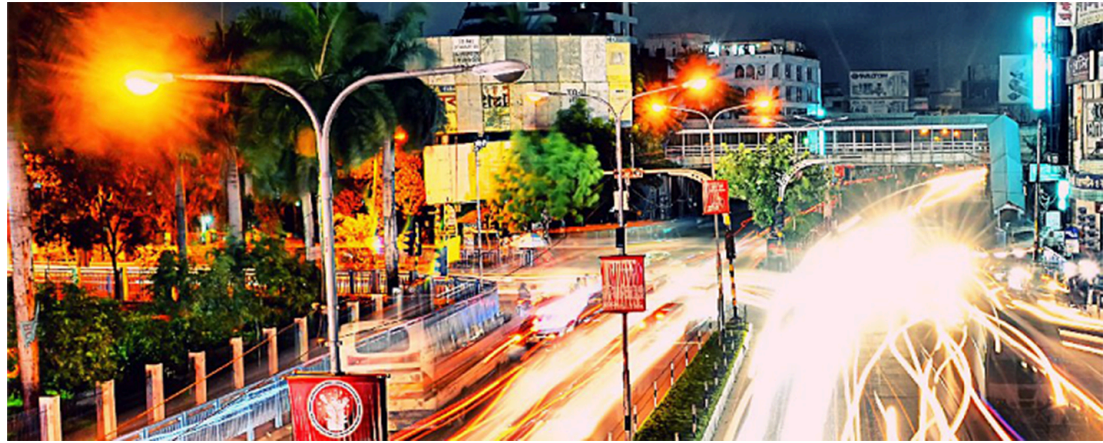


Payouts Getting Started Guide for Acquirers



© 2020. Cybersource Corporation. All rights reserved.

Cybersource Corporation (Cybersource) furnishes this document and the software described in this document under the applicable agreement between the reader of this document (You) and Cybersource (Agreement). You may use this document and/or software only in accordance with the terms of the Agreement. Except as expressly set forth in the Agreement, the information contained in this document is subject to change without notice and therefore should not be interpreted in any way as a guarantee or warranty by Cybersource. Cybersource assumes no responsibility or liability for any errors that may appear in this document. The copyrighted software that accompanies this document is licensed to You for use only in strict accordance with the Agreement. You should read the Agreement carefully before using the software. Except as permitted by the Agreement, You may not reproduce any part of this document, store this document in a retrieval system, or transmit this document, in any form or by any means, electronic, mechanical, recording, or otherwise, without the prior written consent of Cybersource.

For Government or defense agencies: Use, duplication, or disclosure by the Government or defense agencies is subject to restrictions as set forth the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and in similar clauses in the FAR and NASA FAR Supplement.

For civilian agencies: Use, reproduction, or disclosure is subject to restrictions set forth in subparagraphs (a) through (d) of the Commercial Computer Software Restricted Rights clause at 52.227-19 and the limitations set forth in Cybersource Corporation's standard commercial agreement for this software. Unpublished rights reserved under the copyright laws of the United States.

Authorize.Net, eCheck.Net, and The Power of Payment are registered trademarks of Cybersource Corporation. Cybersource, Cybersource Payment Manager, Cybersource Risk Manager, Cybersource Decision Manager, and Cybersource Connect are trademarks and/or service marks of Cybersource Corporation. Visa, Visa International, Cybersource, the Visa logo, and the Cybersource logo are the registered trademarks of Visa International in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Contents

Introduction to Payouts	5
How Payouts Work	6
Payouts Transaction Flow Using an External Processor	8
Payouts Transaction Flow Using Visa Platform Connect (VPC)	9
Payouts Usage	10
Visa Direct	10
Original Credit Transactions	11
Fast Funds	11
Visa Platform Connect (VPC)	13
Business Application Identifiers	13
Transaction and Velocity Limits	15
Auxiliary Services	17
BIN Lookup Service	17
Secure Card Capture Service	17
Tokenization Service	18
Account Validation Service	18
FX Service	19
Transaction Search Service	19
Reporting Service	19
Acquirer Setup Summary	20
Merchant Setup Summary	22
Acquirer Setup	23
Acquirer Setup for Visa Components	23
Acquirer Setup for Cybersource Components	27
Setting Up a Reseller	31
Option 1: Setting Up a Reseller	32
Option 2: Reseller Portfolio with a Single MID per Use Case	33
Option 3: Acquirer Portfolio with Single MID	34
Merchant Setup	35
Acquirer (Financial Institution) Responsibilities	36
Merchant Readiness Activities	36
Cybersource Activities	38

Merchant Onboarding.....	39
Configuring Merchant Information.....	39
Additional Merchant Contact Information.....	40
Configuring Processor Settings.....	41
Adding Processor.....	41
Supporting Products and Features.....	43
Business Center Overview.....	43
Reporting API.....	43
Secure Acceptance.....	46
Tokenization.....	49
Virtual Terminal.....	49
BIN Lookup.....	50
Acquirer Risk Control.....	53
Payouts Settings.....	53
ECI Settings.....	53
API Settings.....	54
FX Rates API.....	54
Merchant Registration for Testing Transactions.....	54
Sandbox Testing.....	55
Going Live.....	55
Glossary of Abbreviations.....	56
Debit Fast Funds Markets in the World.....	59
Cybersource Error Codes.....	61

Introduction to Payouts

CyberSource Payouts enables businesses to take advantage of Visa Direct service to deliver funds directly to a recipient's eligible Visa or Mastercard account.

Unlike a purchase transaction, which debits a cardholder's account, Visa Direct credits the cardholder's account using an Original Credit Transaction (OCT), in most cases within 30 minutes (if enabled for Fast Funds) or a maximum of two business day. An innovative and convenient option for businesses to reimburse, refund, rebate, or pay compared to those that require a checking account or bank routing number as most consumers or small business have a bankcard readily available. Recipients can receive their funds in near real time 24x7x365 which is much quicker than waiting for a check or Automated Clearing House (ACH) bank transfer to clear. Senders also reduce costs by avoiding the processing of paper checks. CyberSource as a channel for Visa Direct, increases access to a key Visa service.

The standard BIN is inadequate for working with Payouts and the business requires a new full financial BIN. • Full liability to pay lies fully with the acquirer. Once the issuer accepts the transaction, the transaction is complete and the funds are pulled from the acquirer in the next settlement window. No reversals or chargebacks can originate from the acquirer. If funds are mistakenly sent, the only recourse available to the acquirer is a good faith adjustment from the issuer.

Consumers and businesses can experience CyberSource Payouts through two main ways:

- Funds Disbursements Businesses (merchants, government entities, or corporations) send funds to a consumer's card account. Examples include insurance claims, corporate and manufacturing rebates, affiliate and contractor payouts, expense reimbursements, and government disbursements (such as value-added tax refunds).
- Person to Person Consumers send funds to their card account or to another person's card account. Examples include from "me to me", "me to you", prepaid loads, and credit card bill payments.

How Original Credit Transactions differ from Traditional Credit Transactions

Payouts differ from a regular purchase transaction in the following ways:

- Funds flow in a different direction. Payouts push funds to an account versus how a traditional credit pulls funds from an account.
- Full financial Business Identification Number (BIN) is required. While many businesses have a BIN, their current BIN is the standard dual message BIN that is used by most ecommerce merchant processors. The standard BIN is inadequate for working with Payouts and the business requires a new full financial BIN.

- Full liability to pay lies fully with the acquirer. Once the issuer accepts the transaction, the transaction is complete and the funds are pulled from the acquirer in the next settlement window. No reversals or chargebacks can originate from the acquirer. If funds are mistakenly sent, the only recourse available to the acquirer is a good faith adjustment from the issuer.

The following points provide additional technical background around CyberSource Payouts:

- Both the merchant (ICS setup/implementation) as well as their acquirer (VISA Direct setup, BIN creation or update) must be setup and configured properly to use this service.
- CyberSource generally works with Acquiring Solutions and other acquirers/partners to set them up with Visa Direct and the Payouts services, guiding the acquirer on the steps to setup both sides (acquirer setup and merchant setup).
- "ics_oct" is the SCMP application name for Payouts.
- Many reporting options are available within the CYBS platform and directly from Visa Online (VOL).

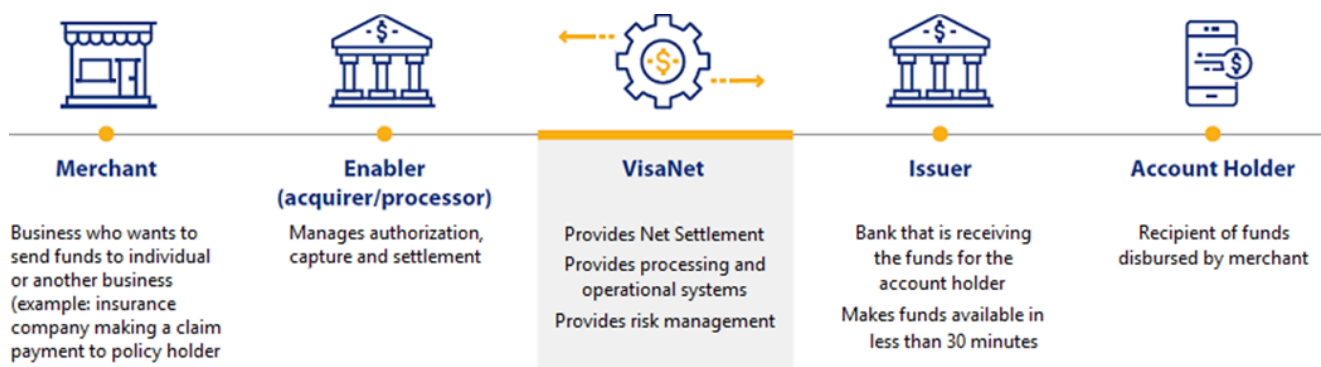
How Payouts Work





An original credit transaction (OCT) enables credit and refund capabilities of the card networks to facilitate sending funds to a card account.

The OCT transaction behaves in many ways like a stand-alone credit. No original authorization and capture are credited back. It is a one-time sending of funds to the customer's card account. The Mastercard equivalent of Payouts is called *MoneySend* (Transaction Code 28).

Cybersource Payouts uses the same four-party model as a traditional card transaction. Every transaction requires a merchant who originates the transaction, an acquirer, an issuer, and a cardholder (person or business receiving the funds).

For traditional purchases, the merchant is the entity that is receiving payment, typically in exchange for goods and services. For Payouts, the originating entity (acquirer, enabler, or merchant) is the entity that is sending the funds, either for themselves as an individual merchant, or as a service provider on behalf of their merchants as noted in the figure below.

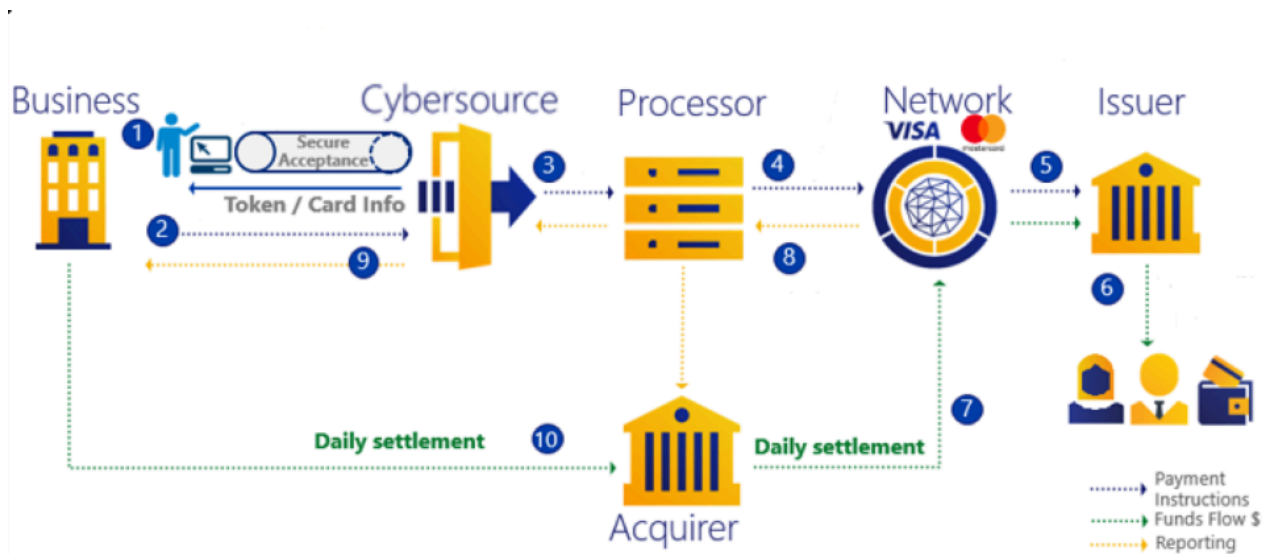


	Visa Customer Debit	Visa Small Business Debit	Visa Reloadable Prepaid	Visa Credit
				
OCT Supported	Yes	Yes	Yes	Varies by market
Issuer Treatment	Deposit to associated bank account.	Deposit to associated bank account.	Load to prepaid account balance. Only for reloadable accounts where issuer verifies cardholder.	Payment to credit card account.
OCT Supported by Issuers	Yes	Yes	Yes	Yes
Timing of Funds Availability by the Issuer	Fast Funds*	Fast Funds*	Fast Funds*	Within two business days of issuer approval of OCT

* The Fast Funds program mandates that funds be available to the recipient within 30 minutes of the transaction.

