RT Merchant Schedules

Edition and scope

Online edition v3.0 | Issued 20 October 2026 | Effective on valid acceptance. These schedules apply through valid acceptance of the v3.0 online Merchant Platform Agreement or a valid later amendment. A is the public description of a separate private order; it contains no merchant pricing. B-K address relevant general obligations; Q, R and S are conditional product schedules.

Acceptance and activation

The platform MSA, private order, provider consent and production approval are separate records. Publication does not create acceptance, amend legacy Byte/DFin or v2.0 agreements, or activate a financial product.

Durable copies

Archive: https://rt.app/legal/merchants/archive/2026-10-20/ | Directory: https://rt.app/legal/merchants/

Contacts

legal@rt.app | support@rt.app | privacy@rt.app | security@rt.app

Schedule A | Commercial Order Form

A.1 Private completion

Schedule A is a private, separately accepted commercial order identifying Merchant, RT entity, MSA edition, selected services, providers, territories, pricing, limits, payout instructions, initial reserve and underwriting conditions. Online MSA acceptance does not accept an unfinished order. This public page is a description only; completed commercial and personal information must not be published.

A.2 Required entries

Complete all identity and notice fields; MSA edition/reference; order ID and version; selected products; provider, program, country and permissions; included/excluded activities; each fee or an explicit not-applicable entry; payout and reserve details; processing limits; conditions; and any exact clause exceptions. State the electronic or signed acceptance route and effective-date rule. Blank pricing or an unselected product does not authorize charges or processing.

A.3 No default from old forms

Historic 10% fees, $0.50 transaction fees, $55 dispute fees, zero reserves, T+5 timing, USDT, Base, excluded-state lists and promises to pay gas do not apply automatically. Each must be agreed for the actual approved program. The selected initial parameters remain subject to the core Agreement's risk, notice and release rules.

A.4 Beneficiary verification

Payout changes require an authenticated instruction and verification. Do not publish or include private keys, seed phrases or bank login credentials. Separate debit mandates and guarantees must meet their own formalities. Schedule A cannot silently waive protective terms or change the contracting company.

A.5 Separate acceptance

A completed order issued as an authorized RT electronic offer takes effect when Merchant affirmatively accepts the exact order and RT confirms and records that acceptance, or a later stated date. A route expressly requiring signatures takes effect only after both authorized signatures or its later stated date. Exceptions to a core protection require express authorized RT acceptance identifying the clause. Retain order bytes/hash and assent evidence separately from signup. Neither route replaces provider acceptance or underwriting.

Schedule B | Definitions and Interpretation

B.1 Agreement and parties

Agreement means the RT online Merchant Platform Agreement accepted under core Section 1.1, applicable schedules identified in Schedule Z, each separately accepted completed Schedule A and valid amendments. RT means only the identified contracting company. Merchant is the business identified at signup and in its order; an owner is personally a party only as a sole proprietor or under a separate valid instrument. Effective Date follows core Section 1.1; each order has its own effective date. End Customer is a purchaser of Merchant's goods or services.

B.2 Services and providers

Services means only software functionality and related support selected and enabled for Merchant. Provider means an independent acquiring, payment, banking, digital-asset, identity or infrastructure provider involved in the approved flow. Provider Terms and Network Rules mean the current applicable agreements, rules and binding instructions for that service. Their application depends on the actual method, country and contractual relationship.

B.3 Transactions and proceeds

Transaction means a genuine approved sale and related payment activity. Authorization means the relevant permission or payment-method approval; it is not a guarantee of final settlement or fulfillment. Settlement means completion of the provider's payment/accounting stage as defined in that program. Payout means the subsequent remittance of eligible proceeds to Merchant's verified destination. A pending, reserved or provisional balance is not necessarily available for withdrawal.

B.4 Disputes and obligations

Chargeback means a reversal or payment dispute under card-network procedures. Return or Reversal means a cancellation, recall, returned payment or other adjustment under the applicable method. Refund means repayment of an amount to a buyer through an approved lawful process. Secured Obligations means Merchant's enforceable payment and performance obligations under this Agreement within the security grant. Fees means charges agreed with RT; Pass-through Amounts means documented third-party charges properly recoverable from Merchant, without double recovery.

B.5 Protective controls

Hold means a temporary restriction on eligible payment or payout activity. Reserve means an identified fixed, rolling, capped or other amount retained within a lawful approved program to secure reasonably evidenced Merchant exposures. Setoff means application of an eligible amount otherwise payable to Merchant against a properly due Merchant obligation. Collateral is limited to Merchant property described in core Section 9; none of these terms by itself establishes custody, title, perfection, priority or an external-wallet control.

