

MERCHANT OPERATING MANUAL

Getnet México Servicios de Adquirencia, S.A. de C.V.
Last Updated: August 2026



This Manual is operational in nature and must be read as a practical guide for processing Transactions, documenting sales, handling inquiries, preventing fraud, retaining evidence, and operating authorized channels. The obligations, responsibilities, restrictions, economic matters, grounds for termination, and all other legal terms governing the relationship between Getnet and the Merchant are set forth in the Contrato de Afiliación and its current annexes.

The description of a channel, service, or feature in this Manual does not automatically authorize its use; the Merchant may use only what has been authorized under the Contrato de Afiliación, the Solicitud, carátula, annexes, appendices, or applicable operational enablements.

Notes on Translation and Legal Terminology

This English version is provided solely for operational reference. To preserve legal meaning under Mexican law, the official corporate name and the Spanish titles or names of governing documents and certain contractual terms, including Contrato de Afiliación, Solicitud, carátula, Fondo de Reserva, Pagaré de Venta, and Programa de Afiliación, remain in Spanish. English equivalents of other defined terms are descriptive only. In the event of any inconsistency, the Spanish-language Contrato de Afiliación and its current annexes prevail.



Contents

1. Purpose and Operational Scope3

1.1 Operating Environments3

1.2 Prohibited Transactions and Operational Restrictions3

2. General Operating Guidelines4

2.1 Operational Acceptance of Payment Instruments4

2.2 Daily Reconciliation4

2.3 Internal Document Management4

3. Security, Data, and Credentials5

3.1 Protection of Cardholder Data5

3.2 Passwords and Access5

3.3 Equipment, Terminals, and Platforms5

3.4 Information Incidents5

4. Transaction Processing6

4.1 General Authorization Flow6

4.2 Possible Operational Responses6

4.3 Authorization Best Practices6

5. Card-Present Operations7

5.1 Pre-Transaction Checks7

5.2 Card-Present Transaction Receipt7

5.3 Common Errors7

6. E-Commerce and Card-Not-Present Operations8

6.1 Operational Requirements for the Online Store8

6.2 Data Captured in E-Commerce8

6.3 Purchase Order and Acknowledgment of Receipt9

6.4 3D Secure and Risk Tools9

7. Refunds and Supporting Documentation9

7.1 Best Practices for Refunds in Card-Not-Present Transactions9

7.2 Recommended Evidence10

8. Receipt Requests, Inquiries, and Chargebacks10

8.1 Responding to a Receipt Request10

8.2 Responding to Chargebacks10

8.3 Common Reasons for Claims10

9. Fraud Prevention11

9.1 E-Commerce Red Flags11

9.2 Recommended Checks Before Delivery11

9.3 Internal Fraud Prevention12

10. Operational Prevention of Money Laundering12

10.1 Operational Red Flags12

10.2 Recommended Actions When Suspicious Activity Is Identified12

11. Special Services and Modules13

12. Additional Information13

Appendix A. Operational Glossary14



1. Purpose and Operational

This Merchant Operating Manual establishes the operational rules, procedures, and controls applicable to Transaction processing, sales documentation, handling inquiries, fraud prevention, evidence retention, and the operation of authorized channels. Its purpose is to serve as a reference tool for Merchant personnel and the teams responsible for monitoring day-to-day operations.

This Manual neither reproduces nor replaces the legal, economic, or contractual provisions of the Contrato de Afiliación. Defined terms, contractual integration, order of precedence, consequences of noncompliance, term, termination, commissions, charges, setoffs, Fondo de Reserva, and all other legal or commercial terms are governed by the Contrato de Afiliación and the documents incorporated into it.

Usage Rule

Use this Manual to learn how to operate. Refer to the Contrato de Afiliación for rights, obligations, responsibilities, economic effects, and legal consequences.

The description of channels, services, or features in this Manual must not be interpreted as authorization to use them. Each operating channel must be enabled and authorized in advance for the Merchant in accordance with the Contrato de Afiliación, the Solicitud, carátula, annexes, appendices, or applicable operating instructions.