Payouts Transaction Flow Using an External Processor

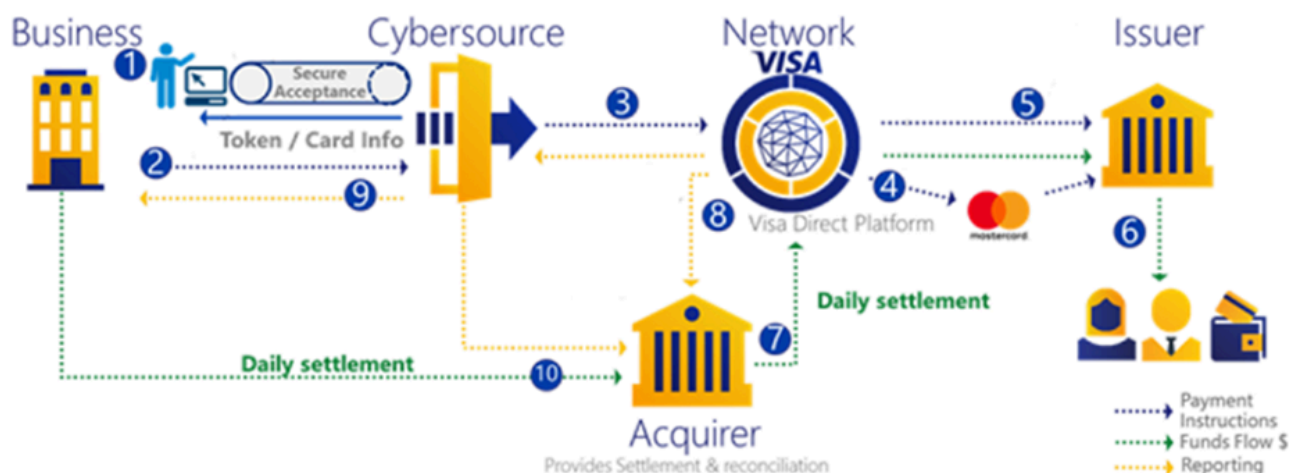
The following sequence occurs when a Payouts transaction is processed using an external processor. The transaction flow differs slightly from when Cybersource services process the transaction.



1. Tokenization can be used to reference payment account data.
2. The business calls the Cybersource API with the token to disburse payment to the recipient.
3. Cybersource sends the payment instruction to the processor (processor integration differs according to the processor).
4. The processor routes the transaction to the network.
5. The network routes the transaction to card issuer for approval.
6. The issuer credits the recipient account in real time. (Actual fund availability varies by financial institution. Visa requires US issuers to make funds available to its cardholders within a maximum of 30 minutes of approving the transaction.)
7. The networks settle with the acquirer by sending funds from the acquirer settlement account.
8. The networks deliver settlement data and reports to the processor. The processor sends details to the acquirer.
9. Daily reports are sent to the merchant from Cybersource and processor.
10. Funds are transferred from the business bank account to the acquirer bank for daily settlement.

Payouts Transaction Flow Using Visa Platform Connect (VPC)

When processing a Payouts transaction using Cybersource services instead of an external processor the transaction flow with an external processor differs slightly.



1. The business designs the customer experience, collects debit card information, and initiates payment. (You can also use tokenization from Cybersource to reference payment account data.)
2. The business calls the Cybersource API with a token to disburse the payment to the recipient.
3. Cybersource sends payment instruction to VisaNet.
4. Mastercard personal account numbers (PANs): Visa uses a Payment Gateway Service form (PPGS) to route transactions to Mastercard for processing.
5. The network routes the transaction to the card issuer for approval.
6. The issuer credits the recipient account in real time.
7. The networks settle with the acquirer sending funds from the acquirer settlement account.
8. The networks deliver the settlement data and the reconciliation data for reporting.
9. Cybersource transaction details and summary-level reporting are available for access by the business and the acquirer.
10. The funds transfer from the business bank account to the bank for daily settlement.

Payouts Usage

Here are some examples of how Payouts can be used.

- **Money Transfer**—Send funds to a payment card account or to another customer's payment card account. In most markets, Money transfer transactions can be sent for amounts up to 5,000 USD and are subject to government regulations.
- **Funds Disbursement**—Send funds from merchants, government entities, or corporations to eligible payment card accounts. Examples include insurance claim reimbursements, corporate and manufacturing rebates, cash compensation, affiliate and contractor payouts, expense reimbursements, government disbursements (such as value-added tax refunds), loan disbursements, online gambling, and lottery payouts. Funds disbursements can be sent for amounts up to 50,000 USD. All payouts are subject to local regulations and could be further limited by controls defined by acquirers.
- **Merchant Settlement**—Settle payments between acquirers or payment facilitators and their merchants much faster. Merchant Settlement transactions can be sent for amounts up to 50,000 USD.
- **Digital Wallets and Instant Deposit**—Move funds out of a digital wallet and deposit funds into a recipient's payment card account. Digital wallet disbursement transactions cannot exceed 50,000 USD.
- **Prepaid Load**—Add value to a reloadable prepaid card. For a prepaid card to be eligible, the card must be a reloadable card for which the card issuer has performed the Know Your Customer process. (A separate prepaid load service called Visa Ready Link is currently available in the U.S. market. For information on Visa Ready Link, contact your regional Visa representative.)
- **Credit Card Bill Payment**—Pay a Visa or Mastercard credit card bill.

Visa Direct

Visa Direct is a payment service that provides the ability to send funds to eligible Visa debit, credit, or reloadable prepaid cards. The send element is in contrast to the traditional withdrawal element of most transactions in which funds are withdrawn from an account.

Visa Direct uses a financial message called the original credit transaction (OCT), which passes between the sender and recipient through VisaNet and carries the destination's 16-digit Visa account number. After a transaction is initiated, VisaNet directs the payment message to the receiving issuer, who then processes the transaction and posts funds to the recipient's account.

Customers and businesses can use Visa Direct through several services:

- **Money Transfer** enables customers to send funds to their Visa account or to another person's Visa account.
- **Prepaid Load** enables customers to add value to a Visa reloadable prepaid card.

- **Credit Card Bill Pay** enables customers to transfer funds to their Visa credit card account to pay their credit card bill.
- **Funds Disbursements** enables businesses (merchants, government entities, or corporations) to send funds to a customer's Visa account. Examples include insurance claims, corporate and manufacturing rebates, affiliate and contractor payouts, expense reimbursements, and government disbursements (such as value-added tax refunds).

Original Credit Transactions

An original credit transaction (OCT), is the financial message in [Visa Direct \(on page 10\)](#) that is passed between the sender and recipient entities. An OCT is similar to a merchandise return in that it credits funds to a Visa account. However, unlike a merchandise return, an OCT is not tied to a prior purchase transaction made by the cardholder. The OCT is a unique transaction type, with its own field requirements, processing needs, and economics.

An OCT is an economical way to send funds to a card. The fees associated with an OCT can be significantly lower than the cost incurred in a purchase or a refund.

The acquiring BIN that is used to originate an OCT must be a full financial BIN and cannot use a standard dual-message BIN that is used by most e-commerce merchant processors.

The key characteristics of an OCT:

- The OCT is a good-funds transaction, meaning that after the issuer approves the OCT authorization, the issuer is guaranteed to receive money from the card network. The acquirer cannot reverse an OCT to retrieve funds in the event of an error. However, the acquirer can correct mistakes using a good-faith adjustment from the issuer.
- When the OCT is approved, the issuer must make funds available in the recipient's account within the time specified by the card network. Globally, Visa rules for [Fast Funds \(on page 11\)](#) require that debit and prepaid card issuers make funds available in the recipient account within 30 minutes of authorization. If Fast Funds capabilities are not mandated, Visa rules for conventional funds availability require that the issuer deposit funds from an incoming OCT into the recipient's account within two business days.
- OCT is a full financial single message. The initial authorization message also carries the clearing component. After an issuer accepts an OCT, the transaction record is cleared. The originator does not submit a capture or clearing record for the transaction.

Fast Funds

An issuer that participates in the Fast Funds program must make funds available to the recipient within 30 minutes of approving the authorization of an OCT, but no later than within two business days of receiving the OCT message. Recipients have faster access to their funds, and it greatly improves the experience for both senders and recipients. Fast Funds issuers might also benefit from interchange rate incentives.

Visa and Mastercard mandated that debit card issuers support Fast Funds. Fast Funds mandates are in effect in the US, Canada, and other markets around the globe. Fast Funds availability around the globe is in various stages of deployment.

Country	Audience	Effective Date
All new issuers in Asia Pacific (AP) and Central Europe, Middle East, and Africa (CEMEA)	New debit and prepaid card issuers	January 1, 2012
All countries in AP and CEMEA, including India (April 15, 2015)	Debit and prepaid card issuers	October 13, 2012
Armenia, Azerbaijan, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Moldova, the Philippines, Tajikistan, Ukraine, and Uzbekistan	Credit, debit, and prepaid card issuers	April 14, 2012
Australia	Debit and prepaid card issuers; domestic only	April 19, 2013
Japan	Debit card issuers, domestic only	October 13, 2018
Canada	Debit, prepaid, proprietary, and proprietary ATM cards that carry the PLUS mark	April 14, 2018
Europe Region	Direct debit card, deferred debit cards with CVV2 and PAN on the card, and prepaid cards	October 13, 2018
LAC	All debit and prepaid card issuers	April 14, 2018
Russia	Credit, debit and prepaid card issuers	October 15, 2011
US	Debit and prepaid card issuers	October 15, 2015

A [complete list of countries \(on page 59\)](#) in which the Fast Funds service is available is at the back of this guide.

Visa Platform Connect (VPC)

Cybersource Payouts supports two processor connections: Visa Platform Connect (VPC) and external processors.

VPC connects the merchant directly to the payment network, bypassing the need for a third-party payment processor. Instead, your connections are facilitated through an acquirer processor that hosts VPC connections. Currently, Cybersource Payouts supports two primary networks:

- **Visa:** Visa Direct comprises enhanced message types that are used for depositing funds to a card account (OCT). Visa Direct also provides the deposit funds for an OCT by withdrawing the funds from a card account in a process known as an Account Funding Transaction (AFT). Visa Direct also provides the processes, policies, and underlying operating regulations and mandates for issuers and acquirers. Currently, Cybersource Payouts does not support AFTs.
- **Mastercard:** Mastercard Send is the program used for transferring funds to Mastercard products. Mastercard Send enables customers to move funds quickly to friends, family, and even their own Mastercard card accounts. Mastercard Send enables you to also receive disbursements from businesses and governments using the Mastercard Network. Currently, Mastercard is supported only as a recipient card type.

VPC transaction processing has the following characteristics:

- **Acquirer Approval:** You must obtain approval from your acquirer before requesting this type of transaction.
- **Merchant Category Code:** You must use the appropriate merchant category code depending on the business flow: for all OCT transactions except for money transfers, use your merchant category code. For money transfer OCT transactions, use 6012 or 4829 as the category code.
- **Transfer Amount Limitations:** For customer-funded transactions (such as money transfers), the amount must be less than or equal to 10,000 USD for domestic transactions and 2,500 USD for cross-border transactions, unless otherwise noted. For any other transactions, the amount must be less than or equal to 50,000 USD, unless otherwise noted. See [Transaction and Velocity Limits \(on page 15\)](#) for more information.

Business Application Identifiers

Acquirers, service providers, and merchants must use an appropriate Business Application Identifier (BAI) and a Merchant Category Code (MCC) in the OCT authorization request message and the clearing and settlement message, to correctly identify the type of OCT and merchant or

business entity that is originating the transaction. Both the BAI and the MCC enable the issuer to recognize the underlying business use of the OCT. The MCC must accurately represent the merchant, acquirer, or service provider and payment facilitator of the OCT transaction.

The BAI is used to identify the type of payment being facilitated with the OCT. The accuracy of the BAI is critical in ensuring effective processing, pricing, reporting, and risk management of OCTs. The Visa Direct team approves BAI use cases on the Program Information Form (PIF). After approval by Visa, the acquirer or merchant enters the approved BAI(s) during the onboarding process. If an acquirer onboards a merchant with a BAI that is not approved by Visa, VisaNet can decline those transactions.