B.6 Digital assets and security

Utility NFT means an approved digital token recording or representing specified consumptive rights to Merchant's goods or services; calling it utility does not determine its legal status. Stablecoin means a digital asset designed to track another reference value, without a guarantee it will do so. Wallet means an approved asset address or interface; it may be self-controlled or provided under independent custody terms. Security Incident includes actual or reasonably suspected compromise of credentials, systems, relevant data or transaction integrity. Personal Data has the meaning in the applicable data-protection law. Business Day and the precedence rules are stated in the core Agreement.

B.7 Interpretation

Defined terms include reasonable singular/plural and grammatical variations. A list of examples is not exhaustive. Capitalization is for readability and does not import an old Byte or DFin definition. A statement of intention does not certify legal or technical implementation. The core Agreement controls interpretation and the accepted version record controls incorporation.

Schedule C | Operational Security and Controls

C.1 Proportionate safeguards

Each party must maintain administrative, technical and organizational safeguards appropriate to the data, systems and risks for which it is responsible. Merchant must use unique users, least privilege, multifactor authentication where offered, controlled administrator access, confidential staff/vendor obligations, secure device practices, timely patching and prompt access removal when roles end. Shared support or administrator credentials should not be used to authorize a financial or security change without verification.

C.2 Integration controls

Keep secrets server-side in protected storage; do not place API secrets or private keys in browsers, public repositories, ordinary documents or support chats. Use current supported encrypted transport, verify certificates and webhook signatures, reject invalid/replayed messages and apply idempotency, access restrictions, logging and reconciliation appropriate to the integration. Logs must omit sensitive authentication data and minimize personal information.

C.3 Incidents

Notify security@rt.app without undue delay and no later than 24 hours after awareness of an actual or reasonably suspected incident affecting the Services. Preserve relevant logs and evidence, contain the event, revoke compromised credentials and supply known facts, likely impact and actions taken, followed by updates. Do not delay notice until confirmation or final forensic conclusions. Required notices to providers, regulators and affected individuals remain the responsible party's duty.

C.4 Investigation and recovery

Merchant must cooperate with proportionate RT/provider investigations and network-mandated independent forensics, limit further exposure and verify remediation before restoring unsafe activity. RT may restrict access or payment functionality during response. Costs follow causation, provider requirements, indemnity and mandatory law; a suspected incident is not itself proof of Merchant fault or a license to retain unrelated funds.

C.5 Assurance and limitations

Any evidence RT supplies may be reasonably redacted for security and confidentiality. This schedule makes no assertion that RT currently holds SOC 2, PCI Level 1 or another certification, operates a particular backup frequency, or promises specified recovery/uptime targets. A particular assurance requires current evidence or an express signed commitment. PCI obligations depend on actual data handling and provider requirements; hosted fields do not automatically prove any particular SAQ eligibility.

C.6 Data and access review

Maintain appropriate access, backup, recovery and retention procedures for systems under each party's control. Review privileged access periodically and after personnel changes. Do not add customer or staff identifiers to public-chain metadata; necessary public wallet/transaction references require a lawful basis, minimization and clear disclosures. Account-owner verification, recovery channels and signing authority are separate controls; a logged-in mailbox or DocuSign profile name is not proof of legal authority.

Schedule D | Provider Roles, Funds Flows and Risk Controls

D.1 Approved configuration

Before production use identify the actual provider/program, Merchant legal entity, charge model, collection recipient, conversion provider if any, asset/network, payout beneficiary, fee flow, reserve holder and RT permissions in Schedule A or the authenticated activation record. RT supplies the enabled software and transmits permitted instructions. A card-funded purchase, direct card acceptance, bank payment and direct digital-asset transfer must be represented as their actual distinct flows.

D.2 Payment and discharge

Only an authorized collection recipient for the approved flow receives payment for Merchant. Receipt by that recipient discharges the buyer for the amount received, subject to applicable reversals and refunds; Merchant must not collect it again. A limited collection-agency appointment applies only to the role actually performed and only where supported by applicable law and the provider program. This schedule gives no blanket agent-of-payee, payment-processor or money-transmission exemption opinion.

D.3 Provider custody and permissions

The provider's terms govern accounts, custody, regulated processing, conversion and settlement it supplies. The actual structure determines legal title, commingling, segregation, insurance and control. RT does not promise that every reserve is held in a segregated merchant-titled account, that a wallet is self-custodial, or that any balance is deposit-insured. RT's instruction rights are limited to the provider permissions and lawful authority actually granted.

D.4 Payouts

Eligible cleared proceeds are paid to the verified Merchant destination under Schedule A, net of agreed fees, valid adjustments and justified reserves. Provider cut-offs, holidays, incomplete verification, compliance reviews, disputes, returns and technical conditions may delay a payout. A displayed amount or schedule estimate is not a guarantee of available funds. RT must account for deductions and may not treat a hold alone as revenue.

