination_amount") to determine the delivered amount of the incoming payment.

For applications interfacing with gatewayd
No special steps are necessary.

For users interfacing with the Ripple Trade Client
Versions v1.0.10-1 and later correctly display the delivered amount of payments.

Background Documentation
The partial payment flag (tfPartialPayment 0x00020000) is documented on the Ripple Developer Portal. Please review this documentation.

How an Attacker Might Exploit Incorrect Implementations
An attacker

- creates a payment transaction
  - sets the partial payment flag (tfPartialPayment 0x00020000)
  - fills the "Amount" field with more funds than available
- submits the transaction

The recipient (e.g. gateway)

- only checks the "Amount" field

- incorrectly credits the user to match the "Amount" field
    - DO NOT DO THIS!

An attacker

- withdraws the assets which have been incorrectly credited to them

Further Risk Mitigation

Hot wallets should never contain more funds than a business can afford to lose. If a hot wallet contains more currency than is necessary to support transactions, the excess should be removed as a cautionary measure.

Auditing Ledgers: Best Practices

Gateways are encouraged to implement best practices for auditing ledger activity. Every ledger close, gateways and exchanges should ensure that their liabilities match their assets to detect and respond to fraud or discrepancies.

If a discrepancy is found, immediate action should be taken, including but not limited to notifying administrators and stopping gateway activity until the discrepancy is resolved. Gateways can also use the global freeze feature to freeze the issuance until they determine the source of the discrepancy. You can read more about the freeze feature in Gateway Bulletin GB-2014-02.

Additional Resources:

Ripple Wiki Resource on Return Payments
Development Portal Documentation on Transactions
Gateway Bulletins in the Ripple Knowledge Center