The following types of BAIs for funds disbursement are supported:

BAI	Definition
FD	Used for merchants, government entities, or corporations to send funds to eligible payment card accounts. Examples include insurance claim reimbursements, corporate and manufacturing rebates, cash compensation, affiliate and contractor payouts, expense reimbursements, government disbursements (such as value-added tax refunds), loan disbursements, online gambling, and lottery payouts.
BB (Supplier Payment)	Used by businesses to send payments for business-related supplies.
CP (Credit card bill payment)	Used for sending funds to a credit card account as a payment.
GD (Government disbursement)	Used for government payments including social security payments, unemployment benefits, disability benefits, jury duty, and disaster and emergency relief payments.
GP (Gambling/Gaming Payouts)	Used for casino payouts at gaming floors and for gambling that is not considered online gambling.
LO (loyalty)	Used to send payment for canceled services, refund deposits, employee rewards, purchase rebate payments.
MD (Merchant settlement)	Used for merchant payments for purchase transaction processing in which the processor sends settlement payments to a card account using OCT.
OG (Online gambling payout)	Used for payout of winnings from online gambling merchants.

BAI	Definition
PD (Payroll & Pensions Disbursements)	Used for independent contractors working for a temporary staffing agency or directly with an employer who submits a time sheet or who completes a project, and is paid to a bank account by using a debit card.
TU (Prepaid card top up)	Used for customers to add value to an eligible, reloadable prepaid card. For a prepaid card to be eligible, the card must be a reloadable card for which the card issuer performed a Know Your Customer (KYC) procedure.

Although Cybersource supports OCT, it does not yet support AFTs. The following types of BAIs are supported only for OCTs or the send portion of the customer-funded (money transfer) transaction.

BAI	Definition
AA	Used by a sender moving money from his own account to his card account (me-to-me money transfer).
PP	Used for sender sending money to someone else's account.
BI	Used for a money transfer that is initiated from an online banking system (bank-initiated transaction).
WT	Used for withdrawal of funds from a digital wallet to a card account.

Transaction and Velocity Limits

Cybersource Payouts enables acquirers to set limits on the number of Payouts transactions and the maximum amount of a single transaction and aggregate transactions during defined periods of daily, weekly, or monthly. These limits can be configured and changed by acquirers for each merchant as needed in Cybersource systems.

Limits are applied on each transaction and enforced by VisaNet based on the program type as identified by the Business Application Identifier (BAI) and may vary by jurisdiction, country, and program basis.

Transaction Limits: To ensure a positive user experience for a client, the originating entity confirms that the transaction amount for business funded transfer programs from the US (such as Funds Disbursement) is equal to or less than the Visa limit of 50,000 USD. Similar customer-funded transactions (for example, money-transfer or P2P) from the US is equal to or less than

the Visa limit of 10,000 USD. Any single transaction over that amount is declined by VisaNet. Issuers can choose to establish transaction limits on their own platforms that are lower than the limits enforced by Visa.

Velocity: VisaNet also enforces maximum velocity limits for OCTs to a single Visa recipient card account. These limits are the maximum number or aggregated dollar amounts of OCTs that a single recipient account can receive in any 1-day, 7-day, or 30-day period. VisaNet declines any OCTs that exceed these amounts. Velocity limits apply at an account level, regardless of the originator. It is important to note that there could be multiple senders to a single recipient account that are not visible to the service provider or to the network. These might exceed the issuer's established velocity limits and cause a card to be declined. Cross-border transaction and velocity limits operate in the same manner as domestic limits.

The following table shows the velocity and transaction limits that Visa enforces at the recipient account level for domestic and cross-border programs.

OCT Transaction Type	Transaction Category	1 Day	7 Day	30 Day
Domestic (US)	Non-Money Transfer	150 transactions or 100,000 USD	250 transactions or 250,000 USD	750 transactions or 500,000 USD
Domestic (US)	Money Transfer	150 transactions or 20,000 USD	250 transactions or 50,000 USD	750 transactions or 100,000 USD
Cross-border	Non-Money Transfer	30 transactions or 25,000 USD	50 transactions or 50,000 USD	150 transactions or 200,000 USD
Cross-border	Money Transfer	30 transactions or 10,000 USD	50 transactions or 25,000 USD	150 transactions or 50,000 USD

Auxiliary Services

To help merchants process Payouts transactions, Cybersource offers other products and services that bolster a merchant's ability to accept Payouts and offer additional transaction security. Some of these services are required for Payouts to work properly but other services are optional. Part of the onboarding process to Payouts is selecting which services you want.

BIN Lookup Service

A BIN lookup service gathers key characteristics of a recipient card before a Payouts transaction is submitted. The BIN of the card issuer can help to uncover whether certain transaction issues are common to cards from certain issuing banks. Some of the information provided in the BIN lookup service includes:

- Issuer name
- Issuer country code
- Billing currency
- Account type (debit, credit, prepaid)
- Fast Funds participation status
- Whether the recipient issuer is OCT-enabled

For more information, see [BIN Lookup \(on page 50\)](#).

Secure Card Capture Service

Some merchants do not want to handle or store card data on their systems. By avoiding having any card data in their systems, merchants reduce their PCI compliance burden and the overall risk.

Secure Acceptance enables a merchant to securely capture payment card data from web or mobile browsers without handling payment card data. There are various implementation options for Secure Acceptance including Secure Acceptance Hosted Checkout and Flex Microform.

To use Secure Acceptance with Cybersource Payouts, the merchant must participate in the Tokenization Management Service (TMS).

For more information, see [Secure Acceptance \(on page 46\)](#).

Tokenization Service

A payment token is an alternate identifier that can be used in place of a Primary Account Number (PAN) to initiate a payment transaction.

A token replaces sensitive payment data and cannot be mathematically reversed. If you do not already have a token provider, you can use Cybersource tokens.

For more information, see [Token Management Service \(TMS\) \(on page 49\)](#).

Account Validation Service

An issuer might decline an OCT for reasons other than that the transaction exceeds transaction and velocity limits. Other reasons to decline a transaction include card expiration, invalid card number, the merchant does not permit OCTs, or the card is lost or stolen. Account validation enables an originator to screen a card for many issues.

The BIN lookup and account validation checks are automatically performed if the Secure Acceptance service is used in conjunction with the tokenization services. If the account validation service is not used, consider doing the following checks before tokenization whenever a card is being collected.

Question	Situation to Mitigate	Impact If Not Done	Solution
Is the 16-digit card number valid?	Cardholder enters the card number incorrectly.	Card declines increase.	Mod-10 check
Is the card active ?	PAN is not valid or is an active account on issuer systems.	Card declines increase.	Payment Account Validation API (zero amount authorization)
Do you want to send money to this type of card?	Cardholder enters credit card, pre-paid card, or a card that was issued outside of the US.	Successful OCT, but customer service issues remain.	BIN Lookup API
Is the card eligible for OCTs?	Card cannot receive OCTs.	Card declines increase.	BIN Lookup API
Is the card enabled for Fast Funds ?	Issuer does not make funds available within 30 minutes.	Successful OCT, but customer expectation on funds availability is not met.	BIN Lookup API

Question	Situation to Mitigate	Impact If Not Done	Solution
Is this the intended recipient?	Fraud or account takeover or the cardholder mistakenly enters an incorrect card number that is a valid number.	Successful OCT, but the transaction sent to the wrong person.	AVS check* CVV2 check

*AVS check: the enabler and merchant must validate that the recipient's address or ZIP code on file with the merchant matches the address on file with the issuer of the entered card. If the cardholder has registered a bank account for ACH payouts, the enabler can match the issuer name of the card with the bank previously used for the ACH deposit.

FX Service

The Foreign Exchange (FX) Rates API provides easy access to the Visa daily currency exchange rate.

For more information, see [FX Rates API. \(on page 54\)](#).

Transaction Search Service

The Transaction Search feature in the Cybersource portal enables merchants to easily search and view payment transactions initiated on the Cybersource platform.

Reporting Service

Many reporting options are available for acquirers and merchants.

Acquirers have access to OCT reporting through the Reports API and in the Business Center. In addition, an acquirer has access to Visa's Settlement Summary (VSS) reports on Visa Online (VOL). An acquirer can also directly receive a number of detailed and summary-level reports directly from Visa after establishing a secure connection.

A Payouts merchant should use the Transaction Reconciliation Report (TRR) for transaction reconciliation. Acquirers and merchants must refer to Visa reports for financial reconciliation. The acquirer is responsible for providing any reconciliation data to the merchant.

For more information, see [Reporting API \(on page 43\)](#).

Acquirer Setup Summary

The following is a list of the tasks required when setting up an acquirer for Payouts.

VISA Setup Tasks (on page 23)

1. Client Readiness Assessment
2. New Acquiring BIN
3. Program Information Form (PIF)
4. Card Acceptor Identifier (CAID) Form
5. VISA Push Payment Gateway Service (PPGS) Form
6. Mastercard MC 1190 Form
7. Settlement Funds Transfer Point (SFTP)
8. Global Routing ID Request
9. Global PCR Station Request
10. Client Implementation Questionnaire (CIQ)

Cybersource Setup Tasks (on page 27)

1. Setup Portfolio Cybersource MID.
2. Setup Acquirer Risk Controls (ARC) Settings.
3. Setup Merchant Cybersource MIDs.

Additional Setup for New VPC Acquirers

1. Complete Cybersource Acquirer Information Questionnaire (AIQ) and send to vpc@visa.com.
2. Follow steps in VPC Activation Guide.
3. Sign Contract.
4. Get regional approvals as required.
5. Create VPC Implementation Plan: Portfolio and Merchant MIDs.
6. Prepare for TC-33A file handling or Visa SMS/VSS report.
7. Subscribe to TC-33A POS Authorization Log (optional).
8. Deploy and configure acquirer VDC gateway.

9. Train acquirer.

Merchant Setup Summary

The following tasks must be completed when setting up a merchant.

Acquirer Readiness (on page 36)

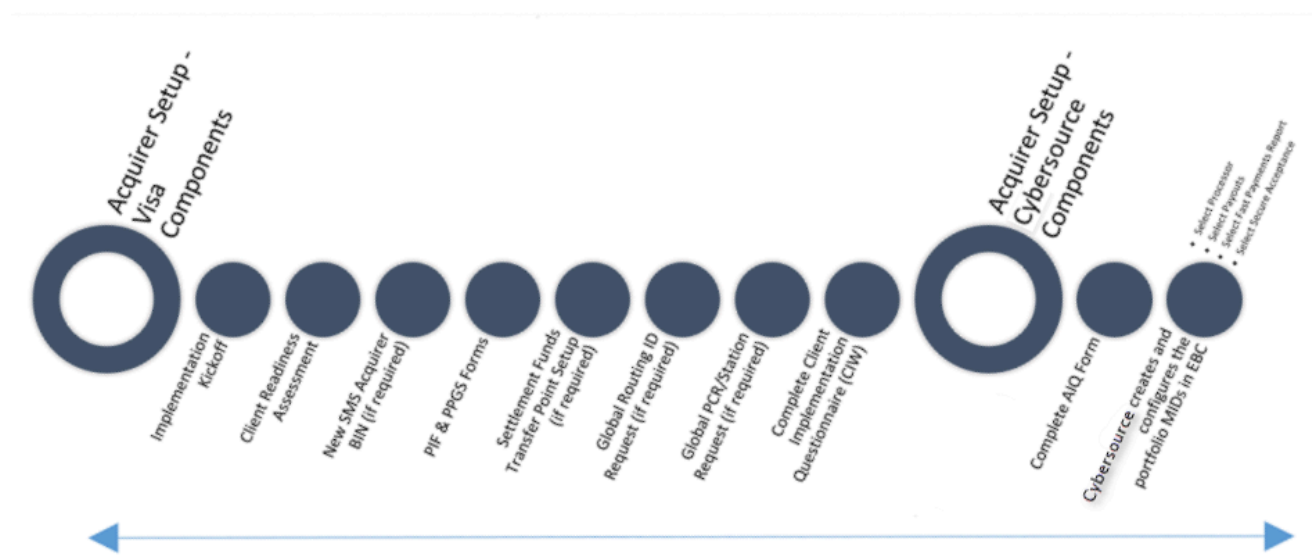
1. Complete merchant underwriting.
2. Enable Visa Direct.
3. Enable Mastercard Send.
4. Enable transaction processing capabilities.
5. Setup Acquirer Risk Controls for merchants.
6. Ensure that Customer Service and Operations are in place and people are trained on the product.
7. Enable the merchant setup for Payouts processing.

Merchant Readiness (on page 36)

1. Select and contract with a Payouts-enabled acquirer.
2. Contract with Cybersource.
3. Create and configure Cybersource MIDs.
4. Request that Payouts, BIN Lookup, and any other required peripheral services are enabled.
5. Update card processing and checkout for the Payouts service.
6. Test Payouts and other services against the test environment simulator (and optionally VCMS).
7. Test the reporting and reconciliation capabilities.
8. Ensure that the support and operational teams are set up to handle disputes and resolution processes with the acquirer.
9. Go live.

Acquirer Setup

When an acquirer engages with Cybersource for a program, the acquirer works with an account executive, sales engineer, and engagement manager who provide information about the implementation process.