D.5 Reserves and review

Core Sections 8-9 govern protective measures, including reserves up to 100% of affected eligible proceeds where reasonably necessary, prompt notice where lawful, documented exposure calculations, review at least every 30 days, partial release when justified and a continuing basis for any extension. No automatic 180-day release is promised where a real exposure or binding restriction continues. A restriction does not transfer ownership to RT or authorize indefinite retention without justification.

D.6 Setoff and security

Recovery must be for a properly payable obligation from eligible Merchant assets within the lawful mandate, with accounting and no double recovery. The security grant is limited to the Merchant's described settlement/reserve rights and proceeds; perfection, priority and enforcement require applicable legal steps. A bank debit, personal guarantee, cross-company recovery or new custody arrangement needs its own valid basis. RT cannot recall or freeze an external wallet merely by writing that power into a contract.

D.7 Regulatory or provider change

RT may restrict or discontinue a flow that loses legal or provider support and require a compliant reconfiguration before further activity. A substitute provider requires appropriate diligence, disclosures, agreements and permissions. Mandatory law and lawful third-party restrictions prevail; Merchant cannot direct RT to evade them.

Schedule E | Payment Acceptance and Network Requirements

E.1 Applicable methods

Accept only the payment methods and transaction types explicitly approved for the account, sales channel and territory. Comply with current method, acquirer and network rules and binding provider instructions. Keep descriptors, merchant category, URLs and beneficiary details accurate. Approval for one method is not permission for another or for an unapproved regulated product.

E.2 Authorization and fraud controls

Obtain the payer's required authorization and method approval before capture. Use mandated authentication, risk and verification controls. Do not split charges, conceal a decline, bypass a risk block, misstate a transaction or retry beyond provider rules. For ambiguous outcomes, check authoritative status and use idempotency rather than charging again. Authorization, 3-D Secure or token minting does not guarantee settlement or defeat every dispute.

E.3 PCI and data handling

Use provider-hosted capture or an expressly approved integration. Maintain the validation and safeguards applicable to actual card-data handling. Never retain CVV/CVC, PIN/PIN block or full track data after authorization. Do not send full payment credentials to RT through ordinary email, chat, logs or legal forms. Any storage of account data requires the appropriate authorization, necessity and PCI safeguards; a generic contract does not certify compliance.

E.4 Sales and prohibited processing

Submit genuine approved sales of Merchant's own business. No card testing, transaction laundering, fictitious/self-funding transactions, undisclosed third-party sales, duplicate charges, unauthorized cash advances or hidden financial products. Recurring, installment, card-present, mail/telephone, advance-sale and marketplace models require specific approval and their mandated disclosures and consents.

E.5 Fees and refunds

Buyer-facing surcharges or convenience fees need RT approval and must satisfy current law and method rules, including debit/prepaid restrictions, registration, caps and disclosure. Return refunds through the original method where required; exceptions need provider approval and lawful verification. Preserve mandatory buyer and dispute rights. Coordinate a refund already subject to chargeback to avoid double payment.

E.6 Evidence and monitoring

Monitor dispute contacts daily on Business Days, provide complete relevant evidence by the notified deadline and implement lawful remedial controls when fraud/return/dispute levels rise. Network program thresholds and charges are the actual applicable requirements, not generic hard-coded figures. Merchant bears attributable payable assessments and transaction liabilities subject to the core Agreement's causation, accounting and legal limits.

Schedule F | Operating Rules and Processing Procedures

F.1 Readiness

Use approved integrations and current supported versions. Test success, failure, decline, duplicate, pending, timeout, webhook, refund, payout and reconciliation cases before production. Do not use real card credentials or unnecessary personal data in test environments. RT/provider production approval is required separately from contract acceptance.

F.2 Order and payment states

Keep order creation, authorization, capture, clearing, token minting, redemption, settlement and payout as distinct states. Fulfillment must follow the appropriate confirmed state for the method and product. Use immutable transaction references and idempotency keys. An uncertain request must be reconciled before retry, and duplicate charges or credits must be corrected promptly through the provider process.

F.3 Customer information and receipts

Clearly identify Merchant, the purchased goods/services, total paid, currency, taxes and fees, support contact and material fulfillment/refund terms. Retain evidence of required consent and product-specific disclosures. Do not put sensitive personal data in receipts, metadata or logs beyond what is necessary and permitted. A token receipt is additional evidence, not proof that a separate physical product was delivered.

F.4 Refunds and dispute files

Submit refunds promptly under applicable deadlines, using linked original-transaction references. Track chargebacks and refunds together to prevent duplicate repayment. Supply factual evidence responsive to the actual reason code; do not include prohibited authentication data. Meet RT's notified cutoff, ordinarily responding within two Business Days or sooner for a real external deadline. RT may require advance funding for reasonable external escalation costs.

F.5 Daily controls

Reconcile orders, provider events, gross amounts, fees, reserves, adjustments and payouts; investigate mismatches promptly. Monitor webhook failures and pending transactions. Keep dispute and risk contacts current. Preserve necessary records and evidence under applicable retention rules without retaining payment credentials or personal data indefinitely.