1.1 Operating Environments

Enviroment	Operational Description
Card-Present	The Card or Payment Instrument is physically presented or used in person through a POS Device or equivalent solution.
Card-Not-Present	The Transaction is processed without the physical presence of the Card, including e-commerce, telephone sales, recurring charges, or payment links when enabled.
E-Commerce	The Cardholder enters data in an Online Store, payment page, or authorized digital flow.
Special Modules	Services such as DCC, recurring charges, MSI, Cashback, Get Commerce, Get Link & Pay, or other modules, as enabled and contracted.

1.2 Prohibited Transactions and Operational Restrictions

The Merchant must not process Transactions that do not correspond to a legitimate, documented sale conducted within its authorized line of business. This rule protects the integrity of operations, reduces fraud risk, prevents misuse of the Merchant number, and helps ensure that Transactions can be supported with sufficient evidence in connection with inquiries or Chargebacks. Accordingly, the Merchant must:

- Not process illegal, fraudulent, fictitious, or unauthorized Transactions.
- Not use the merchant number, POS Device, Online Store, or authorized channel for third-party transactions.
- Not process transactions relating to goods or services not provided by the Merchant.
- Not artificially split a sale to alter authorization or review controls.
- Not improperly or repeatedly reprocess declined transactions.
- Not use Transactions to obtain cash, refinance debt, or move funds without an actual sale.



2. General Operating Guidelines

The guidelines in this section describe day-to-day controls for accepting Payment Instruments, reconciling transactions, and retaining documentation in an orderly manner. Their purpose is to reduce data-entry errors, duplicate charges, claims, Chargebacks, loss of evidence, and fraud risk. The related legal obligations are set forth in the Contrato de Afiliación and the applicable Card Network Rules.

2.1 Operational Acceptance of Payment Instruments

Payment Instruments must be accepted clearly, consistently, and through the authorized channel. The Merchant must avoid practices that could confuse the Cardholder about the amount, currency, the merchant processing the charge, or the terms of the purchase. Accordingly, the Merchant must:

- Confirm that the Card or Payment Instrument is enabled for the channel being used.
- Use only the channel, device, or platform appropriate for the transaction to be processed.
- Avoid practices that may confuse the Cardholder regarding the amount, currency, merchant, or transaction description.
- Not split a sale into multiple Transactions for the purpose of improperly changing authorization or operational controls.
- Not reprocess a declined Transaction without reviewing the reason for the decline and the applicable procedure.

2.2 Daily Reconciliation

Daily reconciliation makes it possible to identify discrepancies before they lead to claims, duplicate Transactions, or settlement errors. It must therefore be performed as part of the standard end-of-day process, not only when an inquiry arises. Accordingly, the Merchant must:

- Reconcile sales, refunds, and POS Device or platform reports at the close of each operating day.
- Compare amounts against individual reports and batch totals.
- Identify duplicate charges, declined transactions, incomplete transactions, and amount discrepancies.
- Record any identified discrepancy internally to facilitate follow-up.
- Retain operational evidence in accordance with the Contrato de Afiliación and the applicable procedure.

2.3 Internal Document Management

Supporting documentation must be retained securely, legibly, in an orderly manner, and in an accessible form. Its operational value depends not only on its existence, but also on the ability to locate it promptly and link it to the correct Transaction when requested. Accordingly, the Merchant must:

- Keep receipts, Pagarés de Venta, purchase orders, acknowledgments of receipt, refund records, and digital evidence organized.
- Classify documents by date, merchant number, channel, order number, or Transaction reference.
- Ensure that information is legible, complete, and retrievable when needed to respond to an inquiry.
- Avoid alterations, cross-outs, or deterioration that could make the evidence difficult to read or validate.
- Do not retain sensitive data that must not be stored after authorization, such as CVV2/CVC2.



3. Security, Data, and Credentials

This section sets out operational controls for protecting Cardholder data, credentials, POS Devices, platforms, Online Stores, systems, and Transaction-related documentation. Legal and contractual obligations relating to confidentiality, data protection, incidents, and compliance with security programs are set forth in the Contrato de Afiliación and the applicable standards.

3.1 Protection of Cardholder Data

The Merchant must:

- Request only the information necessary to complete, authenticate, document, or fulfill the Transaction.
- Not record or store CVV2/CVC2 after requesting Authorization.
- Not print CVV2/CVC2 on receipts, Pagarés de Venta, delivery documents, emails, or documents provided to the Cardholder.
- Truncate the Card number when it is necessary to include it in supporting documents.
- Restrict access to Cardholder information to personnel who need it to operate or respond to inquiries.