A number of activities are required by the sponsoring financial institution (acquirer) to support merchants who want to process OCT transactions whether or not they are integrated with VPC or a traditional processor (like First Data Compass). The acquirer must get the required program approvals from Visa and Mastercard, perform underwriting activities, and board the merchant onto their acquirer processing systems. In addition, the acquirer or acquirer processor provides the back-office support activities such as exception item processing and merchant settlement.

Acquirer Setup for Visa Components

All programs require Visa approval before launch. The Acquirer Solutions Sales and Business Development Team is responsible for contacting the Cybersource Acquirer Solutions implementation support team to secure a resource for support.

Visa Client Services must help with setting up the acquirer BIN and Visa reporting. The sales and business development team must inform the Cybersource product manager so that the Visa Client Services team can plan for upcoming projects and secure resources. The acquirer and Cybersource work with the Visa Client Services team for the Visa Direct Requirements. All forms and detailed instructions are available at [Visa Online](#). To enroll, click on the link and scroll down the page and click **Enroll**.

Client Readiness Assessment	
Description	Visa Client Services does a readiness assessment with the acquirer to determine what is missing or required.
Required?	Yes
Duration	1 day
Form	Conference call to discuss a set of questions.
Who completes form	Visa Client Services
Prerequisite	None
New Acquiring BIN	
Description	Acquirers must use a new or existing SMS full financial acquiring BIN to initiate full financial OCT messages. The BIN license agreement is used to request a new BIN or to change the designated use status of a currently licensed BIN.
Required	Yes
Duration	10 days
Form	Available on Visa Online. Search for Numeric License Agreement and Program Plan. The Visa Program Request Management (PRM) tool available at Visa Online (VOL) can also be used for these requests.
Who completes form	Acquirer
Prerequisite	None
Program Information Form (PIF)	
Description	<p>Required for all Payouts programs that use Visa cards. All acquirers must complete this form and receive approval before launching a Visa Direct program. The PIF details the scope of the proposed origination program and related controls, including information such as BIN, domestic or cross-border program parameters, processor, and third-party agents. A PIF is required for all new Visa Direct programs and for any updates or changes to existing Visa Direct programs; for example, a change in Acquirer, BIN, Participants, or Program types.</p> <ul style="list-style-type: none"> • All PIFs must be submitted by the acquirer. • A new PIF must be submitted if the acquirer, service provider, or merchant plans to initiate new Visa Direct program types not indicated in an earlier PIF.

	<ul style="list-style-type: none"> • An acquirer, service provider, or merchant offering multiple Visa Direct program types is not required to submit a separate PIF for each type of program as long as all other information in the PIF is consistent among service offerings.
Required	Yes
Duration	10 days
Form	Access through the Visa Online, Program Request Management page.
Who completes form	Acquirer
Prerequisite	Acquiring BIN
CAID Form	
Description	A Visa form that is used to capture merchant information including the Card Acceptor ID (CAID). The CAID is an ID that uniquely identifies a merchant. This form is intended only to gather information, not to provide an approval.
Required	Yes
Duration	1 day
Form	CAID form
Who completes form	Acquirer
Prerequisite	Approved PIF
Visa Push Payment Gateway Service Form (PPGS)	
Description	<p>Visa Push Payment Gateway Service (PPGS) enables acquirers, service providers, and merchants to send their OCTs (and AFTs) to Visa for routing to Mastercard. The gateway translates and reformats the message into the correct network format, eliminating the need for an acquirer, service provider, or merchant to develop and maintain transaction formats for each debit network. Acquirers must complete:</p> <ul style="list-style-type: none"> • Visa PPGS Enrollment packet. • Packet for networks they wish to connect to. • Include transaction flow and PCI compliance documents for any entities touching cardholder data. <p>If the acquirer and indirect processor or service provider is only submitting a new merchant for a previously approved program, then they need only complete a portion of the forms (for example, Maestro's 1190) and not the entire packet. The networks do not</p>

	review or approve programs without named merchants. For Visa, a CAID Collection Form is required for each new merchant for information purposes only. No approval is necessary.
Required	Conditional
Duration	20-40 days
Form	Request form from your Visa Client Services representative.
Who completes form	Acquirer
Prerequisite	Acquiring BIN
Mastercard MC 1190 Form	
Description	Required only in the US for all Payouts programs using Mastercard (US). This form is required for each new merchant.
Required	Conditional
Duration	20-40 days
Form	Forms are not yet available on VOL. Contact your Visa Client Services representative for more information.
Who completes form	Acquirer
Prerequisite	Acquiring BIN
Settlement Funds Transfer Point (SFTP)	
Description	Required only when a new SFTP is required for the Visa Direct program.
Required	Conditional
Duration	
Form	Request forms from your Visa Account Manager.
Who completes form	Acquirer
Prerequisite	Acquiring BIN
Global Routing ID Request	
Description	Required only for a new Visa Resolve Online (VROL) Configuration. VROL is the Visa tool to manage exceptions and chargebacks.
Required	Conditional
Duration	14 days
Form	Request forms from your Visa Account Manager.

Who completes form	Acquirer
Prerequisite	Acquiring BIN
Global PCR/Station Request	
Description	Required only for a new Visa Resolve Online (VROL) configuration.
Required	Conditional
Duration	14 days
Form	Request forms from your Visa Account Manager.
Who completes form	Acquirer
Prerequisite	Acquiring BIN
Client Implementation Questionnaire (CIQ)	
Description	A CIQ is required in order to move the new BIN into testing and production. It is used to install new card programs, transfer programs between processors, or request changes to a card program. It is also used to authorize the new SMS BIN for VisaNet in both Test and Production environments.
Required	Required
Duration	30 days
Form	Find on VOL by searching for <i>Client Information Questionnaires (CIQs)-U.S. CIQ Forms</i> .
Who completes form	Acquirer
Prerequisite	Acquiring BIN

Acquirer Setup for Cybersource Components

In addition to the Visa Direct requirements, an acquirer must complete additional tasks with Cybersource. These tasks can be started when the Visa Direct requirements are completed. The tasks that must be completed differ according to the use case that applies to the merchant's circumstances and needs.

Traditional processor New Acquirer (standard or configured) connects to First Data Compass with a signed reseller agreement.

Task	Responsible Party	Description
Portfolio MID	Partner Engagement Manager	<p>Cybersource creates and configures the Portfolio MID in the Business Center:</p> <ul style="list-style-type: none"> • Select Processor (firstdatacompass) • Select Payouts • Select Fast Payments Reports • Select Secure Acceptance
Setup Merchant MIDs	Acquirer / Processor	The acquirer has flexibility in setting up MIDs based on discussion with the acquirer.
Risk Controls	Acquirer / Processor	Ensure that the acquirer and First Data Compass are in agreement with risk controls and processing and reporting for OCT transactions. Acquirers that connect to First Data Compass must leverage the risk controls set by First Data.

New VPC Acquirer (standard or configured model) connects using VPC and has a signed reseller agreement.

Task	Responsible Party	Description
BIN Setup/Visa Reporting	Visa Client Services	<p>Cybersource creates and configures the Portfolio MID in the Business Center:</p> <ul style="list-style-type: none"> • Select Processor (firstdatacompass) • Select Payouts • Select Fast Payments Reports • Select Secure Acceptance
VPC Connection	Account Executive/Sales Engineering	<ul style="list-style-type: none"> • Refer to the VPC Service Activation Guide for detailed information on how to set up a new VPC connection or contact the North America VPC product team: David Wuichet, Matt Roser, Jorge Foy, Robert McLaughlin (INTERNAL ONLY). • Complete the Cybersource VPC AIQ form and email the form to vpc@visa.com. For additional questions about the AIQ form, contact the VPC product team and refer to the wiki.

Task	Responsible Party	Description
		<ul style="list-style-type: none"> Section G.2 Cybersource Payouts enter the Visa Direct Full Financial BIN. <p>The VPC product team schedules enablement of the gateway upon receipt of the completed AIQ form and signed contract (approximately one release cycle).</p>
Portfolio MID	Partner Engagement Manager	<p>Cybersource creates and configures the Portfolio MID in the Business Center:</p> <ul style="list-style-type: none"> Select Processor (vdcmetropolitan, vdcpayouts, etc.) Select Payouts Select Fast Payments Reports Select Secure Acceptance
Setup Merchant MIDs	Acquirer	The acquirer sets up the MID. Depending on the complexity of the merchant setup and capability of the acquirer, they might need help from the Partner Engagement Manager.
Risk Controls	Acquirer	The VPC acquirer must use the Cybersource Risk Controls in the Business Center; therefore, the merchant MIDs must be boarded under the Portfolio MID.
Billing	Partner Engagement	Set up billing for the acquirer based on the agreed upon contract.
Reporting	Partner Engagement Manager	New VPC acquirers connecting to the vdcpayouts do not receive a TC33A capture file and instead must leverage the OCT reports in the Business Center or decide to connect directly to Visa to receive the raw data files.
Training	Partner Engagement Manager or Cybersource Alliance SE	Ensures that the acquirer understands processing and reporting responsibilities and receives Business Center training.

Existing Acquirer with a signed reseller agreement connects using VPC.

Task	Responsible Party	Description
BIN Setup and Visa Reporting Acquirer might not have an SMS BIN	Visa Client Services	<p>Cybersource creates and configures the Portfolio MID in the Business Center:</p> <ul style="list-style-type: none"> • Select Processor (vdcmetropolitan, vdcpayouts, etc.) • Select Payouts • Select Fast Payments Reports • Select Secure Acceptance
Enabling Payouts on existing VPC Connection	Account Executive or Sales Engineering	<p>Using their own VPC gateway setup, an existing VPC acquirer wants to add Payouts capabilities.</p> <ul style="list-style-type: none"> • Complete the Cybersource VPC AIQ form and email the form to vpc@visa.com. For additional questions about the AIQ form, contact the VPC product team and refer to the wiki. This is an update, not a new request. • Section G.2 Cybersource Payouts enter the Visa Direct Full Financial BIN. • VPC Product team schedules enablement of the gateway upon receipt of the completed CIQ form and signed contract (approximately one release cycle).
Setting Up Merchant MIDs	Acquirer	Acquirer sets up the MID. Depending on the complexity of the merchant setup and capability of the acquirer, they might need help from the Partner Engagement Manager.

Existing VPC Acquirer acting as a sponsor and not a reseller connects using VPC.

Task	Responsible Party	Description
BIN Setup and Visa Reporting Acquirer might not have an SMS BIN	Visa Client Services	<p>Cybersource creates and configures the Portfolio MID in the Business Center:</p> <ul style="list-style-type: none"> • Select Processor (vdcmetropolitan, vdcpayouts, etc.) • Select Payouts • Select Fast Payments Reports • Select Secure Acceptance

Task	Responsible Party	Description
Enabling Payouts on an existing VPC connection	Account Executive or Sales Engineering	<p>Using its own VPC gateway setup, an acquirer wants to add Payouts capabilities.</p> <ul style="list-style-type: none"> • Complete the Cybersource VPC AIQ form and email the form to vpc@visa.com. For additional questions about the AIQ form, contact the VPC product team and refer to the wiki. This is an update, not a new request. • Section G.2 Cybersource Payouts: enter the Visa Direct Full Financial BIN. <p>VPC Product team schedules enablement of the gateway upon receipt of the completed AIQ form and signed contract (approximately one release cycle).</p>
Setting up Merchant MIDs	Cybersource (PEM)	<p>Cybersource Partner Engagement Manager sets up the MID. The following information is required from the acquirer for setup:</p> <ul style="list-style-type: none"> • BIN • ABA#

Setting Up a Reseller

An acquirer can sell the Payouts solution to an individual merchant or a reseller that manages and sells to other merchants. There are differences between the setup of an individual merchant and reseller.

There are three ways to set up a reseller:

	Reseller portfolio with a MID for each sub-merchant	Reseller portfolio with a single MID per use case	Acquirer portfolio with a single MID
ARC	The reseller must provide the acquirer access to ARC. The acquirer must ensure that reseller access is limited (contractually). The acquirer assigns a limit for each sub-merchant.	Reseller must provide the acquirer access to ARC. The acquirer must ensure that reseller access is limited (contractually). The acquirer assigns a limit for the reseller.	The acquirer assigns a limit for the reseller.

	Reseller portfolio with a MID for each sub-merchant	Reseller portfolio with a single MID per use case	Acquirer portfolio with a single MID
Implementation	The reseller must set up each merchant.	The reseller sets up a single MID for itself.	The acquirer sets up a single MID (for each use case) for the reseller.

Option 1: Setting Up a Reseller

This is a summary of how to set up a reseller.

Business Center MID Setup

The reseller is assigned a separate portfolio MID from the acquirer.

Cybersource creates and configures the new Portfolio MID in the Business Center doing the following tasks:

- Selecting a Processor.
- Selecting Payouts.
- Selecting Fast Payments Reports.
- Selecting Secure Acceptance.

The reseller is responsible for setting up the MID for each of its individual merchants. Each reseller client is assigned a sub (child) Merchant ID which can be any unique identifier determined by the reseller.