F.6 Changes and interruptions

Inform RT before changing domains, accounts, product scope, ownership, fulfillment, ticket size or volume materially. Implement required security patches and provider/API changes by the reasonable notified deadline. During an outage stop unsafe processing and follow documented provider fallback instructions only where expressly supported; this schedule does not authorize offline capture or voice authorization by default.

F.7 Support and enforcement

Report payment/security incidents to the channels in Schedule K, supplying transaction IDs and timestamps rather than secrets. RT may restrict unsafe integrations, re-underwrite, require remediation or apply core risk controls. A technical log or support response cannot amend pricing, approve a restricted activity or authorize a new funds flow. Changes to these binding rules follow core Section 16.

Schedule G | Data Processing and Privacy Requirements

G.1 Roles and scope

Each party acts as an independent controller/business for processing whose purposes and means it determines, including its own account administration, underwriting, sanctions/fraud prevention, legal duties, disputes and claims. Where RT processes personal data solely to perform Merchant's documented instructions for the selected Services, Merchant is controller/business and RT is processor/service provider. Provider roles follow their actual processing and contracts. RT's public privacy notice at https://rt.app/privacy/ informs individuals and is not a substitute for this processor agreement.

G.2 Processing particulars

Subject matter: operation, integration, support and records of Merchant's selected payment software Services. Duration: the service term plus lawful retention and deletion periods. Nature: collection from approved sources, hosting, organization, access, transmission to approved providers, reconciliation, support, security, return and deletion. Purpose: performing those Services on Merchant's lawful documented instructions. Data subjects: Merchant representatives/users, buyers, payers, payees and relevant contacts. Data: business/contact identifiers, account references, order/transaction/fulfillment data, provider verification results, device/security records and support records, limited to the selected function. No special-category data, government-ID copies, full card credentials or unnecessary public-chain identifiers may be supplied to RT as processor unless specifically approved with suitable legal and technical measures. Provider-hosted collection remains subject to that provider's role.

G.3 Instructions and purpose limits

The Agreement, selected service configuration and authenticated lawful requests are the documented instructions. RT will process processor data only for those instructions or a binding legal obligation, informing Merchant of a legal requirement where lawful. RT must notify Merchant if an instruction appears unlawful and may suspend it. RT will not sell or share processor data for cross-context behavioral advertising, use it for unrelated marketing or outside the direct business relationship, or combine it with other personal data except as applicable law permits. Each party certifies compliance with service-provider restrictions applicable to it. Lawfully de-identified data may be used for analytics only with safeguards, a commitment not to reidentify and corresponding downstream restrictions.

G.4 People and security

RT will ensure personnel access is authorized, necessary and confidential and maintain safeguards proportionate to the nature, scope and risks, including access control, secure transport and storage as appropriate, logging, resilience and incident response. Schedule C supplies the operational control requirements without asserting an unverified certification. Merchant remains responsible for its endpoints, credentials, lawful collection, disclosures and instructions. RT must not treat a hash or wallet address as automatically anonymous.

G.5 Subprocessors

Before processor data is disclosed, RT must provide Merchant a current named subprocessor register identifying function and processing location and obtain the authorization required by law. Merchant gives general authorization to the named register supplied with its activation record and permits changes on at least 30 days' advance notice, except a legally justified urgent replacement with prompt notice. Merchant may object on reasonable data-protection grounds within 15 days; the parties will seek a compliant alternative, and if none is available the affected processing must stop or be terminated without charges for future unused processing. RT must impose materially equivalent processor obligations by contract and remains responsible for its subprocessors' performance as required by law. An independent payment controller is not automatically a subprocessor.

G.6 Assistance and audit

RT will reasonably assist Merchant with rights requests, security duties, breach notifications, impact assessments and supervisory consultations relevant to processor data, taking account of information available to RT. It must forward a request it receives for Merchant unless legally prohibited and not respond substantively without instruction unless required by law. RT will make information necessary to demonstrate processor compliance available and allow proportionate audits by Merchant or an independent auditor, subject to safeguards protecting others' information. Ordinary assurance may begin with existing reports and summaries; restrictions may not defeat mandatory audit rights or regulator access. Reasonable extraordinary assistance costs may be agreed where lawful, excluding costs caused by RT's own breach.

G.7 Incident and notification

RT must notify Merchant without undue delay after awareness of a personal-data breach affecting processor data, with an initial notice where feasible within 24 hours and subsequent updates. Include known nature, affected categories/approximate scope, likely consequences, response measures and a contact point. Merchant must notify RT within 24 hours of awareness of a relevant suspected or actual incident in its responsibility. Notices are not admissions of liability. Mandatory authority/individual deadlines remain applicable and a party must not wait for confirmation where the legal clock starts at awareness.

