PayLink Merchant Services

Company Manual

Merchant Services and Consultancy Services

Version 1.0 | November 10, 2026

This manual sets out how PayLink personnel sell, support and deliver merchant services and consultancy services, protect information, and report problems. It applies to employees and to subcontractors, sales advisors, referral representatives and approved external personnel to the extent relevant to their assigned work and written agreements.

PayLink's business operations are primarily based in Canada, with operations in North America and Europe. The company serves Canadian and U.S. markets and has identified December 1, 2026 as the planned start of service availability across the 27 European Union member states through a fintech partner. Individual services and countries are subject to the approval and availability rules in this manual.

Document control

Item	Document details
Policy owner	Executive Management
Operational owners	Operations, Privacy and Compliance, Information Security, and People Operations. Executive Management must assign named owners and backups.
Audience	Employees and authorized subcontractors and representatives
Status and distribution	Final copy. Executive Management sets the effective date, records approval and authorizes internal distribution.
Review cycle	At least annually after adoption and whenever services, partners, legal obligations or major risks change.

Contents

Page	Section
2	Governance and authority
3	Conduct and sales practices
4	Merchant onboarding and eligibility
5	Payments equipment and support
6	Consultancy services and deliverables
7	Confidential information and payment data
8	Privacy records and cross border transfers
9	Systems vendors and workforce access
10	Incidents complaints and continuity
11	Market approval and launch checklist
12	Field guide and acknowledgment
13	Authorities and operating references

SECTION 01

Governance and Authority

Scope of services

PayLink's scope includes introducing and supporting approved merchant payment processing arrangements, card acceptance and point of sale equipment, online payments, payment links, virtual terminals, recurring billing, invoicing and billing automation, and related implementation advice. [10] Approved partners may offer supported digital asset or stablecoin payment options. Consultancy may include payment workflow reviews, cost analysis, terminal selection, implementation planning and training. The approved service catalogue and signed agreement determine what may be offered to each client.

For each engagement, identify the PayLink contracting entity, the merchant, the processor or acquirer, the equipment or software provider, and any other service partner. Explain who is responsible for approval, transaction processing, settlement, chargebacks and technical support. Use the contracting entity and service description approved for that market. Never imply that a partner's registration, authorization or certifications belong to PayLink.

Responsibilities and approvals

Role	Accountability
Executive Management	Approves policies, markets, services, risk appetite, authority limits and material exceptions. Assigns accountable owners and deputies.
Privacy and Compliance	Determines applicable requirements with counsel, reviews sensitive data and market decisions, owns privacy response and coordinates regulator and partner notices.
Operations and Finance	Maintain partner workflows, merchant records, pricing approvals, complaints and reconciliations. Apply independent verification to sensitive account changes.
Information Security	Maintains access, devices, approved systems, logging and incident containment. Reviews security risks before new tools and integrations go live.
People Operations and contract owners	Manage training, acknowledgments, worker classification review, contractual requirements and offboarding.
All personnel	Work within authority, protect information, record decisions and report concerns promptly.

Authority to commit PayLink

Only a designated signer may execute agreements or change contractual terms. Staff may quote within written delegated limits using approved materials. Seek prior written approval for exceptions, new vendors, public announcements, regulatory communications, new markets or changes to the way funds or data flow. Record the decision, approver, rationale, limits and expiry. No exception overrides law, card network rules or applicable partner obligations.

Applicable laws and binding obligations govern. If instructions conflict, pause the affected work and escalate to Privacy and Compliance or Executive Management. This manual supplements signed terms, and acknowledgment does not amend an agreement or waive statutory rights.

SECTION 02

Conduct and Sales Practices

Professional standards

Treat merchants, colleagues and partners fairly. Harassment, discrimination, retaliation, bribery, kickbacks and deceptive practices are prohibited. Disclose conflicts promptly, including ownership interests, family connections, gifts and personal payments from suppliers or merchants. Recuse yourself pending written direction. Record business courtesies under the approved gifts procedure. Obtain approval before providing anything of value involving a public official. Do not collude on pricing, divide markets or misuse competitors' confidential material.