The MID field must be configured (within the Business Center) using the acquirer approved CAID for each merchant account.

The Portfolio admin account must not be used for operations or technical purposes. The Portfolio admin account is the account with *_acct* after the portfolio ID. The portfolio ID account (parent merchant ID) can be used to login and set up the merchant.

Acquirer Risk Control Setup

The reseller creates credentials (within the Business Center) so that the acquiring bank can grant user permissions to access the Acquirer Risk Controls.

The reseller administrator must abide by the following:

- To **not** access the Acquirer Risk Controls.
- To not create any user credentials (besides the acquiring bank) with the Acquirer Risk Controls access.

The reseller agrees that the acquiring bank is the only entity permitted to access and configure the Acquirer Risk Controls in the Business Center.

The acquirer might need to add a clause to the legal agreement (check with legal) to ensure restricted access.

Billing

In the reseller setup, the billing is sent to the entity that owns the portfolio, for example, the reseller. Billing statements can be viewed and payments made from the Business Center by going to the left navigation pane and selecting **Account Management > Pay My Invoice**.

Metakey

A single API metakey is used for all MIDs. It is not specific to Payouts but it is an architectural choice for setting up a seller solution.

Option 2: Reseller Portfolio with a Single MID per Use Case

Business Center MID Setup

The reseller is assigned a separate portfolio MID from the acquirer. Cybersource creates and configures the new Portfolio MID in the Business Center doing the following tasks:

- Selecting the Processor
- Selecting Payouts
- Selecting Fast Payments Reports
- Selecting Secure Acceptance

The reseller must set up a single MID for itself (per use case) using the acquirer-approved CAID.

Acquirer Risk Control Setup

The reseller creates credentials (within the Business Center) so that the acquiring bank can grant user permissions to access the Acquirer Risk Controls. The reseller administrator must abide by the following stipulations:

- To **not** access Acquirer Risk Controls.
- To not create any user credentials (besides the Acquiring bank) with Acquirer Risk Controls access.

The reseller agrees that the acquiring bank is the only entity that is permitted to access and configure the Acquirer Risk Controls in the Business Center. The acquirer might need to add a clause to the legal agreement to ensure restricted access (check with legal department).

Billing

In the reseller setup, the billing is sent to the entity that owns the portfolio; for example, the reseller. Billing statements can be viewed and payments made from the Business Center by going to the left navigation pane and selecting **Account Management > Pay My Invoice**.

Metakey

A single API metakey is used for all MIDs. This is not specific to Payouts but an architectural choice for setting up a reseller solution.

Option 3: Acquirer Portfolio with Single MID

Business Center MID Setup

A single MID is used for the reseller under the acquirer's portfolio. This setup works only for a reseller that can manage the sub-merchants on their own system. Individual MIDs are not set up for each sub-merchant. Cybersource loses visibility (search, reporting, support) into each sub-merchant.

Billing

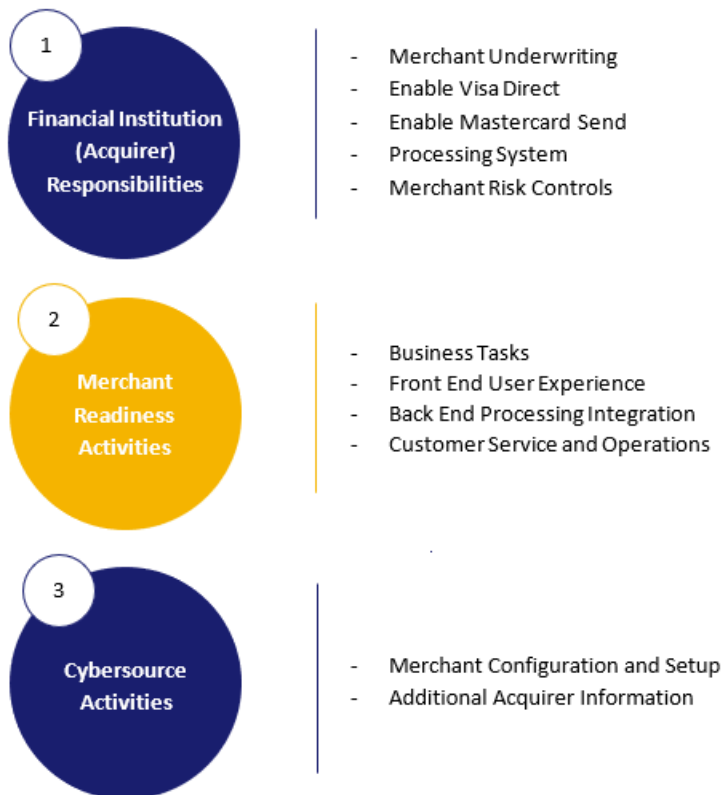
In the reseller setup, the billing is sent to the entity that owns the portfolio. In this case, it is the acquirer.

Merchant Setup

When a merchant plans to implement Cybersource Payouts, a number of activities are required by the sponsoring financial institution (acquirer), the merchant, and Cybersource. The financial institution must get the required program approvals from Visa and Mastercard, perform underwriting activities, and onboard the merchant into their acquirer processing systems.

The merchant might need to enhance user interfaces to add capabilities for a customer to select push-to-card payment options as well as the capturing of card data and ensuring PCI compliance. The merchant has to incorporate various Cybersource services including an API call to initiate a Payouts transaction.

Cybersource configures the merchant on the Cybersource platform and enables the merchant to participate in Cybersource Payouts and any additional service being implemented, such as Secure Acceptance and the Token Management Service (TMS). This section provides a checklist of activities required when a merchant implements a Cybersource Payouts program.



Acquirer (Financial Institution) Responsibilities

The following tasks are required by acquirers when a new merchant is set up for Cybersource Payouts.

- **Perform Merchant Underwriting:** Similar to standard card programs, financial institutions must do the due diligence and credit validation required for their push-to-card customers. Merchants might be required to establish an account at the sponsoring financial institution. Financial institutions can also request that minimum account balances be maintained for a merchant participating in Payouts.
- **Submit a Visa Direct Program Information Form (PIF):** Because Cybersource Payouts uses Visa Direct for sending payments to Visa cards, the acquirer must submit a Visa Program Information Form (PIF) for each new merchant program. Visa must approve the merchant use case.
- **Submit a Mastercard Send MC 1190 Form:** Because Cybersource Payouts uses Mastercard Send for sending payments to Mastercard cards, the acquirer must submit an MC 1190 form for each new merchant program. Mastercard must approve the merchant use case.
- **Create a Merchant Account on the Acquirer Processing System:** Acquirers often use third-party processors like First Data or TSYS to perform card-processing activities. The acquirer might have these systems in-house or participate in Visa Platform Connect (VPC). The acquirer processing systems must be configured with the appropriate acquiring BIN for processing push-to-card programs. These systems must have merchant identifiers (MIDs) and might have Terminal ID (TID) requirements, depending on the processor. Before someone sets up a merchant account at Cybersource, these MID and TID values must be provided to Cybersource during the implementation process.
- **Establish Merchant Risk Controls:** Cybersource Payouts enables acquirers to set limits on the number of Payouts transactions and the maximum amount of a single transaction and aggregate transactions during defined daily, weekly, and monthly periods. These limits can be configured in Cybersource systems for individual merchants and can be changed as needed.

Merchant Readiness Activities

The following checklist is a generalized list of tasks to be considered when a merchant is onboarded into the Cybersource Payouts program. Depending on the use case and program being implemented, some of the tasks listed might not be needed and others that are not listed might be needed.

Business Tasks

- **Select and Contract with a Financial Institution:** To participate in Cybersource Payouts, a merchant must contract with a financial institution to provide acquiring services. A limited set of acquirers currently supports push-to-card. See [Supported Acquirers and Processors](#) for the current acquirers that support Cybersource Payouts.

- **Contract with Cybersource:** Existing Cybersource customers need an amendment to the pricing schedule of their existing contract. A new merchant requires a contract with Cybersource.

Front-End User Experience

- **Add Push-to-Card As a Payment Option:** Merchants must modify systems in which the payment method is selected to include push-to-card as an option. These applications could be customer facing web or mobile applications or internal-facing applications. When the option is selected, card data can be entered.
- **Enable User Interface to Capture Card Data:** Similar to a checkout experience on an e-commerce page, the merchant's user interface must capture the card data for push-to-card. The merchant can use Cybersource Secure Acceptance and Token Management Service (TMS) to provide this capability.
- **Integrate APIs for Validating Card :** If a merchant is not using Secure Acceptance, the merchant should use the Cybersource BIN Lookup. This API returns key attributes about the card that can enhance the user experience and that ensure the card is an appropriate destination for a push-to-payment. If the merchant is using Secure Acceptance, this data can be returned in the post response as described in the Secure Acceptance section.
- **Card Rejection Error Messaging:** If the card entered is not eligible for a push-to-card transaction, the user experience must prompt the user to enter a new card or select an alternative payment method.
- **SMS/Email Notifications:** SMS or email notifications are relevant for multiple areas within the user experience. For example, depending on the use case, the merchant can send a link to the application that enables the cardholder to enter card data. Also after the payment is initiated, a message can be sent to the customer indicating success or failure of the payment request.
- **View Payment History:** The merchant can provide the ability for customers to view the status or history of payments within their web or mobile application. Any new payment method might require changes to enable the customer to view the new method.

Back-End Processing Integration

- **Store Payment Instrument:** The card data or token must be associated to the customer in the merchant's systems.
- **Integrate to Cybersource Payouts API:** The merchant must decide which API approach to use. See [APIs for Payouts](#) for different API options.
- **Create Merchant Account and Credentials:** A merchant account and associated credentials must be created. [Authentication and Key Generation](#) depends on the API approach selected for integration in the previous step.
- **Accounting Integration :** Push-to-card payments are similar to other outbound payments that must be accounted for in a merchant's general ledger. It also requires sub-ledger entries. Note that a successful push-to-card transaction means that the funds are sent to the recipient. No subsequent step for clearing the funds is needed.

- **Treasury:** Push-to-card payments pay in real-time. Some financial institutions require a minimum balance on deposit. Business processes and integration into the selected financial institution are required.

Customer Service and Operations

- **Update Customer Service Materials:** Customer service scripts and messaging must be changed to include push-to-card transactions. Training is required for customer service agents.
- **Training Program:** Training materials and a FAQ must be created for back-office and support teams.
- **Back-Office Processes:** New back-office processes are required in order to support push-to-card payments. These include processes for transaction search and financial reconciliation.
- **User Accounts and Access to Cybersource:** It might be appropriate for support, operations, and back-office teams to access Cybersource for transaction search and reporting.
- **Processes for Dispute Management:** If a payment is not received by a customer, or the wrong party is paid, resolution processes are needed between the merchant and the financial institution.

Cybersource Activities

When a merchant is onboarded to Cybersource Payouts, merchant configuration and setup is required in order to enable the merchant to successfully process Payouts transactions. The activities vary depending on whether the merchant is onboarded by a reseller or by Cybersource as a direct sale.

Visa Platform Connect

A VPC setup in which Cybersource manages the processing requires additional information from the acquirer, including the full financial acquiring BIN to be used for Payouts. When an acquirer processor that supports Payouts is selected for the merchant in the Business Center, the configuration fields relevant for Payouts become available.

Direct Sale Merchants

For direct sale merchants, Client Support Services configures the client using the MAMs Configuration Portal. The minimum information required depends on whether the processor is a traditional processor or VPC.

Resellers

Resellers can onboard merchants using the Business Center. When an acquirer or processor that supports Payouts is selected for the merchant, the Payouts configuration items become available.

Merchant Onboarding

There are two fundamental steps the acquirer or reseller must do in the Business Center as part of the onboarding process before a merchant can begin transacting:

- Configuring the merchant profile
- Configuring a processor

These fields must be completed in the Basic Merchant Information section of the merchant profile when adding a new merchant:

Field	Description	Required/Optional
Cybersource Merchant ID	Merchant identifier	Required
Merchant Name	Merchant name Alphanumeric characters and the following special characters allowed (space _ + - * " / ' & , () ! \$; : ? @ #)	Required
Country	Merchant country	Optional
Address (line 1)	First line of merchant street address	Required
Address (line 2)	Second line of merchant street address	Optional
City	Merchant city	Required
State/Province	Merchant state or province	Required (for addresses in USA, Canada, and Australia)
ZIP/Postal Code	Merchant ZIP or postal code	Required (for addresses in USA, Canada, and Australia)
Phone	Merchant phone number	Required
Website URL	Merchant web site URL	Required
Time Zone	Merchant time zone	Required

Configuring Merchant Information

Merchants are onboarded from the Business Center. All acquirers are provided with an account in the Business Center where merchant accounts are managed and transaction payments can be reviewed.

You can either add and modify individual merchants manually or add new merchant accounts or modify existing merchants by batch uploading data in a CSV file on the Merchant File Upload page in the Business Center.

