Fyntiq.

Fyntiq Wallet Privacy Policy

Effective Date: July 1, 2026 | Last Updated: May 15, 2026

Fyntiq Technologies LLC respects your privacy and is committed to protecting personal information collected through Fyntiq Wallet and related services. This Privacy Policy explains what we collect, how we use and disclose it, how long we retain it, and the choices and rights available to you.

1. Scope of this Privacy Policy

This Privacy Policy applies to personal information processed in connection with the Fyntiq Wallet mobile application, websites, online portals, individual and business accounts, USD-account features, cards, transfers, direct deposits, USDC conversion, subscriptions, rewards, customer support, marketing, advertising, analytics, security, and other products or services that link to this Policy.

Certain financial institutions, card issuers, payment processors, wallet-infrastructure providers, digital-asset providers, identity-verification providers, advertising platforms, and other partners may provide separate privacy notices. Their notices govern when they independently determine how personal information is processed. If a product-specific privacy notice conflicts with this Policy, the more specific notice controls for the relevant activity.

2. Fyntiq's Role

Fyntiq is a financial-technology company and is not a bank. Fyntiq provides the technology platform, customer interface, account experience, and related software services. Banking, card issuance, payment processing, money transmission, digital-asset conversion, and other regulated services may be provided by regulated financial institutions or licensed financial partners.

Depending on the processing activity, Fyntiq may act as a business or controller, a service provider or processor, a joint participant in a financial program, or a technology provider supporting a regulated partner.

3. Personal Information We Collect

The information we collect depends on the Services you use, your location, whether you have an individual or business account, and how you interact with Fyntiq.

3.1 Identification and profile information

- full legal name, preferred name, username, date of birth, age, citizenship, nationality, residential and mailing addresses, country of residence, tax residency, email address, telephone number, occupation, employer, account preferences, photograph, signature, and customer-support records.

3.2 Government identification and KYC information

- Social Security number, taxpayer or national identification number, passport number, driver's license or state identification, images of identity documents, proof of address, immigration or residency information, document-authenticity results, selfie and liveness images, facial-comparison or biometric-derived verification results, sanctions and watchlist results, politically exposed person screening, adverse-media results, source-of-funds information, source-of-wealth information, and information needed for enhanced due diligence.

3.3 Business-account information

- legal and trade names, formation jurisdiction, formation documents, employer identification number, business address, website, industry, merchant category, expected transaction activity, business purpose, ownership structure, beneficial-owner information, controlling-person information, officer and director information, licenses, registrations, financial statements, bank statements, invoices, tax records, source-of-funds information, and information concerning the authorized account representative.

3.4 Financial and transaction information

- assigned routing and account numbers, linked bank-account information, payment-card details or tokens, wallet and USDC balances, transaction amounts, dates and times, sender and recipient information, merchant names and categories, ATM information, direct-deposit information, ACH and wire instructions, bank-transfer information, withdrawals, authorizations, settlements, refunds, reversals, disputes, chargebacks, fees, subscriptions, cashback, rewards, negative balances, holds, and reserves.

3.5 Non-custodial wallet and blockchain information

- wallet addresses, public keys, blockchain transaction identifiers, network and smart-contract information, wallet creation and recovery events, device-authentication information, wallet signatures, transaction status, token balances, and publicly available blockchain information.

3.6 Card information

- virtual and physical card identifiers, masked card numbers, card tokens, card status, card tier, activation information, shipping information, mobile-wallet provisioning information, merchant authorizations, card-present and card-not-present indicators, ATM activity, card controls, replacement requests, disputes, and fraud indicators.

3.7 Device, internet, and usage information

- IP address, device identifiers, advertising identifiers where permitted, device model, operating system, app version, browser type, language, time zone, mobile carrier, network information, login details, session information, pages and screens viewed, features used, buttons selected, referring URLs, crash data, diagnostics, cookies, software development kits, and interactions with emails, notifications, or advertisements.

3.8 Location information

- country or region inferred from IP address, approximate device location, transaction location, ATM or merchant location, and precise location when you grant permission and the feature or security process requires it.

3.9 Communications and customer support

- emails, chat messages, support tickets, telephone records, recorded calls, recorded video calls, complaint information, photographs or documents you submit, survey responses, social-media communications, and other correspondence.