Maintain truthful records of sales, expenses, commissions and referral activity. Use written commission terms and record qualifying activity accurately. Never create artificial transactions, duplicate referrals, conceal cancellations or direct payments to an unapproved account. Raise pay or commission disputes through the designated manager or contract owner.

Outbound calls and electronic outreach

Use an approved campaign, list source, script and company communication channel. Identify yourself and PayLink accurately. Check local rules for the target country and region, calling hours and time zones, dialing and recording technology, consent and suppression lists before outreach. Business contacts can still be subject to telemarketing and marketing rules. Never assume a public phone number or business email authorizes unrestricted outreach. Log the basis for contact, honor opt-outs, and synchronize suppression lists. Use approved identification and unsubscribe language in electronic messages. Do not record calls without an approved process and any required notices or consent. [8]

Quotes and marketing

Explain the expected total cost and material terms in writing. Where relevant, show transaction rates, fixed fees, equipment cost or financing, monthly charges, renewals, early termination, settlement timing, reserves, chargebacks and currency conversion. Identify which charges are set by the partner and which are PayLink's. Describe illustrative savings with the underlying assumptions and a comparable period. Use a documented review before stating that PayLink will match or beat a competitor's pricing or provide a free terminal, and clearly show conditions.

Use approved copy for partner claims, product availability, endorsements and testimonials. Disclose material referral relationships and compensation where required and as directed. Never promise approvals, waived reserves, guaranteed savings, fraud immunity, reversible digital asset transfers or fixed settlement timing. Publish partner logos and merchant testimonials only with documented permission.

Reporting concerns

Report suspected misconduct to your lead, Privacy and Compliance, or directly to Executive Management if your usual contact is implicated. PayLink prohibits retaliation for a good faith report or participation in a review. The company will limit disclosure to those who need it and investigate fairly. This policy does not limit protected reporting to authorities or other legal rights.

SECTION 03

Merchant Onboarding and Eligibility

Application workflow

1. Qualify the opportunity. Record the merchant's legal name, operating name, website, locations, activities, sales channels, expected volume and currencies. Confirm the service, geography and intended use against the approved partner catalogue.
2. Disclose terms and responsibilities. Provide the approved proposal, application notice and relevant partner documentation. Explain that underwriting, pricing exceptions, funding, holds and reserves remain subject to the appropriate party's approval.
3. Collect minimum information through the approved secure application workflow. Where required, direct identity, ownership and bank verification documents to the authorized processor or restricted intake portal. Keep only the reference number and information needed for support in the CRM.
4. Escalate unusual facts. Flag unclear beneficial ownership, inconsistent identities or bank details, suspicious volume estimates, unusual geographies, restricted products, or attempts to use another entity's account. Do not alter details, split submissions or suggest a different merchant category to gain approval.
5. Wait for documented approval and signed terms. Record the partner's decision, any restrictions, pricing and merchant identifier in the approved system. Operations confirms provisioning, funding destination verification and handoff to the merchant.
6. Monitor changes. Report changes in ownership, bank information, products, location, currency or transaction model before relying on existing approval. Route disputes, risk flags, reserve questions and termination requests through the partner workflow.

Restricted and higher risk sectors

Use the current restrictions for the applicable partner, market and service. Escalate regulated products, online pharmacies, high chargeback models, gambling, adult services, financial services and digital assets before quoting or submitting. Any enhanced due diligence, sanctions screening or monitoring must follow a documented allocation of duties. PayLink personnel must not bypass controls, open substitute accounts, or advise a merchant to obscure what it sells. Never disclose a suspected regulatory report or investigation without authorization.