1. Open the side navigation bar in Business Center and select **Portfolio Management > Manage Merchants**. The Manage Merchants window appears.
2. Click **ADD MERCHANT** at the upper right part of the window. The Merchant Boarding window appears.
3. To group this new merchant under an existing merchant account, select that account from the drop-down list in the **Account Selection** field of the Hierarchy section. If you want this merchant to have its own account, leave the default option at **None**.
4. In the **Merchant ID** field, enter the identification code created when the merchant account was registered with Cybersource.
5. In the **Merchant Name** field, enter the name of the merchant.
6. The **CSKK Information** fields are optional.
7. To skip the emails that welcome a new merchant to the Business Center, select **Skip Boarding Emails**.
8. To subscribe to reporting reconciliation services, choose the **Reconciliation Subscription** option.
9. Choose **NEXT** and enter the address and contact information for the business including the URL for the business website and the time zone that the merchant resides in. Any field marked with an asterisk must be completed.
10. In the Business Contact section, enter contact information for the person designated to be notified of the registration completion and any merchant status changes. This person receives instructions for logging into the Business Center.
11. In the subsequent Technical Contact section, enter the contact information for the person to be contacted about technical issues. In the Emergency Contact sections, enter the contact information for the person to be contacted about any urgent issues. The person designated in each section can be the same person designated as the Business contact or it can be different individuals. Select the **Use Business Contact Info** option as needed to use the same person for all contacts.

Additional Merchant Contact Information

Complete the business contact information for the merchant.

The technical and emergency contact information can be the same as the business contact information. Check the Use Business Contact as Technical Contact option to use the same contact information in another section.

Table 1. Merchant Contact Information

Field	Description	Required/Optional
First Name	Business contact first name	Required

Table 1. Merchant Contact Information (continued)

Field	Description	Required/Optional
Last Name	Business contact last name	Required
Email	Business contact email This address is used to notify merchant of registration completion, merchant status changes, and login instructions to the Business Center.	Required
Phone Number	Business contact phone number Plus sign (+) and 13 digits are allowed for international numbers.	Required

Configuring Processor Settings

After adding the merchant and configuring its contact information, you must select a company to process the merchant's transaction payments and configure how the processing is managed. Any field marked with an asterisk must be completed.

Processors that support Payouts transactions are listed below.

Acquirer	Country	Comment
Fiserv (First Data Compass)	USA	Live with PNC Bank
Metropolitan Commercial Bank (MCB)	USA	Live
Yes Bank	India	Live
Generic (gateway name: vdcpayments)	Global	Live#This can be the default gateway for all new VPC connections.

Adding Processor

After you add the merchant information, select a company to process the merchant's transactions. Any field marked with an asterisk must be completed.

1. In the **Processor** field, select a processor from the drop-down menu. You can add multiple processors to handle different types of payments, but one processor must be designated as the primary one. The **Use this processor as primary** option is selected by default until more than one processor is added to the merchant account.
2. In the **Processor Settings** field, choose which payment types are managed by the selected processor.

3. In the **Currencies** field, click **Expand All**. Scroll down the list and choose the **USD (US Dollar)** option and enter the terminal ID in the field beside it. The terminal ID identifies the source of the transaction. (Currently, Payouts supports only US dollars.) After your selection, save screen space by clicking on **Collapse All**.
4. In the **Merchant Industry** field, enter the Merchant Category Code.
5. In the **Extended Transaction Settings** section, complete any options that are relevant for the merchant.
6. To add another processor, choose **Add Another** and repeat this procedure. When you finish adding processors for the merchant, choose **Acquirer Configuration**.

Supporting Products and Features

Cybersource Payouts is an e-commerce transaction that is supported by a suite of different Cybersource products offering a comprehensive solution for the customer. Many of these products have their own detailed documentation available.

Business Center Overview

Businesses that participate in Cybersource Payouts and other Cybersource services have access to the transaction search and reporting capabilities within the Business Center.

The Business Center features enhanced reporting, analytics, and transaction search capabilities. For businesses that use Cybersource Payouts, the Business Center is used as the exclusive merchant platform for their transaction search and reporting practices.

Merchants sign in with the following credentials:

- Organization ID
- Username
- Password

If this is your first time signing in, your organization ID and username are likely the same. They can be changed later after the initial login. After successfully signing in, you are directed to the dashboard where you can manage merchants and transactions in addition to leveraging powerful API applications within the Business Center like Transaction Search.

Reporting API

Acquirers have access to OCT reporting through the reports API. The reports API offers transaction reconciliation data in the API response. This data is provided to enable the reconciliation of the transactions sent by your systems with the transactions that were processed through Visa. This data can be used solely for such purposes. The reports are available in the [Business Center](#).

You can choose to download one-time reports or configure your preferences to receive subscription reports to be sent daily, weekly, monthly, etc., at specified times.

Your report can include any of the following report fields and their respective child attributes.

Application	BankInfo	BillTo	Check
Device	FundTransfer	GiftCard	LineItems
MerchantDefinedData	PaymentData	PaymentMethod	Profile
Recipient	Request	Risk	Sender
ShipTo	Shipping	Token	Travel

Two types of reports are compiled using information from different sources and intended for different audiences. The reports that Cybersource provides are intended for use by the merchant. Reports from Visa, called Visa Settlement Summary reports, are intended for acquirers to monitor merchant activity within their portfolio.

Acquirer OCT Reports

Acquirers have access to OCT [reporting through the Business Center](#). The Reports API provides reporting capabilities such as transaction reconciliation data in the API response. The data needed for reconciliation OCT transaction details and any exceptions such as chargebacks and reversals are available in a report format.

For an acquirer to access the OCT acquirer reports within the Business Center and through APIs, the acquirer must subscribe to these reports. The acquirer needs to complete the Acquirer Client Implementation Questionnaire (CIQ) in the SMS Reports and Raw Data section. The acquirer also needs to add the subscription to Cybersource 736081-0002 for Raw Data Reports.

General Help

Acquirer CIQ

VISA

Front Cover

Print Preview

Validate Data

Previous Service

Next Service

SMS Reports and Raw Data

SMS reports and raw data are transaction detail reporting data that can be used to reconcile a client's daily processing activity. Reports are 'print-friendly' formatted files that are available in different sort orders. Raw Data provides transaction level detail in machine-readable format. For further information, refer to the VSS User's Guide, Volumes 1 and 2.

AEL1-Va

D03 - Specify the Visa or Plus Delivery Endpoint (BIN/Network)

736081

0002

AEL1-Vb

D04 - Specify the BII CIB Delivery Endpoint

AEL1-Ia

D05 - Specify the Interlink SMS BIN Delivery Endpoint (BIN/Network)

AEL1-Ib

D06 - Specify the BII CIB Interlink Delivery Endpoint

GA6

D07 - Specify the financial institution name as it should appear on the SMS Reports

METROPOLITAN COMMERCIAL BANK

SMS Reports

ID	Report Name	Reports Sorted by:			
		Retrieval Reference Number	Issuer BIN	Card Number	Time
SMS601	D08 - ACQUIRER TRANSACTION DETAIL				
SMS608	D09 - FEE COLLECTION & FUNDS DISBURSEMENT	-----	-----		-----
SMS611	D10 - ACQUIRER CHARGEBACK DETAIL				-----
SMS613	D11 - ACQUIRER REPRESENTMENT DETAIL				-----
SMS615	D12 - ACQUIRER ADJUSTMENT & MERCHANDISE CREDITS				-----
SMS617	D13 - ACQUIRER CANCELLATION & REVERSAL DETAIL		-----		-----
SMS626	D14 - ADMINISTRATIVE MESSAGE DAILY SUMMARY		-----	-----	-----
SMS641	D15 - ACQUIRER ERROR DETAIL	-----	-----	-----	
SMS643	D16 - ACQUIRER RETURNED EXCEPTION DETAIL		-----	-----	-----

SMS Raw Data
NOTE: SMS Raw Data release 2.2 and 2.3 are mutually exclusive. Version 2.3 Raw Data is a subset of Version 2.2 and is not intended to be a complete record of a transaction

VIP (SMS) Raw Data Release 2.2

ID	Report Name	Action
V22120	D17 - VSS SPECIFIC RECORD	Add
V22200	D18 - FINANCIAL TRANSACTION RECORD 1*	Add
V22255	D19 - FINANCIAL TRANSACTION FEE COLLECTION / FUNDS DISBURSEMENT	Add
V22260	D20 - FINANCIAL TRANSACTION RECORD / MULTICURRENCY RECORD	Add
V22261	D21 - FINANCIAL TRANSACTION RECORD / FEE RECORD	Add
V22276	D22 - FINANCIAL TRANSACTION MONEY TRANSFER & PERSONAL PAYMENT	Add
V22300	D23 - FINANCIAL MAINTENANCE TRANSACTION RECORD	Add

To ensure that an acquirer can view the OCT reports, during initial set up, the portfolio MID must be enabled in MAMS for OCT reports:

The OCT reports use the Visa Direct SMS Raw Data files from Visa to create user-friendly reporting formats for acquirers to monitor OCT transactions and perform merchant settlement activities. Cybersource OCT acquirer reports include:

Report Name	Description
Acquirer Detail Report	Lists the details of all OCT transactions.
Acquirer Exception Detail Report	Lists exception transactions for a single processing day.
Acquirer Chargeback Detail Report	Lists chargebacks and chargeback reversal transactions received by the acquirer during the processing day.
Reconciliation Summary Report	Summarizes the total OCT transactions and total amount processed.

VOL Reports

Acquirers have access to Visa Settlement Summary (VSS) reports on Visa Online (VOL). These reports are available daily at 12:00 p.m. EST/9:00 a.m. PST.

To obtain access to the VSS reports on Visa Online, the acquirer goes to the VOL homepage and chooses **Help > Feedback/Contact Us**. In a message sent to VOL, the acquirer specifies the VOL ID and requests access to the VisaNet Settlement Service application. The VSS reports that are available are:

Report Name	Description
VSS-110 Reconciliation Report	Shows the daily net settlement position and matches the wire amount to the settlement account at the financial institution.
VSS-115 SRE Settlement Recap Report	Shows the summarized totals of the interchange value, reimbursement fees, and Visa charges for the <i>reporting</i> SRE.
VSS-120 Interchange Value Report	Provides the interchange values in the settlement currency. The interchange value totals for each business mode balance to the interchange values on the VSS-110 Settlement Summary Report and the VSS-115 SRE Settlement Recap Report.
VSS-130 Reimbursement Fees Report	Totals the balance to the reimbursement fees on the VSS-110 (Settlement Summary Report) and the VSS-115 (SRE Settlement Recap Report).

Report Name	Description
VSS-300	Provides the summarized totals of the interchange value, reimbursement fees and Visa charges for each SRE that is directly subordinate to the <i>reporting</i> SRE.
VSS-900-S	Enables clients to reconcile items cleared to items settled. Totals for each business mode and clearing currency reconcile to the totals shown on the SMS detail reports. This report uses the same disposition categories as the VSS-900 report.

Secure Acceptance

Cybersource Secure Acceptance securely captures payment card data from a web or mobile browser, enabling the merchant to avoid handling payment card data. There are different implementation options for Secure Acceptance including Secure Acceptance Hosted Checkout and [Flex Microform \(on page 46\)](#).

When using Secure Acceptance for Cybersource Payouts, the merchant must use the Cybersource Token Management Service. The only supported Secure Acceptance transaction type is *Create Token*.

There are different implementation options for Secure Acceptance, including Secure Acceptance Hosted Checkout which enables cardholders to securely enter payment instrument data. Secure Acceptance Hosted Checkout enables the merchant to embed an iframe into their web or mobile application or to redirect cardholders to a Cybersource mobile optimized web page.

Secure Acceptance Hosted Checkout is configurable to ensure customers entering card data on their website or mobile application is seamless with consistent branding throughout the process. The payment data is transmitted from customers directly to Cybersource, bypassing the merchant, so the PCI-DSS responsibilities of a merchant are significantly reduced.

The page displayed is hosted by Cybersource and is where the payment card data is securely captured. Secure Acceptance Hosted Checkout initiates a POST request back to the merchant's site where a Payment Card token is provided. Various data elements about the card, including the last four numbers of the card, card type (debit, credit, or prepaid), and eligibility for OCT and Fast Funds participation of the issuer are also sent.

Secure Acceptance Flex Microform

Flex Microform makes it easier for you to become PCI DSS compliant without requiring any compromise in user experience. The capture of card numbers is fully outsourced to Cybersource, which can qualify you for SAQ A-based assessments. Using Flex API, Flex Microform provides the most secure method for tokenizing card data. Sensitive data is encrypted on the customer's device before HTTPS transmission to Cybersource. This method mitigates any compromise of the HTTPS connection through a man-in-the-middle attack.