These measures reflect the principle that data minimization reduces operational exposure and facilitates compliance with security controls.

3.2 Passwords and Access

Credentials must be treated as personal and non-transferable. Sharing usernames or passwords impairs Transaction traceability, makes it difficult to assign operational responsibility, and increases the risk of unauthorized system or platform use. Accordingly, the Merchant must:

- Assign credentials only to authorized users.
- Do not share passwords among users, branches, or departments.
- Change or revoke access when compromise is suspected.
- Do not store passwords in visible documents or on shared devices.
- Train personnel to recognize unusual requests or attempts to obtain credentials.

3.3 Equipment, Terminals, and Platforms

The Merchant must:

- Use devices and platforms in accordance with the intended operational flow for each channel.
- Physically secure terminals, equipment, servers, and mobile devices used to accept payments.
- Do not operate equipment that shows faults or error messages without reviewing the applicable procedure.
- Keep equipment in a condition that allows legible receipts to be printed or generated.
- Retain backups or reports that make it possible to reconstruct the transaction in the event of a

3.4 Information Incidents

If any unauthorized access, use, disclosure, transmission, or compromise involving information, systems, documents, or credentials is suspected, the operational priority is to preserve evidence and escalate the incident through the designated channels. Manipulating or deleting records may prevent the facts from being reconstructed.



The Merchant must:

- Preserve records, reports, logs, emails, and electronic evidence if unauthorized access is suspected.
- Do not delete, alter, or manipulate evidence related to the incident.
- Escalate the incident internally through the channels defined by Getnet and the Contrato de Afiliación.
- Cooperate in reconstructing the facts and identifying the data involved.
- Implement corrective measures to reduce the risk of recurrence.

4. Transaction Processing

In general, processing a Transaction includes capturing transaction data, requesting Authorization, receiving the Issuer's response, documenting the transaction, and settling the applicable batch or record. Authorization allows the sales flow to continue, but does not guarantee final payment or eliminate the risk of a Chargeback, claim, reversal, subsequent decline, or request for documentation.

4.1 General Authorization Flow

1. The Customer or Cardholder seeks to purchase goods or services using a Payment Instrument.
2. The Merchant captures or receives the transaction data through the authorized channel: POS Device, Online Store, software, payment link, or the applicable platform.
3. The request is sent electronically to the Acquirer or the applicable system for routing.
4. The Issuer determines whether to approve, decline, or refer the Transaction for additional verification.
5. The Merchant receives the response and acts according to the result.
6. The Transaction is documented with the receipt, reference, order, acknowledgment, or other evidence applicable to the channel used.

4.2 Possible Operational Responses

Response	Suggested Operational Action
Approved	Complete the sale and retain evidence of the Transaction, delivery, or provision of services.
Declined	Request another form of payment and avoid improper or repeated retry attempts.
Referral / Additional Verification	Follow the applicable verification procedure before completing the transaction.
Technical Error	Do not assume that the sale was approved; review reports, possible duplicate processing, and transaction status before reprocessing.

4.3 Authorization Best Practices

Authorization best practices are intended to ensure that the amount, channel, date, and evidence correspond to the actual transaction. The Authorization Code must be retained with the applicable documentation, but must not be viewed as sufficient evidence on its own.

In addition, the Merchant must follow these best practices:



- Request Authorization for the exact amount of the Transaction.
- Process the Transaction on the date of the sale or provision of the service, unless the channel procedure specifies otherwise.
- Do not complete delivery of goods or provision of services unless sufficient operational confirmation of the applicable authorization or payment has been received.
- Do not assume that an Authorization Code eliminates the possibility of subsequent claims.
- Retain the Authorization Code or the reference generated by the system.

5. Card-Present Operations

Card-present operations require confirming that the Payment Instrument is processed through the appropriate device and that the receipt or record accurately reflects the minimum required Transaction details.