Bank detail changes and verification

Verify sensitive account changes through an approved channel using a contact already on file. Obtain separate review from an authorized second person and record evidence before submission. Do not use a callback number supplied only in the change request. If instructions conflict or independent verification fails, suspend the change and escalate.

Handling applications

Business contact records, owner information, signed agreements and statements may contain personal or confidential data. Send secure links instead of requesting attachments. Keep ownership records and identity documents out of sales notes and shared drives. For a declined or abandoned application, apply the retention schedule and avoid giving reasons beyond the approved partner communication.

SECTION 04

Payments Equipment and Support

Keep payments in approved systems

Use only approved terminal models, configurations, integrations and payment channels for the merchant and market. For e-commerce, use the partner-approved checkout or hosted payment link. For phone orders, use only a separately authorized workflow with safeguards for call recording and card entry. PayLink personnel must never take card details on behalf of a merchant through general email, messaging, CRM, recorded calls or paper forms.

For recurring billing, use the approved provider's stored credential or token workflow. Document the customer's authorization, amount or calculation, billing schedule, cancellation terms and any required notices. Follow the provider's procedures for failed payments and cancellations. [1–2]

Terminal installation and servicing

Match device model, serial number, merchant location and merchant account to the approved deployment record. Verify packaging and device integrity. Use approved installers and partner provisioning. For handoff, verify connectivity and permissions and use a partner-approved test method. Show the merchant how to inspect devices and report swaps or tampering. Log training and merchant acceptance. Keep a current terminal inventory and record moves, replacements and returns.

If a device appears tampered with, has an unexpected serial number, or was changed by an unknown person, stop use of that device and report immediately. Do not dismantle or reset it without direction. Replace or decommission devices through the approved partner process. Never take payment credentials or secret keys off-site for troubleshooting.

Settlement refunds and disputes

Where PayLink acts as a referral or support provider, the designated processor or acquirer handles settlement and transaction decisions. PayLink personnel must not take custody of merchant or cardholder funds or route refunds, reserves or settlements through PayLink or a personal account. Any proposed change to this model requires prior legal and executive approval. Explain settlement cutoffs, holidays, reserves and possible holds using the applicable agreement. Staff may assist with reconciliation using approved records and masked transaction references.

The merchant or designated provider approves refunds and executes them under its procedures. Use the original payment method where required. Escalate off-channel refund requests, unusual split payments or suspected fraud. For disputes, capture the case number, deadline and approved evidence list. Submit evidence through the authorized portal. Do not send full card details or promise a result. [1–2]

Stablecoin and cryptocurrency

Discuss digital asset payment options only for approved merchant types and jurisdictions using approved disclosures. Explain the provider's role, conversion, settlement currency, fees and refund process. Never receive funds in a personal or PayLink wallet, request seed phrases or private keys, direct transfers to unverified addresses or represent a stablecoin as risk free. Treat any displayed reference price as informational unless an approved provider expressly offers a binding quote. Route unexpected wallet instructions, suspicious activity or address changes to Privacy and Compliance. [7]

SECTION 05

Consultancy Services and Deliverables

Engagement acceptance

Before accepting work, check client identity, competence, capacity, conflicts, referral arrangements and the effect of any partner relationship on the advice. Decline or obtain documented mitigation for conflicts. Identify what information is needed and who may access it. Sign a statement of work or approved engagement letter before substantive work begins. [9]

Agreement topic	Record before starting
Scope and deliverables	Objectives, included services, exclusions, acceptance criteria and decision owners
Commercial terms	Fees, taxes, expenses, payment schedule, referral compensation and written change process
Information handling	Authorized systems and recipients, data roles, location and transfers, retention, return and deletion
Rights and restrictions	Ownership or licensing, third-party material, permitted reliance, confidentiality and approved publicity
Delivery and exit	Dependencies, milestones, subcontractors, handoff, complaints and termination procedure

Analysis and recommendations

Separate client-provided facts, verified evidence and assumptions. In cost comparisons, show the time period, volume, card mix, processor charges, hardware and other recurring charges. Explain any assumptions or missing statements that could change the outcome. Compare available options fairly and disclose compensation or incentives that might affect a recommendation. Ask a qualified colleague to review material estimates, recommendations and deliverables before release.