G.8 Transfers

No restricted international transfer may begin merely because this schedule is posted. The parties must first establish an applicable adequacy basis or a valid transfer instrument with completed annexes, actual parties, processing/locations, security measures and subprocessor details. Where required and validly selected, the European Commission 2021 standard contractual clauses, appropriate Module 2 or 3, and applicable UK addendum apply in their unmodified official text and prevail over conflicting terms. They are available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj and the UK ICO website. This reference does not falsely represent that missing annexes are complete or that a transfer assessment has been performed. If no lawful basis exists, the affected transfer must not proceed.

G.9 Return and deletion

At Merchant's choice on termination RT will return or delete processor data and require its subprocessors to do likewise, except necessary lawful retention. Merchant may request an available export for 30 days; RT will then delete active processor copies within a reasonable documented period, ordinarily 90 days, with isolated backup expiry under an established retention cycle. Legally retained copies must remain protected, restricted to the retained purpose and deleted when the basis ends. RT will provide reasonable confirmation on request. Public-chain erasure cannot be promised; direct personal identifiers must remain off-chain; necessary public wallet/transaction references require a lawful basis and disclosure.

G.10 Oversight and changes

Merchant may take reasonable steps to confirm processor compliance, require notice if RT can no longer comply and require unlawful processing to stop or be remediated. No liability cap limits an individual's or authority's mandatory rights. This schedule controls data-processing matters; mandatory transfer clauses prevail. Material reduction of mandatory processor protections requires a lawful written agreement, not a silent page edit. Statutory rights and appropriate complaints to supervisory authorities are preserved.

Schedule H | Acceptable Use and Restricted Businesses

H.1 General boundary

Use the Services only for genuine, lawful, approved business transactions. Merchant must comply with restrictions of its actual providers, methods and territories, which may be stricter than this policy. RT may refuse an activity that presents unacceptable legal, financial, fraud or reputational exposure. A lawful product may still be unsupported; silence or a working technical integration is not approval.

H.2 Prohibited conduct

Prohibited uses include fraud, money laundering, terrorist financing, sanctions evasion, false identity or ownership information, card testing, fictitious or duplicate transactions, transaction laundering, sham self-funding, undisclosed third-party processing, credential sharing or unauthorized access, malware, phishing, circumvention of risk controls, deceptive marketing, counterfeit or stolen goods, infringement, exploitation, trafficking, child sexual-abuse material, and any transaction that is unlawful in a relevant jurisdiction.

H.3 Regulated or sensitive sectors

Prior specific written RT and provider approval, supported legal permissions and any required separate contract are necessary for gambling, betting, sweepstakes and paid contests; cannabis or controlled substances; pharmaceuticals, medical devices and regulated health/telemedicine; research chemicals/peptides where support is legally available; adult services; weapons and hazardous goods; financial services, lending, investments, token offerings or custody; digital-asset exchange or third-party marketplaces; charitable/political fundraising; high-exposure travel, tickets, subscriptions, advance sales and other restricted activities. Illegal, unlicensed or deceptive activity cannot be approved under this policy.

H.4 Product truthfulness

Merchant must accurately disclose actual products, intended and marketed use, fulfillment and beneficiaries. It must not replace a prohibited product description with "NFT", "digital service" or "research" to evade a restriction. Health, efficacy and investment claims require lawful substantiation and approvals. An NFT does not legalize the underlying sale or establish a licensing exemption. RT may require listings, labels, licenses and fulfillment evidence before or during processing.

H.5 Digital assets and personal data

No securities, yield/profit-sharing token, stored-value/cash-out product, gambling token or regulated financial instrument may be offered through the ordinary utility-NFT program. A separate review and approved legal model are required where support is available. Do not place personal or confidential information on public-chain metadata, expose credentials, or imply guaranteed redemption, asset value or chargeback immunity.

H.6 Enforcement

RT may investigate credible risk, request information, restrict listings or methods, suspend access, require remediation, apply justified reserves/holds or terminate under the core Agreement. RT may disclose information to providers or authorities for a lawful purpose with appropriate safeguards. A restriction is not a finding of criminal guilt, a contractual forfeiture or permission to retaliate against a protected complaint. Changes follow the core notice and version procedures.

Schedule I | Merchant Platform Use Terms

I.1 Scope

This schedule applies to a business that accepts the RT online MSA. It does not independently enroll a consumer, establish a financial account or replace a cardholder agreement. General browsing follows website terms; the accepted core and product terms control merchant-specific Services. Contract formation, a private order and service activation are separate.

I.2 License and users

Use the enabled software only for the approved business, account and territories. Each user must have authority and an individual access credential. No resale, sublicensing, reverse engineering beyond non-waivable rights, unauthorized testing, data scraping, third-party processing or misuse of RT/provider marks. Merchant is responsible for users and vendors within the permissions it grants, subject to law and the core loss allocation.