3.10 Contacts and recipient information

- names, usernames, email addresses, phone numbers, wallet identifiers, payment descriptions, and device-contact information when you grant permission.

3.11 Marketing and preference information

- marketing and notification preferences, campaign interactions, referral source, promotional eligibility, advertisement engagement, attribution data, survey responses, and inferred interests based on your use of the Services.

3.12 Information from public and third-party sources

- information from identity and business verification providers, financial institutions, card issuers and networks, payment processors, digital-asset providers, blockchain analytics providers, fraud-prevention services, sanctions and watchlist providers, credit or identity databases, government records, public records, merchants, counterparties, advertising and analytics providers, and social networks.

4. How We Use Personal Information

4.1 Provide and operate the Services

- establish and maintain accounts; verify identity and eligibility; provide assigned USD account details; create and operate non-custodial wallets; process deposits, transfers, ACH transactions, wires, bank withdrawals, card transactions, ATM withdrawals, mobile-wallet provisioning, subscriptions, cashback, rewards, statements, receipts, and support requests.

4.2 Verify identity and comply with law

- conduct KYC and KYB; verify beneficial owners and controlling persons; screen for sanctions and restricted parties; detect money laundering, terrorist financing, fraud, or prohibited activity; conduct enhanced due diligence; verify source of funds; comply with tax and recordkeeping requirements; respond to legal process; and submit legally required reports.

4.3 Protect users and prevent fraud

- authenticate users; approve devices; identify account takeover; detect stolen, synthetic, or duplicate identities; evaluate transaction risk; block suspicious transfers; restrict insecure devices; detect location inconsistencies; prevent reward abuse; investigate disputes; recover funds; protect systems; and enforce our Terms.

4.4 Communicate with you

- send service notices, security alerts, transaction confirmations, direct-deposit notifications, statement notices, card notices, subscription notices, policy updates, support responses, legally required disclosures, marketing messages where permitted, and surveys.

4.5 Improve and develop the Services

- analyze product usage; diagnose issues; improve user experience; measure performance; develop and test features; train fraud and risk models; forecast demand; evaluate eligibility; and create aggregated or deidentified insights.

4.6 Advertising, attribution, and marketing

- measure advertising campaigns; identify how users found Fyntiq; deliver or measure Fyntiq advertising; create advertising audiences where permitted; prevent duplicate or irrelevant advertising; personalize marketing communications; and attribute app installs or conversions through providers such as Meta, Google, TikTok, Firebase, AppsFlyer, Adjust, Branch, or comparable services.

4.7 Corporate and legal purposes

- conduct audits, manage claims, enforce agreements, perform accounting, obtain insurance, evaluate business transactions, conduct due diligence, protect legal rights, and comply with regulatory examinations.

We do not use full bank-account numbers, full payment-card numbers, PINs, private keys, recovery phrases, or similar access credentials for third-party advertising or unrelated marketing.

5. Legal Bases for Processing

Where applicable law requires a legal basis, we process personal information based on one or more of the following:

- Contract: processing is necessary to provide the Services or take steps at your request.
- Legal obligation: processing is necessary to comply with financial, sanctions, tax, reporting, consumer-protection, or other laws.
- Legitimate interests: processing is necessary for fraud prevention, security, support, analytics, product improvement, business operations, or protection of legal rights, where those interests are not overridden by your rights.
- Consent: you consented to precise location, contacts, cookies, marketing, biometric verification, call recording, or another activity.
- Public interest or substantial public interest: processing is necessary for financial-crime prevention or regulatory purposes where recognized by law.
- Legal claims: processing is necessary to establish, exercise, or defend legal claims.

6. How We Disclose Personal Information

6.1 Financial and regulated-service partners

- banks, card issuers, card networks, payment processors, ACH and wire providers, ATM networks and operators, licensed money-service providers, digital-asset and stablecoin providers, wallet-infrastructure providers, mobile-wallet providers, and other entities needed to provide financial Services.

6.2 Identity, compliance, fraud, and security providers

- identity and business verification providers, sanctions-screening providers, device-intelligence services, blockchain analytics providers, fraud-prevention services, cybersecurity vendors, and compliance consultants.

6.3 Vendors and service providers

- cloud hosting, data storage, customer support, communications, analytics, session replay, app performance, card production, shipping, document storage, email, SMS, push notifications, accounting, auditing, legal services, insurance, and marketing providers.