Provide advice within the agreed scope and the team’s competence. Refer matters that require legal, tax, investment or other regulated advice to qualified advisers. Use approved claims about security or compliance and do not certify a merchant or partner unless authorized and qualified to do so. Never import a client’s confidential material into another client’s work.

Changes and closeout

Log decisions, changes, risks and open actions. Obtain written agreement to material changes in scope, fees, data use or delivery dates before implementation. Deliver the approved final version through the agreed channel, confirm receipt and acceptance, and record unresolved items. Close access, return or securely delete materials as required, and retain only records justified by the schedule or legal hold.

Subcontracted delivery

Obtain written approval before subcontracting. Use qualified providers under written terms covering scope, confidentiality, data instructions, security, incident reporting, approved locations, further subcontracting, return and deletion, and audit or assurance rights as appropriate. PayLink’s engagement owner remains accountable for supervision and final quality.

SECTION 06

Confidential Information and Payment Data

Classify before collecting or sharing

Classification	Examples and handling
Public	Approved website copy and published materials. Only authorized personnel may approve release.
Internal	Training, routine process notes and operational reports. Use approved systems and share with authorized personnel.
Confidential	Merchant agreements, pricing, statements, client work product and personnel records. Restrict to named roles and share through approved access controls.
Restricted	Identity records, bank details, credentials, full card numbers and sensitive incident records. Use only approved restricted workflows. Store only when specifically authorized and required.

Treat unclassified merchant and personal information as confidential or restricted according to its sensitivity. Check the identity and authority of recipients, share only what they need, restrict external links to named users and remove access when the purpose ends. Use encryption in transit and at rest as provided by approved systems. Avoid downloading, printing or forwarding sensitive files. If an approved paper process is necessary, secure the documents and use approved destruction.

Payment card data

PayLink's default process keeps full primary account numbers (PANs) and sensitive authentication data out of PayLink sales, support and consultancy systems. Route card entry to the approved terminal or hosted workflow. Use a token, case reference or last four digits where a transaction identifier is needed. Never ask for a PIN, magnetic stripe or chip equivalent track data, card security code, online banking credentials or one-time code through PayLink channels. Do not retain sensitive authentication data after authorization, even if encrypted. Any proposed cardholder data environment requires a formal PCI scope review, approval and documented safeguards before use. [1]

If a customer sends card data to an unauthorized channel, stop processing the message. Do not forward, quote, screenshot, export or copy it into a ticket. Alert Information Security and Privacy and Compliance immediately using only safe identifiers. Follow their containment and evidence instructions, then redirect the customer to the approved payment channel.

Confidentiality in daily work

Use information only for an authorized business purpose. Never use a merchant list, price schedule, client document or application for personal benefit, another client or a new employer. Avoid confidential calls in shared spaces and protect screens. Check recipients, permissions and attachments before sending. Use synthetic or properly de-identified data for demonstrations. Do not upload company or client information to unapproved AI tools or browser extensions. Confidentiality continues after the engagement, subject to law and signed terms. This does not restrict lawful protected disclosures.

SECTION 07

Privacy Records and Cross Border Transfers

Collection and individual rights

Document the purpose and legal basis or consent requirement before collecting personal information. Give the approved notice at collection, including meaningful information about purpose, disclosures, retention and privacy contacts as applicable. Collect only necessary fields. Use information for the original or otherwise lawfully authorized purpose. Separate application processing from marketing. Keep contact, recruitment and merchant files in their designated systems.

Route requests for access, correction, deletion, objection, restriction, portability or consent withdrawal to Privacy and Compliance immediately. Log receipt, verify identity proportionately, preserve relevant records and apply the appropriate deadline and exceptions. Do not promise deletion where legal retention, contract obligations or a hold require preservation. Review legal demands for authority and scope before disclosure, unless law requires immediate action.