5.1 Pre-Transaction Checks

Before processing a card-present transaction, the Merchant must perform the following checks:

- Confirm that the Card has not expired when physical inspection is applicable.
- Use chip, PIN, contactless, magnetic stripe, or authorized manual entry, as available in the applicable flow.
- When the flow requires a signature, obtain it and check it for consistency with the Card, where applicable.
- Do not ask the Cardholder to disclose the PIN verbally.
- Do not process the transaction if the device displays a decline or Authorization is not obtained.

5.2 Card-Present Transaction Receipt

After processing a card-present transaction, the Merchant must perform the following checks:

- Verify that the receipt shows the amount, date, merchant name, reference, and Authorization, where applicable.
- Keep the Merchant copy or record in good condition and legible.
- Provide the Cardholder with the appropriate copy or receipt.
- Do not alter, punch, staple, or damage the receipt if doing so affects its legibility.
- Internally record any operational irregularity identified during the sale.

5.3 Common Errors

To reduce processing errors, claims, and Chargebacks, the Merchant must avoid the following practices:

- Processing the same sale twice.
- Entering an amount different from the amount disclosed to the Customer.
- Closing the batch without reviewing discrepancies.
- Using illegible receipts.
- Reprocessing declined transactions without operational justification.
- Using a terminal or channel that does not correspond to the establishment or operational flow.



6. E-Commerce and Card-Not-Present Opera-

Card-Not-Present Transactions present a higher level of operational risk because the Card is not physically presented to the Merchant and the Cardholder's identity may depend on digital, documentary, or authentication controls. Accordingly, this section sets out validation controls, information that must be visible to the Customer, security measures, and documentary evidence to reduce claims, fraud, and disputes relating to nondelivery of goods or nonperformance of services.

6.1 Operational Requirements for the Online Store

The Online Store must provide the Cardholder with clear, complete, and visible information before the purchase is completed. This enables the Customer to identify the Merchant or business, understand the relevant transaction terms, and recognize the charge on their account statements. Accordingly, the Online Store must include the following information, where applicable:

- The Merchant or business name, visible to the Cardholder.
- A complete description of the goods or services offered.
- The price, total Transaction amount, and currency.
- The delivery policy, including applicable time frames, costs, and terms.
- The return, refund, and cancellation policy, where applicable.
- Customer service contact information, such as an email address, telephone number, or physical address.
- The address of the permanent establishment or location information required by the channel.
- Any applicable legal, export, geographic, or delivery restrictions.
- The policy governing privacy or the processing of Customer data.
- Security measures applicable to the payment flow, such as SSL, 3D Secure, or other enabled tools.

6.2 Data Captured in E-Commerce

Purpose	Data Identified in the Source Documents
Payment	Card number, expiration date, CVV2/CVC2, Card brand, and, when required by the flow, Issuer name.
Identification	Cardholder's full name and contact telephone number, when necessary.
Billing	Full billing address when required by the flow or validations.
Delivery	Delivery address and the name of the person authorized to receive goods or services.
Evidence	Purchase order, order number, acknowledgment of receipt, delivery date, and the recipient's name and signature, as applicable.

Data Minimization

The preceding list does not mean that all data must be requested in every case. Only the data necessary to operate, authenticate, document, fulfill, or handle the Transaction should be requested.



6.3 Purchase Order and Acknowledgment of Receipt

The purchase order and acknowledgment of receipt are key evidence of what was sold, when the transaction was authorized, to whom it was delivered, and under what conditions. In disputed transactions, these documents help link the Transaction to the corresponding delivery or provision of services.

When the transaction involves delivery of goods or provision of services, the Merchant must:

- Generate an order or order reference for each sale involving product delivery or service provision.
- Include the order number, the Merchant's trade name, date, Cardholder name, amount, Authorization, and description of the good or service.
- Include the delivery address and authorized recipient, where applicable.
- Obtain an acknowledgment of receipt showing the date, delivery address, and the recipient's name and signature, when the nature of the delivery permits.
- Retain the order and acknowledgment as operational evidence for inquiries or claims.

6.4 3D Secure and Risk Tools

Authentication and risk management tools, such as 3D Secure, risk modules, additional validations, or tokenization, can strengthen operational controls for Card-Not-Present Transactions. However, their use does not replace sales documentation or fully eliminate the risk of fraud, claims, or Chargebacks. Their effectiveness depends on the channel used, the reason for the dispute, the applicable Card Network Rules, the enabled configuration, and the available evidence.