6.4 Merchants, recipients, and transaction participants

- recipients, senders, merchants, acquiring banks, financial institutions, ATM operators, payment networks, and other participants needed to complete, investigate, or reverse a transaction.

6.5 Government and legal recipients

- courts, regulators, tax authorities, law-enforcement agencies, sanctions authorities, government agencies, and parties involved in valid legal process.

6.6 Affiliates and corporate transactions

- current or future affiliates and parties involved in a merger, acquisition, financing, reorganization, asset sale, bankruptcy, program transfer, or similar transaction.

6.7 With your direction or consent

- other parties when you request or authorize the disclosure, connect a third-party service, or otherwise consent.

6.8 Aggregated and deidentified information

- information that has been aggregated or deidentified so it cannot reasonably be linked to you.

7. Sale, Sharing, and Targeted Advertising

Fyntiq does not sell personal information for money. We may use advertising, analytics, and attribution providers. Depending on applicable law, some disclosures of identifiers, advertising identifiers, device information, internet activity, or interaction data may be considered a sale, sharing for cross-context behavioral advertising, or processing for targeted advertising.

Eligible users may opt out through the "Do Not Sell or Share My Personal Information" control available through our website or application, cookie and privacy-preference settings, a legally recognized opt-out preference signal where required, or a request sent to privacy@fyntiq.com.

Fyntiq does not disclose full bank-account numbers, full card numbers, PINs, private keys, recovery phrases, government identification numbers, or account-access credentials for targeted advertising. We may continue using information for measurement, fraud prevention, security, contextual advertising, service communications, and activities not treated as sale, sharing, or targeted advertising under applicable law.

8. Cookies, SDKs, Session Replay, and Similar Technologies

We and our providers may use cookies, software development kits, pixels, tags, local storage, mobile advertising identifiers, session-replay tools, heatmaps, screen analytics, crash analytics, interaction recording, and similar technologies.

These technologies may support essential functions, authentication, fraud prevention, preferences, analytics, performance, support, advertising attribution, and advertising where permitted.

Session-replay and interaction tools may capture clicks, scrolling, screen navigation, field interactions, device information, and technical events. We configure such tools to avoid intentionally collecting PINs, passwords, full payment credentials, private keys, recovery phrases, or other sensitive authentication information. You should not enter confidential information into fields not intended for that purpose.

You may manage certain choices through browser settings, device settings, cookie controls, the Do Not Sell or Share control, or privacy-request mechanisms. Blocking essential technologies may prevent the Services from functioning properly.

9. Automated Decisions and Risk Evaluations

We and our providers may use automated systems to verify identity, detect fraud, assess transaction risk, screen sanctions, identify account takeover, determine limits, delay or reject transactions, identify prohibited activity, and determine whether additional verification is required.

These systems may evaluate identity information, transaction patterns, device data, location indicators, account history, and third-party risk signals. Where applicable law provides a right to information about or review of certain solely automated decisions producing legal or similarly significant effects, you may submit a request to privacy@fyntiq.com.

10. Biometrics and Identity Verification

Fyntiq and its identity-verification providers may collect and process identification-document images, selfie photographs, selfie video, facial geometry, facial-comparison results, liveness signals, document-authenticity results, biometric-derived templates or identifiers, identity confidence scores, and related fraud and verification signals.

This information may be used to confirm identity, compare you with an identification document, detect impersonation, detect duplicate, stolen, or synthetic identities, prevent account takeover, comply with financial-crime requirements, conduct reverification, and protect users and the Services.

Fyntiq or the applicable provider may retain biometric information for the period disclosed at collection, for up to seven years following account closure or termination, or for another period required or permitted by applicable law. Where legally required, Fyntiq or the provider will obtain consent and provide a separate biometric notice before collection.

Fyntiq does not use biometric information collected for identity verification to build advertising profiles or identify users for unrelated marketing purposes. Device-based Face ID, Touch ID, or similar authentication may be controlled by your device provider; Fyntiq generally receives an authentication result rather than the underlying biometric template.

11. Precise Location and Device Contacts

With your permission, Fyntiq may collect precise location information and access device contacts. Precise location may be used for fraud prevention, sanctions screening, security, transaction verification, geographic eligibility, support, and features that require location. Device contacts may be used to help you identify recipients, invite contacts, or send money.

You may withdraw permissions through your device settings. Disabling permissions may limit certain functionality or require additional verification.