For healthcare merchants, use invoice or transaction references for payments and consultancy. Keep diagnoses, treatment details and patient records out of CRM notes, payment descriptors and training material. Any proposed service involving patient information requires a separate legal and security assessment and approved agreement before intake.

Data roles and international access

Map what PayLink and each partner collect, where data is stored or accessed, and who decides the purpose and means of use. Document whether each organization is an independent controller, joint controller or processor where those concepts apply. Put required terms in writing, including GDPR Article 28 terms where PayLink or a vendor acts as a processor. Update notices, records of processing and impact assessments where required. Treat remote access from another country as a transfer risk requiring review.

For EU data, verify the legal basis and applicable GDPR Chapter V mechanism before a restricted transfer or onward transfer. The EU adequacy finding for Canada applies to commercial organizations covered by PIPEDA within its scope. Where adequacy does not apply, assess suitable safeguards such as standard contractual clauses, transfer risks and supplementary measures. Obtain written approval before enabling a new hosting region, remote work location or subprocessor. Review provincial requirements separately, including Québec assessments where applicable. [3–5]

Retention and disposal

Privacy and Compliance maintains a schedule for each record class, its system owner, trigger, retention period, lawful basis and destruction method. Cover leads, applications, contracts, transaction support, complaints, personnel files and incident records. Avoid duplicate copies. Suspend deletion on receipt of a legal hold, dispute or preservation instruction. Resume scheduled disposal only after written release. Record destruction or return and address backup expiry and restoration safeguards. Where PIPEDA applies, retain records of every breach of security safeguards for at least 24 months after determining the breach occurred. [3]

SECTION 08

Systems Vendors and Workforce Access

Secure systems and devices

Use assigned accounts, multifactor authentication and unique credentials in the approved password manager. Never share credentials or MFA codes. Use approved devices with encryption, supported software, automatic locking, current patches and endpoint controls. Personal devices require written authorization and company controls. Use approved connections for remote work. Report phishing, lost devices, unexpected login prompts and unsafe browser extensions promptly.

Keep restricted files in the designated system. Use company-managed file sharing and restrict export permissions. Review data permissions for forms, integrations and dashboards before launch. Test with synthetic records and check routing, access, and retention. Do not send restricted application content in notification emails. Use a case reference and a secure link instead. Keep credentials and live tokens out of code, screenshots, documents and ticket systems.

Access lifecycle and monitoring

Require manager approval and system owner review before granting access. Use the least access needed, set expiry for temporary accounts, and log privileged activity. Review access on a documented schedule and on role change. Remove access promptly on departure or suspension, revoke tokens and sessions, recover equipment, rotate exposed shared secrets, transfer business records and obtain a return or deletion attestation where appropriate.

Vendor and partner diligence

Before activation, verify the vendor’s identity, authority, security posture, incident terms, data locations, subprocessors and deletion capabilities. For payment providers, obtain applicable PCI compliance evidence, verify covered services and maintain a responsibility matrix. Review service levels, complaints, continuity, exit and data portability. Reassess material changes and review high-risk providers regularly. Never assume a provider’s compliance covers PayLink’s activities. [1]

Workforce standards

Complete confidentiality, privacy, payment handling, ethics and role-specific training before unsupervised access, annually thereafter, and after material changes. Keep completion and acknowledgment records. Managers document exceptions, corrective action and monitoring. Employees follow applicable workplace policies and have access to approved reporting channels. Subcontractors follow signed requirements and must ensure their authorized personnel do the same.

People Operations and counsel review worker classification, location and applicable compensation obligations before recruitment and contracting. A commission arrangement or contract label alone does not determine legal status. Written terms must address commissions, expenses, payment timing and responsibilities for the applicable jurisdiction. Only authorized personnel may promise employment terms.