When these tools are enabled for the applicable product, channel, or flow, the Merchant must:

- Use 3D Secure or other authentication mechanisms where applicable.
- Retain evidence of the authentication result, when available.
- Apply risk rules, email validations, manual review, tokenization, or other controls only when enabled for the applicable service.
- Do not assume that a security tool fully eliminates the risk of fraud, claims, or Chargebacks.
- Review unusual transactions before releasing goods for delivery or beginning to provide the service when risk indicators warrant further review.

7. Refunds and Supporting Documentation

Refunds must be clearly documented to prevent duplicate refunds, accounting discrepancies, or claims. This section describes operational controls without governing economic or contractual consequences.

7.1 Best Practices for Refunds in Card-Not-Present Transactions

In Card-Not-Present transactions, refunds must be processed in a traceable manner and linked to the original Transaction. This helps prevent duplicates, provide evidence of the refund to the Customer, and retain sufficient evidence in the event of inquiries, claims, or Chargebacks. For these purposes, the Merchant must:

- Process the refund through the channel corresponding to the original Transaction, where applicable.
- Identify the original Transaction, date, amount, Authorization, or reference.
- Generate a receipt or refund record when the system permits.
- Provide the Customer with a copy or confirmation appropriate to the channel used.
- Internally record the reason for the refund and retain supporting evidence.



7.2 Recommended Evidence

Transaction Type	Operational Evidence
Card-Present Sale	Receipt, Pagaré de Venta or electronic record, Authorization, batch, and device report.
E-Commerce Sale	Purchase order, payment confirmation, 3D Secure result, and evidence of delivery or service performance.
Refund	Refund record, original reference, processed receipt, and confirmation to the Customer.
Chargeback or Inquiry	Documentation specified in the request: receipt, order, acknowledgment, evidence of service, or related communication.

8. Receipt Requests, Inquiries, and Chargebacks

A request for a receipt or Pagaré de Venta is intended to obtain evidence of a Transaction. A Chargeback is a Transaction disputed by the Cardholder or Issuer. In both cases, the Merchant's ability to respond depends on whether the documentation exists, is legible and complete, and can be clearly linked to the requested transaction.

8.1 Responding to a Receipt Request

The response to a Receipt Request must be prompt and orderly. The objective is to locate the correct evidence, verify that it corresponds to the requested Transaction, and submit it through the designated channel without altering its content. For these purposes, the Merchant must:

- Immediately identify the requested Transaction using the date, amount, merchant number, Authorization, and reference.
- Locate the receipt or equivalent evidence.
- Confirm that the receipt is legible and that the amount and date match.
- Submit the documentation through the operational channel designated by Getnet.
- Retain proof of submission and a copy of the documentation submitted.

8.2 Responding to Chargebacks

Responding to a Chargeback requires analyzing the reason for the dispute and preparing a coherent documentary response. Merely accumulating documents is not sufficient; the evidence must consistently explain the sale, Authorization, delivery, refund, or provision of services, as applicable.

To respond to a Chargeback, the Merchant must:

- Read the notice or request to identify the reason, operational deadline, and requested evidence.
- Gather supporting documents relating to the sale, delivery, service, refund, or communications with the Customer.
- Confirm that the evidence is consistent and legible.
- Submit the documentation through the designated channel.
- Internally record the case for follow-up and operational learning.

8.3 Common Reasons for Claims

Claims may arise from differences between what the Customer recognizes, what the Merchant documented, and what actually occurred during the transaction. Identifying the most common reasons helps strengthen controls, improve evidence retention, and reduce Chargeback risk.

Common reasons include:



- The Customer does not recognize the Transaction.
- The Customer claims that the goods were not delivered or the services were not provided.
- The Customer questions the quality or characteristics of the good or service.
- A duplicate charge exists.
- The transaction was processed after a decline or without sufficient evidence.
- The requested documentation could not be located or is illegible.

9. Fraud Prevention

Fraud prevention requires combining system validations, personnel review, documentary evidence, and monitoring of unusual patterns. The objective is to identify potentially fraudulent Transactions before goods are delivered or services are provided.