I.3 Integrations and permissions

Follow approved interfaces, data schemas and security requirements. A permission is limited by the actual account configuration and law. RT may change, retire or restrict an interface with notice where practicable, and urgently for security, provider or legal needs. Merchant must implement required supported updates and must not continue unsafe calls after revocation.

I.4 Products and buyers

Merchant remains responsible for its listings, lawful product supply, buyer disclosures, consents, support, refunds and fulfillment. RT may remove unsafe or unlawful content or integrations. Any token function, redemption control, agent feature, accelerated payout or supported method must actually be enabled; a published description alone does not make it part of Merchant's Services.

I.5 Changes and exit

The core Agreement governs amendments, suspension, termination, retention and migration. No binding uptime, service credit or certification is created by a general availability statement. No non-disparagement language limits protected complaints or truthful communications. Merchant may contact support@rt.app for operational matters and legal@rt.app for contractual notices.

Schedule J | Digital-Asset Risk Disclosures

J.1 Asset and provider risk

Stablecoins and NFTs are digital assets, not ordinary insured bank deposits. A stablecoin can lose its reference value or liquidity and can be affected by issuer reserves, redemption restrictions, sanctions, freezes, blacklists, insolvency, governance or regulatory changes. Provider custody or conversion has its own counterparty risks. No deposit or investment insurance applies merely because RT displays a balance; any coverage must be expressly established by the applicable provider and law.

J.2 Network and contract risk

Transactions can be delayed, reorganized, censored, incorrectly routed or affected by a fork, bridge, smart-contract bug, upgrade, compromise or network outage. Finality depends on the network and provider requirements. Gas and other costs can change and may be nonrecoverable where law permits. A wrong address, network or token contract may cause permanent loss. Confirm supported destinations and token contracts before authorizing a transfer.

J.3 Control and recovery

Completed public-chain transfers generally cannot be reversed by RT. A provider or issuer may have specific freeze or recovery powers; their existence does not give RT unilateral control or guarantee recovery. Wallet security, authorized signers, recovery mechanisms and custody depend on the actual setup. Merchant and buyers must not share seed phrases or private keys and must understand the applicable provider recovery process.

J.4 Card versus on-chain finality

A token mint or stablecoin payout does not eliminate a card chargeback, bank return, fraud claim or refund obligation on the funding side. Direct on-chain payment may lack a card-network chargeback mechanism but remains subject to applicable contractual and legal remedies. Merchant must fund its obligations even if proceeds have already moved to a wallet.

J.5 NFT rights and persistence

An NFT conveys only the rights validly specified for it; ownership does not automatically transfer intellectual property, verify product legality, ensure delivery or promise investment value. On-chain records may be immutable/public, while linked content can be unavailable or separately hosted. Burning a token may not erase metadata, copies or underlying rights. Direct personal identifiers must remain off-chain; necessary public wallet/transaction references follow Schedule G.

J.6 Geographic and legal limits

Supported assets, methods and territories can change. EU/EEA crypto-asset and stablecoin services require the applicable legal and provider permissions, including MiCA requirements where relevant. No service is approved merely by publication of this disclosure. Merchant must accurately explain the actual transaction, material risks, fees, redemption/refund terms and responsible providers before a buyer pays.

Schedule K | Service Transparency, Support and Complaints

K.1 Contacts

Operational support and payment inquiries: support@rt.app; +1 844-604-1604. Legal notices, reserve reviews and contract disputes: legal@rt.app. Security incidents: security@rt.app. Privacy requests: privacy@rt.app. Include Merchant/account reference, relevant transaction IDs, timestamps, affected product and a concise description. Never send private keys, seed phrases, passwords, full card credentials or unnecessary identity documents through ordinary support channels.

K.2 Scope and authority

RT supports the software and interfaces it controls. Payment, account, custody, issued-card and network issues may require the relevant provider and its mandatory process. A support agent or administrator cannot create signing authority, waive underwriting, move funds outside a valid mandate or promise a regulator's outcome. Urgent lost/stolen-card or unauthorized-payment reports must also follow the applicable provider agreement.

K.3 Availability and maintenance

RT uses reasonable care in providing its agreed software duties. Provider networks, blockchains, internet/cloud services, compliance restrictions and maintenance can affect availability or payout timing. Scheduled maintenance is communicated where practicable; urgent security or stability work may begin immediately. No fixed uptime percentage, response SLA, service credit, backup frequency or recovery objective applies unless expressly agreed in writing.

K.4 Complaints

RT will acknowledge a complaint within two Business Days and aim for a substantive response within 15 Business Days. If investigation or provider information is still needed, RT will give an update and expected next step. Shorter mandatory deadlines prevail. A lawful hold review follows core Section 8, including review at least every 30 days. A complaint does not automatically release funds or suspend undisputed liabilities.