SECTION 09

Incidents Complaints and Continuity

Respond immediately

1. Report the suspected incident immediately to Information Security and Privacy and Compliance using the approved emergency channel. If unavailable, escalate to Executive Management. Use an approved out-of-band channel if company systems may be compromised.
2. Stop the affected activity if safe. Do not erase records, factory reset devices, delete messages or contact suspected attackers. Avoid forwarding restricted evidence. Preserve relevant timestamps, device identifiers, case numbers and other safe facts.
3. The response lead opens a restricted incident record, assigns owners, records discovery and awareness times with time zones, assesses scope and risk, and preserves evidence. Operations coordinates containment with partners and verifies integrity before restoring service.
4. Privacy and Compliance maps legal and contractual clocks and coordinates partner, insurer, regulator and individual notices. Only authorized spokespeople issue notices. Escalate immediately even when details are incomplete or a deadline appears uncertain.

Notification decision guide

Framework	Decision for the authorized lead
PIPEDA where applicable	Report to the federal Privacy Commissioner and notify affected individuals as soon as feasible where there is a real risk of significant harm. Consider notice to organizations able to reduce harm as required. Record every breach. [3]
GDPR where applicable	A processor notifies its controller without undue delay. A controller reports to the competent authority without undue delay and, where feasible, within 72 hours of awareness unless the breach is unlikely to pose a risk. Notify individuals without undue delay where high risk applies, subject to exceptions. Document all breaches. [4]
Other duties	Check provincial, U.S. state and sector rules, card network, acquirer and contractual deadlines. Use the applicable clock for each duty. A shorter partner deadline may apply. [2, 5, 7]

Merchant complaints and outages

Open a case, acknowledge it under the applicable service commitment and confirm the facts. Route funding, chargeback, billing and cancellation disputes to the authorized decision-maker. Keep the merchant informed through approved channels. Record the resolution and corrective action. For outages, use only partner-approved fallback methods. Never improvise a manual card record or route payments to an alternate account. Test backups and continuity procedures, and review incidents for corrective actions, owners and completion dates.

SECTION 10

Market Approval and Launch Checklist

Service and jurisdiction assessment

Market	Review before approving a service
Canada	Confirm federal and provincial privacy scope, marketing and workforce rules. Map any activities under the Retail Payment Activities Act and assess FINTRAC money services business obligations, including where payment or virtual currency functions are proposed. [3, 5, 6, 8]
United States	Assess relevant state privacy and breach laws, federal and state outreach rules, FTC Safeguards Rule applicability and any money transmission or other financial regulatory requirements for the actual activity. Confirm the partner's applicable approvals and permitted scope. [7–8]
European Union	Map GDPR, local direct marketing and worker rules. Confirm the contracting partner, authorization and country coverage for the services being offered. Review payment services and digital asset rules where applicable, including PSD2 and MiCA and local implementation or transitions. [4, 7]

Management release checklist

- Identify legal entities, contracting parties, countries, merchant segments and services. Confirm insurance, responsibility for support, settlements and disputes, and authorized signers.
- Map actual flows of funds and data. Document whether PayLink introduces, advises, transmits instructions, processes data, controls funds, or provides another regulated function. Record required registrations or authorizations, status and the responsible party. Reassess when functions change.
- Confirm the EU fintech agreement, country and product schedule, and partner authorization where applicable before personnel make launch commitments. Approve country-specific disclosures, languages, currencies, partner terms and sales scripts.
- Approve processor agreements, service catalogue, authority limits, pricing, high-risk sector rules, privacy notices, retention schedule, transfers and security controls. Confirm contact and reporting paths with partners.
- Populate and test the internal contact directory. Assign primary and backup contacts for merchant operations, privacy, security, urgent incidents, employment, partner support and protected reporting.
- Test the application and support workflows with synthetic records. Confirm intake permissions, notification routing, rights request handling, device deployment, access removal and response to a mock incident.
- Obtain Executive Management sign-off after review by counsel and operational owners. Publish the controlled copy, retire older copies and document staff and subcontractor training.