9.1 E-Commerce Red Flags

In e-commerce transactions, the Merchant must pay particular attention to purchase patterns, contact details, delivery addresses, and transaction patterns that depart from the merchant's ordinary profile. The presence of a red flag does not necessarily mean that a transaction is fraudulent; however, it should prompt additional review before goods are released for delivery or services are provided.

The most relevant red flags include:

- Orders with quantities or amounts that are unusually large relative to the merchant's typical pattern.
- Multiple orders using different Cards but the same user, email address, physical address, or IP address.
- Orders using Cards with sequential numbers or anomalous patterns.
- Deliveries requested to post office boxes or unusual addresses.
- Requests to deliver goods to carriers or other third parties without a clear justification.
- Purchases of easily resold products in unusual volumes.
- Multiple Transactions within a short period or at unusual times.
- Material inconsistencies among billing information, delivery information, user details, and method of contact.

When one or more red flags are identified, the Merchant must apply additional validations, retain evidence of the review performed, and refrain from releasing goods for delivery or providing services if there is insufficient information to confirm the legitimacy of the transaction.

9.2 Recommended Checks Before Delivery

Before releasing goods for delivery or providing services in e-commerce transactions, the Merchant must verify that the transaction information is consistent and reasonable in light of the merchant's usual pattern. These checks help identify potential inconsistencies before delivery is completed and preserve sufficient evidence in the event of claims or Chargebacks..

For these purposes, the Merchant must:

- Confirm that the name, telephone number, email address, delivery address, billing address, and purchase pattern are consistent with one another.
- Apply additional validations when the transaction is unusual because of its amount, frequency, timing, origin, destination, or order characteristics.
- Review the 3D Secure authentication result or the results from available risk tools when they are enabled for the applicable channel.
- Retain evidence of communications with the Customer when necessary to confirm the transaction.
- Document delivery through an acknowledgment of receipt, shipping record, proof of delivery, or equivalent evidence, where possible.
- If the review identifies material inconsistencies, the Merchant must examine the transaction in greater detail before releasing the product for delivery or beginning to provide the service.

9.3 Internal Fraud Prevention

The Merchant must implement internal controls to reduce the risk of misuse of information, access credentials, systems, or sensitive operational functions. These controls must make it possible to identify who performs each transaction, limit access based on personnel responsibilities, and detect activity that departs from the merchant's ordinary pattern.

For these purposes, the Merchant must:

- Limit access to Cardholder information to personnel who need it to perform their duties.
- Restrict sensitive transactions, such as refunds, adjustments, cancellations, or modifications, to expressly authorized personnel.
- Monitor access events, modifications, refunds, adjustments, and transactions that depart from the merchant's usual pattern.
- Do not store sensitive Card data in files, spreadsheets, emails, internal notes, or any other unauthorized medium.
- Train personnel on the proper handling of information, use of credentials, fraud indicators, and escalation procedures.

10. Operational Prevention of Money Laundering

This Manual addresses prevention solely from an operational perspective and is limited to red flags and conduct that must be escalated internally. Specific legal and contractual obligations are set forth in the Contrato de Afiliación.

10.1 Operational Red Flags

The Merchant must be alert to transactions that do not correspond to its ordinary activities, involve unauthorized third parties, or appear not to reflect an actual sale of goods or services. These situations may represent misuse of the merchant account and must be reviewed before processing or proceeding with the transaction.

The main red flags include:

- Processing Transactions on behalf of a third party or a business other than the one disclosed.
- Allowing another business to use the merchant account to charge for its own sales.
- Processing transactions that do not correspond to the Merchant's line of business, activities, or operating profile.
- Processing transactions with amounts, frequencies, volumes, or characteristics that do not correspond to the merchant's ordinary activity.
- Receiving proposals from third parties to process payments in exchange for a fee, commission, or benefit.
- Processing transactions that appear intended to refinance debts, obtain cash, move funds, or simulate sales without an actual transaction involving goods or services.

When any of these red flags is identified, the Merchant must refrain from processing the transaction until it has confirmed that the transaction reflects a legitimate, documented sale within its authorized line of business.