K.5 Records and escalation

Merchant should retain records and escalate an unresolved material issue with the relevant references to legal@rt.app. The Agreement preserves lawful court, provider, regulator and data-supervisory complaints. RT will provide retained contract copies on request. Online status, an internal comment, uploaded draft or sent envelope proves only that state, not successful execution, production activation or a completed payout.

K.6 AI-assisted text support

Where enabled and permitted, RT may use AI-assisted systems to organize text support requests, help prepare replies and answer routine questions. Human support remains available on request. Such systems cannot themselves authorize payments, refunds, access changes or other consequential actions. Required law, platform permissions, data-processing safeguards and any specific participant consent must be satisfied first. This clause does not activate AI voice answering, backdate consent, or authorize processing of historic or restricted chats.

Schedule Q | Connected-account payment processing

Q.1 Conditional scope

These terms apply only where Schedule A selects Stripe Connect and the specific Merchant/program is approved and enabled. Stripe Connect is a distinct payment-acceptance flow from card-funded NFT checkout. Nothing here represents that Stripe has approved RT, Merchant, a country, product or transaction type. Stripe's actual onboarding and capability decisions control use of its service.

Q.2 Separate Stripe agreement

For full-service accounts, processing is supplied by Stripe under the applicable country's Stripe Connected Account Agreement at https://stripe.com/connect-account/legal/full, including its Stripe Services Agreement. Recipient-only payouts instead use https://stripe.com/connect-account/legal/recipient. Before use, RT must present the correct agreement and obtain Merchant's express acceptance; acceptance of this MSA without that presentation and assent is insufficient. Disclose Stripe's Privacy Policy at https://stripe.com/privacy and, for full-service accounts, the country-specific acquirer disclosure at https://stripe.com/legal/acquirer-disclosure. Custom branding does not remove these requirements.

Q.3 Authorized activity

Merchant authorizes RT, only within the actual Connect configuration and permissions, to create or facilitate onboarding for the relevant connected account, transmit required accurate account/business information, access relevant account and transaction data, facilitate payment/refund/dispute and reconciliation instructions, communicate required information to Stripe, and collect agreed platform fees from eligible balances where supported and lawfully authorized. Payout scheduling, restrictions, reserves and loss recovery may be performed only where the program supports them and the required authority exists. These permissions do not grant control over unrelated Stripe accounts or external assets.

Q.4 Data and instructions

RT accesses and uses connected-account data for providing/supporting the selected Services, account administration, fraud/security, compliance, disputes and enforcement under Schedule G and RT's privacy notice. Merchant must keep information current and respond to Stripe and RT requirements. It must not authorize false onboarding data or misrepresent its products, beneficiary or location. Acceptance evidence and the configured permissions must be retained before production use.

Q.5 Fees and liabilities

Schedule A must state RT fees and whether Stripe/provider fees are included or separate. Merchant authorizes supported deductions only for agreed or otherwise lawfully payable amounts. Chargebacks, refunds, returns and negative balances attributable to Merchant remain Merchant's reimbursement obligations under the core Agreement, including where Stripe initially charges RT under a separate platform liability arrangement. RT cannot contract away its independent obligations to Stripe or charge Merchant twice.

Q.6 Restrictions and exit

Stripe may independently restrict capabilities, payouts or the account under its terms. Disconnection or termination does not erase existing disputes, reserves or payment liabilities. RT may stop its own Services and permitted instructions; any ongoing Stripe access or relationship is governed by Stripe and the actual account configuration. This schedule does not include Stripe Treasury, Issuing, crypto services, lending or a merchant-of-record model unless separately expressly contracted and approved.

Schedule R | NFT Checkout Product Terms

R.1 Actual approved flow

This schedule applies only to enabled NFT checkout. Schedule A and the activation record must identify the checkout/on-ramp/payment provider, Merchant, buyer collection recipient, asset/network, token function, fulfillment/redemption method and payout route. A card-funded digital-asset purchase and the subsequent token/utility and settlement steps must be described accurately. Do not substitute a generic Stripe Connect flow or assume every provider has the same merchant-of-record role.

R.2 Buyer clarity and underlying products

Before payment Merchant must explain the purchase, any NFT or digital-asset component, the actual seller, total price/fees, fulfillment and redemption rights, refund/cancellation terms and material blockchain risks. The NFT must represent the approved consumptive function. Merchant remains responsible for the underlying goods/services and lawful delivery. It must not disguise a prohibited physical or regulated product as an NFT, an investment, software or a research label.

R.3 Minting and redemption

Use only approved smart contracts, assets and networks and supported transfer/redemption controls. Keep records linking the authorized purchase, token issuance, entitlement and fulfillment. Do not duplicate entitlements or permit reuse after valid redemption/refund. A mint, burn or wallet event is not automatic proof that off-chain goods were supplied, does not determine legal classification and does not eliminate buyer rights or funding-side disputes.