Review cadence

Review this manual at least annually and after significant incidents, service or partner changes, market launches or legal changes. Track overdue training, access removal, incidents, complaints and unresolved partner risks. Assign an owner and due date to each corrective action and review completion.

SECTION 11

Field Guide and Acknowledgment

What to do in common situations

Situation	Required response
Merchant emails a bank statement or ID	Do not forward it. Ask the merchant to use the approved upload portal. Report the off-channel receipt through the applicable privacy procedure and follow the retention or disposal instructions.
Merchant sends a card number by chat	Stop. Do not copy or repeat it. Report immediately using a safe case reference and redirect the merchant to the approved payment channel.
Someone requests a last-minute payout change	Pause the change. Verify through the independently known contact and obtain a second approval before submission.
A merchant asks for a guarantee on approval or price	Use the approved quote and disclose conditions. Refer approval and any exception to the authorized owner.
A consultancy client wants to send patient records	Pause the intake. Use nonclinical information where possible and refer any proposed access to Privacy and Compliance.
A prospect asks for service in a new country	Check the approved country and product schedule before making any commitment. Escalate unavailable or unclear cases.
A partner sends new wallet instructions	Do not initiate a transfer. Verify via the approved independent channel and escalate the change.

Reporting directory to complete before issue

Function	Primary and backup contact
Privacy requests and incidents	To be designated by Executive Management
Security and urgent out-of-hours response	To be designated by Executive Management
Merchant operations and partner support	To be designated by Executive Management
People Operations and protected reporting	To be designated by Executive Management

Personnel acknowledgment

I acknowledge receipt of the approved version of this manual. I understand the requirements applicable to my role, including approved systems, confidentiality, payment data handling and reporting. I will seek direction when authority or procedures are unclear and complete required training. This acknowledgment records receipt and does not waive any rights or change my signed agreement.

Name _____ Role or company _____

Signature _____ Date _____ Version _____

APPENDIX

Authorities and Operating References

The following primary sources informed this manual. Card network and partner requirements depend on the applicable agreements and the services in scope. Privacy and Compliance should maintain a current register by service, entity and jurisdiction.

Payment acceptance and consultancy

[1] PCI Security Standards Council. PCI DSS v4.0.1 and the Council's merchant guidance. Use these for cardholder data scope, sensitive authentication data, service provider responsibilities and secure payment practices.
PCI SSC Document Library
[2] Visa and Mastercard. Network rules and published transaction processing standards. Implement through the applicable acquirer and processor agreements.
Visa Rules
Mastercard Rules
[9] International Council of Management Consulting Institutes. Professional conduct and ISO 20700 implementation resources inform engagement acceptance, conflicts, confidentiality and delivery.
ICMCI Code of Conduct
ICMCI ISO 20700 resource
[10] PayLink's public service descriptions establish the merchant service categories used in this manual. Internal approval determines service availability.
PayLink Merchant Services

Privacy and market obligations

[3] Federal Canadian privacy law and breach recordkeeping.
PIPEDA
Breach of Security Safeguards Regulations
[4] EU privacy law. See GDPR Articles 3, 5–6, 12–22, 28, 32–35 and 44–49, and the European Commission adequacy list.
GDPR
European Commission adequacy decisions
[5] Provincial privacy law examples.
British Columbia PIPA
Québec private sector privacy act
[6] Canadian payment supervision and financial crime registration guidance.
Bank of Canada retail payments supervision
FINTRAC money services businesses
[7] U.S. information security guidance for covered financial institutions and EU payment and digital asset rules.
FTC Safeguards Rule guidance
PSD2
MiCA
[8] Official marketing and outreach guidance.
CRTC anti-spam
CRTC telemarketing
FTC CAN-SPAM guide