10.2 Recommended Actions When Suspicious Activity Is Identified

When the Merchant identifies an unusual transaction, a proposal to process transactions on behalf of third parties, or any situation that does not correspond to a legitimate and documented sale, it must act cautiously and escalate the matter through the appropriate channels. The objective is to prevent misuse of the merchant account, preserve available evidence, and reduce operational risk.



For these purposes, the Merchant must:

- Refrain from processing suspicious transactions when there is no legitimate, actual, and documented sale.
- Escalate the situation internally to the department or channel designated by Getnet.
- Preserve the available evidence without altering, deleting, or otherwise modifying it.
- Reject instructions from third parties seeking to simulate sales, process unrelated transactions, or misrepresent the actual source of funds.
- Train personnel to identify and escalate proposals to process transactions on behalf of third parties or attempts to misuse the merchant account.

If the Transaction cannot be supported as an actual, documented sale within the Merchant's authorized line of business, it must not be processed.

11. Special Services and Modules

Special services and modules are addressed in this Manual solely from an operational perspective. Their commercial terms, specific configurations, costs, cancellations, annexes, and contractual effects are governed by the Contrato de Afiliación and the applicable documents. The inclusion of a service in this section does not mean that all Merchants are authorized to use it.

Service / Module	Treatment in this Manual
DCC	Retain operational instructions for obtaining Cardholder consent when required by the flow. Do not include costs or contractual terms.
MOTO / Telephone Sales	Retain data capture, evidence, and validation controls for Card-Not-Present transactions.
Recurring Charges	Retain documentary controls for Authorization, supporting evidence, and operational cancellation procedures if included in the source documents.
Cashback	Include only the operational flow and clear identification of the purchase amount and cash withdrawal amount when enabled. Do not include commissions.
MSI (Meses sin intereses / Interest-Free Installments)	Include instructions for selecting the installment period and validating the promotion when enabled. Do not include rates or contractual minimum amounts.
Get Link & Pay	Retain the operational description of generating and sending payment links when the product is enabled.
Get Commerce	Retain the operational description of gateway integration and security modules. Do not include any Chargeback guarantee or commissions.
CoDi	Include only an operational reference to enablement and reconciliation if the service is contracted.

12. Additional Information

The Merchant must consult the current applicable sources for operating rules, security standards, Payment Network guidelines, and product- or channel-specific terms. This section is a general reference only and does not replace the current versions of those sources or modify the provisions of the Contrato de Afiliación, its annexes, or applicable communications.



Relevant reference sources include:

- Payment Networks: Visa, MasterCard, American Express, and any others applicable to the enabled Payment Instrument.
- Security standards: PCI DSS and other security programs associated with the Payment Networks.
- Brand operating guides: including the Guía Operativa del Comerciante American Express (American Express Merchant Operating Guide), where applicable.
- Contrato de Afiliación and current annexes: for legal, commercial, economic, operational, or liability terms.
- Getnet support channels: those contractually designated or communicated to the Merchant for assistance, support, or inquiries.

Appendix A. Operational Glossary

Term	Operational Definition
Acquirer (Adquirente)	Getnet México Servicios de Adquirencia, S.A. de C.V., acting in its capacity as Acquirer.
Merchant (Afiliado)	An individual or legal entity that accepts payments through Payment Instruments within the Programa de Afiliación.
Authorization	The Issuer's response approving, declining, or referring a Transaction.
Authorization Code	A code generated when the Issuer authorizes a Transaction.
Chargeback	A Transaction disputed by the Cardholder or Issuer.
CVV2/CVC2	A security code used in Card-Not-Present Transactions; it must not be retained after Authorization.
POS Device (Dispositivo TPV)	A terminal, software, or point-of-sale device used to process Transactions.
Issuer (Emisor)	The institution or entity that issues the Card to the Cardholder.
Payment Instrument (Medio de Pago)	A Card, device, or mechanism used to process a Transaction.
Pagaré de Venta / Receipt	A physical or electronic record documenting a Transaction.
Card-Not-Present	A transaction conducted without the physical presence of the Card, such as e-commerce, MOTO, a payment link, or recurring charges.
Card-Present	A transaction in which the Card or Payment Instrument is physically present or used in person.
Online Store (Tienda Virtual)	A website, page, or digital flow through which the Cardholder makes a purchase over the Internet.
3D Secure	An Issuer authentication service for Card-Not-Present Transactions.