R.4 Content and data

Merchant must own or license the relevant content and specify buyer rights. Do not add direct personal identifiers or confidential data to public-chain metadata; use minimal approved wallet/transaction references with a lawful basis, disclosures and appropriate off-chain safeguards. Record any contract administrator, upgrade, pause, transfer or burn powers accurately and disclose material buyer-facing features. RT makes no promise of universal technical reversibility or content deletion.

R.5 Payout and losses

Provider settlement and verified Merchant payout follow the agreed model. Card chargebacks, bank returns, required refunds and properly attributable provider assessments can arise after a token or stablecoin payout. Merchant must fund those obligations and any justified reserve. No blanket statement that token payments are irreversible may be used to deny a card dispute or required refund. USDC, USDT, Base, token standard, gas allocation and accelerated payout are included only if explicitly approved for the actual program.

R.6 Legality and service changes

Calling a token utility, a receipt or closed-loop does not establish a securities, payments, stored-value or licensing exemption. RT may suspend an unsupported or legally uncertain feature, require compliant changes and remove unlawful content from systems it controls. Merchant must arrange lawful fulfillment, refunds and content migration during wind-down; public records and third-party copies may persist. A provider's independent terms remain applicable.

Schedule S | Merchant APIs and Authorized-Agent Acceptance

S.1 Conditional product

These terms apply only to selected and enabled merchant API or agent-initiated acceptance. Publication is not a production-availability statement. They do not enroll Merchant as a cardholder, extend credit, authorize investment management or turn RT into an autonomous payer. Any issued-card or financial-account product remains separately governed.

S.2 Identity, permissions, rules and spending

Before accepting an automated request validate the identity of the requesting integration and the actual payer/merchant authorization, then apply the configured rules, then execute the permitted spending or acceptance action. An agent's text is not consent by itself. Enforce scope, beneficiary, amount/currency, expiry, budget, method, geographic and approval restrictions; preserve evidence of authority and the resulting transaction. Do not let a prompt or tool response override payment or security policy.

S.3 Payment methods

Single-use or scoped card flows and direct USDC payments are different methods with their own providers, permission models, finality, disputes and restrictions. Optional x402-compatible requests do not replace authentication, payer consent, sanctions controls, idempotency or reconciliation. The selected and actually enabled method must be identified; no route may silently substitute a different asset, beneficiary, price or provider.

S.4 Safe operation

Protect credentials and webhooks, validate signatures and state, prevent replay and duplicates, reconcile pending/failed/settled requests and apply rate limits. Revocation stops new actions within the supported architecture; it may not cancel a transaction already authorized or submitted to a network. Human approval is required where configured, legally necessary or needed to resolve an ambiguous consequential request. Keep customer and secret data out of prompts, public metadata and logs unless properly authorized and necessary.

S.5 Responsibility and intervention

Merchant is responsible for its authorized integrations, accurate listings and fulfillment and must cooperate in investigating unauthorized requests. RT may pause unsafe access or revoke credentials under the core Agreement. Liability depends on the actual authorization, causation, applicable method/provider rules and mandatory law; possession of an API key alone does not irrebuttably prove legal authorization. No AI system guarantees error-free fraud or compliance decisions.

Schedule Z | Version Control and Incorporation

Z.1 Register

The online MSA and these schedules are v3.0, issued 20 October 2026, effective for each Merchant under core Section 1.1. The accepted core's Schedule Z identifies the incorporated schedule PDF by immutable URL and SHA-256. The archive is https://rt.app/legal/merchants/archive/2026-10-20/ and the current directory is https://rt.app/legal/merchants/. The v2.0 signed edition remains separately archived and is not rewritten by this publication.

Z.2 Applicability

The schedules apply through valid acceptance of the online MSA or a later valid amendment. A website visit, waitlist entry, application or publication is not acceptance. A is the description of a separate private order; B-K cover relevant general topics; Q connected-account processing, R NFT checkout and S authorized-agent/API acceptance apply only to selected approved products. Legacy letters do not import their contents; historical L is excluded.

Z.3 Retained evidence

Retain accepted core and schedule bytes, versions and hashes, party identities, representative authority, authenticated account, timestamps, lawfully collected IP/user-agent data, exact consent/button wording and durable receipt. Keep each private order, provider consent, permissions, underwriting and activation record separately. Signed routes also require their envelope/completion evidence. Do not publish private acceptance records.

Z.4 Changes

A new edition must receive a distinct version/effective date and archive. Do not overwrite the archived edition referenced by a completed envelope. Material changes require the core Agreement's notice and consent procedures and cannot retroactively change accrued obligations. If current text conflicts with the accepted edition before a valid amendment, the accepted archive controls. RT will supply a retained copy if a URL is unavailable.