Secure Acceptance Hosted Checkout Response API Fields

The POST request from Secure Acceptance Hosted Checkout returns many data elements. The elements returned depend on the configuration selected by the merchant, such as if the merchant participates in the Preauth Address Verification Service. The data that is returned also depends on the card brand, card type, and the issuer of the card. Many of the elements in the Secure Acceptance documentation are relevant only for purchase transactions initiated through Secure Acceptance and are not relevant for Payouts. The following list contains the attributes that are important to initiating and managing most Payouts transactions:

Field	Description	Usage Notes
reason_code	Contains a numeric value that corresponds to the decision response of the transaction. See Secure Acceptance documentation for values and meaning.	100 is a success reason code. Any other reason code implies an error occurred and that the card was not successfully captured.
payment_token	Identifier for the payment details.	This field must be stored by the merchant and is used as the subscription ID.
req_consumer_id	Identifier for the customer account. This value is defined when creating a customer subscription.	This is the merchant's identification of the cardholder. If consumer_id is sent in the request, it is returned in the response. The consumer_id value is considered by Cybersource as a reference value only. It is stored in the Cybersource token vault but is not validated by Cybersource.
bin_lookup_card_sub_type	Type of card, such as: Debit Credit Prepaid Credit/debit	Merchants may want to only support push-to-card for debit or debit and prepaid. This information enables the merchant to inform the cardholder that the card being used is not supported and that they should enter a Visa or Mastercard debit or prepaid card.
bin_lookup_card_product_category	Category of product, such as business, commercial, or customer.	Enables a merchant to restrict push payments to specific categories if desired.
bin_lookup_card_type	Three-digit value that indicates the card type (001 = Visa, 002 = MC).	Payouts is valid only for Visa and Mastercard. If the card type is anything other than 001 or 002, the merchant must ask the customer to enter a valid Visa or Mastercard.
bin_lookup_card_type_name	Name of the card type (Visa, Mastercard).	

bin_lookup_billing_currency	Cardholder's billing currency.	Informational. Not important if the merchant does not support cross-border payments.
bin_lookup_billing_currency_minor_digits	Number of decimal positions for the amount in the cardholder's billing currency.	Related to billing currency.
bin_lookup_cross_border_eligible	Indicates whether cross-border transactions are supported for this card. Cross-border means that the issuer and acquirer are in different countries. Possible values: <ul style="list-style-type: none"> • Y: Supported • N: Not supported 	Important only when the merchant supports cross-border transactions. Can be used to validate whether a cross-border transaction is supported for the card.
bin_lookup_issuer_country	Two-character alpha ISO country of the issuing bank.	Can identify a potential cross-border transaction. If a merchant does not support cross-border, the merchant can request that the cardholder enter a different card.
bin_lookup_issuer_country_numeric_code	Three-digit numeric ISO code for the issuer's country.	Same as bin_lookup_issuer_country .
bin_lookup_issuer_name	Bank that issued the card, such as Bank of America, Chase, PNC, or Wells Fargo.	Informational. Can be displayed to customer as part of the user experience.
bin_lookup_oct_indicator	Indicates whether the account can receive original credit transactions (OCTs). Possible values: <ul style="list-style-type: none"> • A • B • C • N: Push-to-card transactions are blocked. 	Returned only for Visa cards. Indicates whether the issuer supports push-to-card transactions. If the value is N, the merchant must ask a customer for a different card. All other values are good.
bin_lookup_oct_fast_funds_indicator	Speed at which funds are made available to the customer: Possible values: <ul style="list-style-type: none"> • B: Within 30 minutes 	Returned only for Visa cards. Indicates whether the issuer makes funds available to customers immediately. If the value is N, the merchant can inform

	<ul style="list-style-type: none"> • C: Within 30 minutes • D: Within 30 minutes • N: Within two business days 	the customer that funds will be available within two business days or to use another card.
--	---	--

Tokenization

When using Secure Acceptance for Payouts, you must also use the Tokenization Management Service (TMS). Tokenization replaces sensitive payment data with a unique identifier or token that cannot be mathematically reversed.

In documentation and APIs, tokens are referred to as either Recurring Subscription Info or Subscription ID. When submitting Payout requests using a Subscription ID (or the token), the merchant sends the Recurring Subscription Info data block containing the Subscription ID. The merchant **does not** send the payment card data block or any of the card payment data. Card data is retrieved from the vault using the provided subscription ID.

The actual payment data is securely stored in Cybersource data centers that are operated by Visa. For Payouts merchants, creating and receiving tokens are managed through Secure Acceptance. The following links provide details about managing tokens.

API Integration Guides

[Secure Acceptance Checkout API Integration Guide](#)

[Secure Acceptance Hosted Checkout Integration Guide](#)

Virtual Terminal

Cybersource Virtual Terminal acts as a web-based point-of-sale where merchants and partners can accept payments for services rendered. It is currently not available for OCTs and push payments. It will be part of a future enhancement.

The Virtual Terminal is an online order form where you can enter a customer's order information. You log in to the Cybersource Business Center through your Web browser with your Cybersource username and password and select the Virtual Terminal order form. The Virtual Terminal uses your current Internet connection and Web browser. The terminal set up takes about 15 minutes.

The advantages of using the Virtual Terminal are:

- Fast and simple: Requires no development time or technical skills.
- Flexible: Processes transactions from any computer with an Internet connection.
- Secure: Encrypts order data to protect customer information.
- Compliant: Complies with regulations for storing sensitive payment information.

- **Organized:** Uses the Business Center and reports to review and manage all of your orders.

While the Virtual Terminal has many advantages, it is not the best solution for all circumstances. The Virtual Terminal is suitable for:

- Any merchant or business that has an order volume small enough to enter each order manually (unless used with another communication method).
- Mail and Telephone Order companies with multiple call center users.
- Small Internet businesses without an online order form.
- Merchants who transmit orders through more automated methods, but only occasionally do manual entries or adjustments.

The Virtual Terminal might not meet your business needs if your business:

- Has more orders than you can enter by hand.
- Is already set up with a shopping cart on your Web site.
- Needs extensive customization of your order form.
- Has access to someone with scripting or programming skills.
- Needs to share order data with a fulfillment house.

BIN Lookup

The Bank Identification Number (BIN), also known as *Issuer Identification Number (IIN)*, is the standardized global numbering scheme globally used for identifying institutions that assign primary account numbers (PANs) to their customer. The BIN Lookup API accepts the card account number and returns information on items like issuer country code, billing currency, account type, Fast Funds participation status, and the recipient issuer's ability to receive OCTs.

Based on the issuing BIN, using account lookup functionality, confirm that the card is eligible for receiving OCTs and meets the criteria of originating entity and merchant:

- **Card Type:** What type of card is this (debit, credit, reloadable, or prepaid)?
- **Country of Card Issuance:** In which country is the card issued?
- **OCT Enabled:** Is the card is enabled to receive OCTs?

- **Fast Funds Enabled:** Is the card enabled for Fast Funds? (You may want to restrict non-Fast Funds enabled cards.)

In general, the key advantage of BIN lookup is to identify characteristics of a card and check eligibility for OCT/fast funds. For example, when a customer registers their card, the merchant can use BIN lookup to ensure only certain type of cards (for example, only debit/prepaid but no credit) are used. The BIN lookup can also be used to check for fast funds eligibility, and restrict registration to only fast funds enabled cards. The merchant can check for many other characteristics ensuring that the card profile used for receipt of funds meets their business requirements.

Currently, BIN lookup is supported only for Visa and Mastercard.

There are currently two versions of the BIN Lookup APIs available: version 2 and version 3. Version 3 of the API includes additional information for Visa cards only.

BIN Lookup API

Account Lookup is available as a standalone API used in conjunction with Payouts. This API accepts the card account number and returns information on issuer country code, billing currency, account type, Fast Funds participation status, and the recipient issuer's ability to receive OCTs.

This enhanced information in version 3 includes:

- OCT and fast funds enablement with a separate flag for domestic and cross-border transactions.
- OCT and fast funds enablement with a separate flag for money transfer transactions (for example, P2P) and non-money transfer transactions (for example, Funds Disbursement).

BIN Lookup Version 2.0

The API should be called with the Use Mode of **P** which specifies that the service should return the OCT details about a specified card account number. The BIN lookup service resource is appended to the hostname with a **useMode** parameter of 'P': `/vas/v2/account-number-lookup/?useMode=P`

When reviewing the response supplied by the BIN lookup service, a merchant should review the `pushFundsBlockIndicator` API field response. This identifies to a merchant whether a card is eligible for OCT payments.

- If the response value is *A*, *B*, or *C*, the card is eligible for OCT payments.
- If the response value is *N*, the card is not eligible for OCT payments.

For Mastercard, the values are presented in `pushFundsDomesticIndicator` and `pushFundsCrossBorderIndicator`, and are set to either true or false.

The `fastfundsindicator` indicates the issuer's level of support for Fast Funds transactions. A Fast Funds transaction makes funds available to the recipient within 30 minutes. An issuer that supports original credit transactions (OCTs) but not Fast Funds transactions makes funds available within two business days.

- If the value is *B*, *C*, or *D*, funds are available to the recipient within 30 minutes of successful transfer.
- If the value is *N*, the funds are available within two business days of successful transfer.

The only required field in the request is **accountNumber**.

```
{ "paymentAccountInformation": { "card": { "number": <<CARD NUMBER>> } } }
```

The **networkroutingorder** field is optionally used by Push Payments Gateway participants (merchants and acquirers) to get the attributes for specified networks only. This is supported in the US only for domestic transactions involving Push Payments Gateway Service.

Below are links to the API documentation containing details of the request and response fields for BIN Lookup:

[BIN Lookup Service, Using the SCMP API](#)

[BIN Lookup Service, Using the Simple Order API](#)

BIN Lookup Version 3.0

Similar to version 2, the version 3 API should be called with the Use Mode of **P**, which specifies that the service should return the OCT details about a specified card account number.

Destination: <https://apitest.cybersource.com/vas/v3/account-number-lookup>

For Visa cards, the response contains the following indicator with a Y or N response indicating OCT or Fast Funds availability:

- `onlineGamblingPushFundsDomesticIndicator`
- `onlineGamblingFastFundsDomesticIndicator`
- `businessFundedTransferFastFundsCrossBorderIndicator`
- `businessFundedTransferPushFundsDomesticIndicator`
- `consumerFundedTransferFastFundsDomesticIndicator`
- `consumerFundedTransferFastFundsCrossBorderIndicator`
- `onlineGamblingPushFundsCrossBorderIndicator`
- `businessFundedTransferFastFundsDomesticIndicator`
- `consumerFundedTransferPushFundsDomesticIndicator`
- `onlineGamblingFastFundsCrossBorderIndicator`
- `businessFundedTransferPushFundsCrossBorderIndicator`
- `consumerFundedTransferPushFundsCrossBorderIndicator`

With Mastercard, these values are indicated by setting the **pushFundsDomesticIndicator** and **pushFundsCrossBorderIndicator** parameters to either true or false.

Acquirer Risk Control

The Acquirer Risk Control (ARC) settings are enabled only for resellers. In the Business Center, merchants configure risk controls for Payouts to protect themselves from risky transactions.

Restricting specific payment attributes and setting limits for specific fields provides the merchant with greater control over their transaction. Different risk control settings can be configured and saved as a profile to be assigned to a merchant. These ARC profiles provide flexibility when managing different risk potential with various merchants in a portfolio. In the Business Center, the ARC settings are accessed from the left navigation pane by selecting **Portfolio Management > Merchant Risk Controls Profile**. You can create a new ARC profile or assign an existing profile to a merchant. There are three sections available to configure:

- Payouts
- ECI Settings
- API Settings

Payouts Settings

An acquirer can set restrictions specific to Payouts transactions for a merchant by enabling the **Activate Payouts Risk Controls** option in the Acquirer Risk Controls section of merchant configuration.

After the Payouts Risk Controls are enabled, restrict the types of accounts eligible for Payouts and set limits on the value and volume of Payouts transactions allowed during a specified time period. The acquirer can also be notified when a merchant approaches designated limits. From these settings, the ability to accept Payouts transactions can also be suspended (and resumed).

ECI Settings

The Risk Controls module enables acquirers to configure Electronic Commerce Indicator (ECI) settings for a merchant.

The ECI is used in payer authentication to indicate the level of security used when the cardholder provides payment information to the merchant. Its value corresponds to the authentication result and the characteristics of the merchant checkout process. Each card network, such as Visa, Mastercard, or JCB has specific rules managing the appropriate values and use of the ECI settings.

API Settings

Merchants can configure API Service Settings in Risk Controls to manage credit card transactions. These API Service controls work only with credit cards.

1. From the left navigation pane of the Business Center, select **Portfolio Management > Merchant Risk Controls Profile**.
2. Enable the **Activate API Risk Controls** option.
3. Check the appropriate **Reject** box or boxes.
4. Click **Save**.

FX Rates API

The Foreign Exchange (FX) Rates API offers access to the Visa daily currency exchange rate providing a better user experience for cross-border and multi-currency transactions.

The FX Rates API accepts a source and destination currency pair and returns the current day's Visa exchange rate for the pair. It can also take a transaction amount in the source currency and return the same amount in the destination currency. This API is used in conjunction with the OCT transaction.

Merchant Registration for Testing Transactions

Cybersource offers a set of APIs that provide Visa functionality for your applications.

You can set up a test account in a test environment and evaluate the Payouts API services and other enterprise payment management solutions. You can send test transactions or evaluate various configurations as if you were the customer. When finished testing the application, you can request to move to the production environment and go live.

Merchants work with three different environments:

- **Test** Set up and test transactions from the customer perspective to ensure that the transaction process runs smoothly.
- **VCMS** Test transactions using the VisaNet Certification Management Service. Work with your acquirer to verify that this service is available. VCMS testing is compulsory before a new acquirer can start submitting OCTs to VisaNet.
- **Production** Any issues uncovered during the testing phase are resolved, and you start processing transactions with customers.

You must submit an evaluation form that contains business contact information and create your Merchant ID (MID). Register for an evaluation account by completing this [evaluation form](#). Once you are registered, you will receive an email with instructions for setting up an **Account Admin** account and a **Merchant Admin** account.

- An **Account Admin** account is the master account for managing a specific Merchant ID.
- A **Merchant Admin** account is an account that enables the user to view transactions details, perform Virtual Terminal transactions, and view reports for a specific Merchant ID.

Sandbox Testing

We encourage you to send test transactions to the Cybersource test server to verify that your implementation works as expected. If you are testing payment services, be aware that the Cybersource test server simulates processor responses.

Test server hostname: **apitest.Cybersource.com**

Managing your Evaluation Accounts

To view Evaluation account test transactions, click **Transaction Search**, and click **General Search**.

Administer users and access privileges

- To access Evaluation Account administration options, click **Account Management**.
- To add sub-users and manage their passwords and access permissions, click **User Administration**.
- To create Roles with pre-defined access permissions, click **Role Administration**.

View Reports

The Cybersource Reporting System offers a number of reports to assist with your evaluation. Click **Reports** on the left side of the page.

Going Live

Before you can process real payment transactions with Cybersource, we must migrate your evaluation account to a production system and update your Merchant ID status. Contact your [local sales representatives](#) to discuss Cybersource solutions and pricing to begin the Go-Live process.

Glossary of Abbreviations

Acronym	Full Name
ABA	American Bankers Association
ACH	Automated Clearing House
AFT	Account Funding Transactions
AIQ	Acquirer Information Questionnaire
AP	Asia-Pacific (region)
API	Application Programming Interface
ARC	Acquirer Risk Controls
ATM	Automated Teller Machine
AVS	Address Verification Service
B2B	Business-to-Business
BAI	Business Application Identifier
BAMS	Bank of America Merchant Services
BIN	Bank Identification Number
CAID	Card Acceptor Identifier
CAS	Customer Acceptance System
CEMEA	Central Asia, Middle East, Africa (region)
CIQ	Client Implementation Questionnaire
CSV	Comma-Separated Values (file format)
CVV/CVV2	Card Verification Value
DSS	Data Security Standard
ECI	E-Commerce Indicator
EMS	Expert Monitoring Solution (Mastercard feature)
FAQ	Frequently Asked Questions
FX	Foreign Exchange
HDFC	HDFC Bank
HMAC	Hashed Message Authentication Code

Acronym	Full Name
IIN	Issuer Identification Number
ISO	International Standards Organization
JNLP	Java Network Launch Protocol
JSON	JavaScript Object Notation
JWT	Java Web Token
KYC	Know Your Customer
LAC	Latin America and Caribbean (region)
MAMS	Merchant Account Management System
MCB	Metropolitan Commercial Bank
MCC	Merchant Category Code
MID	Merchant ID
OCT	Original Credit Transaction
P2P	Person-to-Person
PAN	Personal Account Number
PCI	Payment Card Industry (standard)
PCR	Processing Control Record
PEM	Partner Engagement Manager
PIF	Partner Information Form
PPGS	Payment Gateway Service Form
PRM	Program Request Management
S/MIME	Secure/Multipurpose Internet Mail Extensions
SAQ	Self-Assessment Questionnaire
SCMP	Simple Commerce Messaging Protocol
SFTP	Settlement Funds Transfer Point
SMS	Single Message System
SOAP	Simple Object Access Protocol
TC33A	TC33A Capture file This file is sent at the end of day to the acquirer and contains information about the purchases and refunds that a merchant submits to Cybersource.

Acronym	Full Name
TID	Terminal ID
TMS	Token Management Service
UI	User Interface
US	United States
USD	United States Dollar
VOL	Visa Online
VPC	Visa Platform Connect
VROL	Visa Resolve Online
VSS	Visa Settlement Summary

Debit Fast Funds Markets in the World

The following is a list of the countries where debit Fast Funds are enabled:

Albania	Cook Islands	Indonesia	Mongolia	Slovakia
Angola	Costa Rica	Israel	Montenegro	South Africa
Anguilla	Cote D'Ivoire	Jamaica	Myanmar	Spain
Armenia	Cyprus	Kazakhstan	Namibia	Sri Lanka
Azerbaijan	Czech Republic	Kenya	Nicaragua	St. Lucia
Barbados	Djibouti	Kiribati	Nigeria	St. Vincent & Grenadines
Belarus	Egypt	Kosovo	Occupied Palestinian Territories	Tajikistan
Benin	El Salvador	Kuwait	Oman	Thailand
Bolivia	Equatorial Guinea	Kyrgyzstan	Pakistan	Tonga
Botswana	Estonia	Laos	Philippines	Tunisia
British Virgin Islands	Ethiopia	Latvia	Puerto Rico	Turkey
Brunei Darussalam	Gambia	Libyan Arab Jamahiriya	Republica Dominicana	Turkmenistan
Burkina Faso	Georgia	Lithuania	Romania	Turks & Caicos Islands
Burundi	Gibraltar	Macedonia	Russian Federation	U.S. Virgin Islands
Cambodia	Greece	Madagascar	Rwanda	Uganda
Cameroon	Grenada	Malaysia	Samoa	Ukraine
Canada	Guatemala	Maldives	Saint Maarten	United Republic of Tanzania
Chad	Guinea	Malta	Senegal	United States of America
Comoros	Guyana	Mauritania	Seychelles	Vietnam

Congo	Guinea-Bissau	Mauritius	Sierra Leone	Yemen Arab Republic
Congo, Republic of	Haiti	Moldova, Republic of	Singapore	Zambia

Cybersource Error Codes

Error Code	Steps	VIP Decline Response Codes	Reason for Decline
208-DCARDREFUSED	A GCT resource will provide the sequence and script the response.	12 (Invalid transaction)	If the recipient issuer received a waiver related to the receipt of OCTs, the recipient issuer declines an OCT with a response code 12.
208-DCARDREFUSED	A GCT resource will provide the sequence and script the response.	57 (Transaction not permitted to cardholder)	For money transfer OCTs destined to an issuer PCR that cannot accept Processing Code 26, V.I.P. declines the transaction with a response code 57. If the issuer PCR is not set up in VisaNet to support Field 104 in TLV format, V.I.P. declines the transaction with response code 57.
210 - DCARDREFUSED	Repeat as many times as needed to exceed the limit. A Visa test analyst may need to change the country code that is associated with the test card being used if the originator supports only domestic OCT.	61 (Exceeds approved amount limit)	On enhanced OCTs, if a transaction exceeds an issuer-defined 1-day, 7-day or 30-day amount limit, and the issuer option is to decline when a limit is exceeded, V.I.P. declines the transaction with a response code 61. On enhanced OCTs, if a transaction exceeds both an issuer-defined amount limit and an issuer-defined count limit, and the issuer option is to decline when a limit is exceeded, V.I.P. declines the transaction with a response code 61.

Error Code	Steps	VIP Decline Response Codes	Reason for Decline
211-DCARDREFUSED	A GCT resource will provide the sequence and script the response.	62 (Restricted card – card invalid in this region or country)	If an OCT is sent to an embargoed country (Cuba, Iran, Syria, or Sudan), V.I.P. declines the transaction with a response code 62.
233-DINVALIDDATA	Follow the steps in the Decline Reason column.	64 (Transaction does not fulfill AML requirements.)	On enhanced Money Transfer OCTs, if either the Sender Reference Number (Tag 01) or the Sender Account Number (Tag 02) in Field 104, Usage 2, Dataset Value 5F is not present, V.I.P. declines the transaction with a response code 64. For all domestic U.S. and all cross-border enhanced money transfer OCTs, if Sender Name (Tag 03), Sender Address 47(Tag 04), Sender City (Tag 05), Sender State (Tag 06) (if Field 43, pos. 39–40 is US or CA), and Sender Country (Tag 07) in Field 104, Usage 2, Dataset Value 5F are not present, V.I.P. declines the transaction with a response code 64. On enhanced money transfer OCTs, if Source of Funds (Tag 08) in Field 104, Usage 2, Dataset ID 5F is not present on transactions destined to the U.S, V.I.P. declines the transaction with a response code 64. V.I.P. Processing Rule for the Recipient/Name On cross-border enhanced money transfer OCTs, if the Recipient Name (Tag 0A) in Field 104, Usage 2, Dataset ID 5F is not present or contains all spaces or zeros, V.I.P. declines with a response code 64. V.I.P. Processing Rule for Sender Name (Tag 03) and Recipient

Error Code	Steps	VIP Decline Response Codes	Reason for Decline
			Name (Tag 0A) in Field 104 Dataset ID 5F V.I.P. declines 0200 OCTs with a BAI of AA/PP with a response code 64 if the Sender Name (Tag 03) or Recipient Name (Tag 0A) in Field 104 Dataset ID 5F, Tag 03 or 0A, contains: >? (Question mark) >All numerics >Only one character
251-DCARDREFUSED	Repeat as many times as needed to exceed the limit. A Visa test analyst may need to change the country code that is associated with the test card being used if the originator supports only domestic OCT.	65 (Exceeds approved count limit)	On enhanced OCTs, if the transaction exceeds an issuer-defined 1-day, 7-day or 30-day count limit and the issuer option is to decline when a limit is exceeded, V.I.P. declines the transaction with a response code 65.
150-ESYSTEM	F14 not present (expiration date) F104 Dataset ID 5F Tags 02, 03, 04, 05, 07, and 08 present.	91 (Issuer unavailable)	If the issuer is unavailable for an OCT, V.I.P. declines the transaction with response code 91.
233-DINVALIDDATA	Follow steps in Column D (Decline Reason)	93 (Transaction cannot be completed – violation of law)	If an acquirer, service provider, or merchant sends an OCT to a recipient issuer BIN that is blocked from receiving it, V.I.P. declines the transaction with a response code 93. When a U.S. acquirer, service provider, or merchant sends OCTs with an MCC value of 4829 or 6012, the OCT must contain a BAI of AA or PP. If the OCT does not, V.I.P. declines the transaction with a response code 93. On U.S.

Error Code	Steps	VIP Decline Response Codes	Reason for Decline
			<p>and non-US domestic and all cross-border enhanced Money Transfer OCTs, if Field 104, Dataset ID 5F, Tag 07 (Sender Country) does not contain a 3-digit ISO numeric country code, V.I.P. declines the transaction with response code 93.</p> <p>If a recipient issuer is blocked from receiving the OCT, VisaNet will decline the transaction with a response code 93 except for embargoed countries (Cuba, Iran, Syria, and Sudan), where the response code is 62 (Restricted Card – card invalid in this region or country). On domestic enhanced money transfer OCTs, if the amount is greater than 2,500 USD or the specific country limit, V.I.P. declines the transaction with a response code 93.</p> <p>On cross-border enhanced money transfer OCTs, if the amount is greater than 2,500 USD, V.I.P. declines the transaction with a response code 93. V.I.P. Processing Rule for the Sender's Country</p> <p>On enhanced OCTs, if Sender Country (Tag 07) in Field 104, Usage 2, Dataset ID 5F is for a country on the list of U.S. OFAC comprehensively sanctioned countries or regions that currently consists of Iran, Sudan, Syria, Crimea, and North Korea V.I.P. declines the transaction with response code 93</p> <p>Note: Visa currently blocks transactions when the acquirer, service provider,</p>

Error Code	Steps	VIP Decline Response Codes	Reason for Decline
			or merchant's or issuer's country is on the list of U.S. OFAC comprehensively sanctioned countries.
233-DINVALIDDATA	GCT resource to provide the sequence and script the response	94 (Duplicate transmission)	If a duplicate transaction is received, V.I.P. declines it with response code 94.
233-DINVALIDDATA	Follow steps in Column D (Decline Reason)	0494 (Field or data missing or invalid)	V.I.P. Processing Rule V.I.P. rejects 0200 OCTs with reject code 0494 if they do not contain the Business Application Identifier (BAI) in Field 104 Dataset ID 57. V.I.P. Processing Rule V.I.P. rejects domestic 0200 OCTs with a BAI of AA or PP with reject code 0494 (Field or data missing) if they do not contain both Field 104 Dataset IDs 5F and 71. V.I.P. rejects enhanced OCTs with the existing reject code 0494 (Field or data missing or invalid) for which any of the following tags in Field 104 Dataset IDs 5F exceeds its maximum length: Tags 01–07 and 0A.