12. Call, Chat, and Communication Recording

We may record or monitor customer-support calls, video calls, chats, and other communications for security, quality assurance, employee training, dispute resolution, fraud prevention, and compliance.

Where applicable law requires consent from all participants, Fyntiq will provide notice and obtain the required consent before recording. An alternative communication channel may be offered where required by law.

13. Data Retention

Fyntiq generally retains personal information for seven years after your account is closed or terminated.

We may retain information longer when reasonably necessary or legally required for anti-money-laundering and identity-verification obligations, sanctions screening and reporting, transaction and financial recordkeeping, tax reporting, fraud prevention, cybersecurity investigations, unresolved transactions, disputes, complaints, chargebacks, negative balances, collections, audits, regulatory examinations, subpoenas, court orders, litigation, enforcement of agreements, unclaimed-property obligations, or legal claims.

Different categories may be subject to different retention periods. Biometric information, advertising data, device data, customer-support recordings, blockchain records, and financial records may be retained according to separate legal, contractual, operational, or security requirements. Public blockchain information may remain permanently available and may not be capable of deletion or alteration by Fyntiq.

After the applicable retention period expires, Fyntiq may delete, destroy, anonymize, aggregate, or securely isolate personal information unless continued retention is permitted or required by law.

14. Data Security

Fyntiq maintains administrative, technical, and physical safeguards designed to protect personal information. These may include encryption, access controls, multifactor authentication, security monitoring, network protections, vendor oversight, incident-response procedures, employee training, security testing, vulnerability management, secure software-development practices, and retention controls.

No system is completely secure. You are responsible for protecting your phone, email account, security PIN, and other credentials. Fyntiq support will not ask you for your full PIN, private key, or recovery phrase.

15. Security Incidents

If we identify a security incident affecting personal information, we may investigate, contain, remediate, notify affected individuals, notify regulators or law enforcement, require credential changes, restrict accounts, and take other legally required or appropriate steps. Notification timing and content will depend on applicable law, the nature of the information, and the risk created by the incident.

16. International Data Transfers

Fyntiq is based in the United States and may process personal information in the United States and other countries where Fyntiq or its providers operate. Those countries may have privacy laws different from those where you live.

Where required, we use recognized safeguards for international transfers, such as adequacy decisions, standard contractual clauses, data-processing agreements, contractual safeguards, and supplementary security measures.

17. Geographic Availability

Fyntiq Wallet may be available to eligible users in multiple countries and territories. Availability varies by country, state, residency, citizenship, product, feature, payment method, card program, financial partner, digital asset, network, compliance requirements, and current in-app eligibility.

Certain Services may be available in one jurisdiction but unavailable in another. Fyntiq may add, restrict, suspend, or discontinue availability in any jurisdiction at any time, subject to applicable law. The current supported-country and feature-availability information may be displayed in the application, website, Help Center, or onboarding flow.

18. Your Privacy Rights

Depending on your location and applicable law, you may have the right to:

- confirm whether we process your personal information;
- access personal information and obtain a copy;
- correct inaccurate information;
- delete certain information;
- restrict or object to processing;
- withdraw consent;
- opt out of targeted advertising, sale, or sharing;
- receive portable data;
- appeal a denied privacy request;
- request information about certain automated decision-making;
- limit certain uses of sensitive personal information; and
- lodge a complaint with a privacy or data-protection authority.

These rights are subject to exceptions. We may retain or continue processing information when necessary to complete transactions, provide requested financial Services, comply with KYC, AML, sanctions, tax, or recordkeeping obligations, prevent fraud, protect security, resolve disputes, enforce agreements, or establish or defend legal claims.

19. Exercising Your Privacy Rights

You may submit a privacy request by emailing privacy@fyntiq.com, using a privacy-request form made available through the application or website, or using another method identified in a jurisdiction-specific notice.

Your request should identify your name, the email address or phone number associated with your account, the right you wish to exercise, and your jurisdiction. We may need to verify your identity before responding. Verification may require account authentication or additional information depending on the sensitivity of the request.

We will not discriminate against you for exercising an applicable privacy right. An authorized agent may submit a request where permitted by law; we may require evidence of the agent's authority and may independently verify your identity.

20. U.S. State Privacy Disclosures

Some U.S. state privacy laws provide eligible residents with rights to access, correct, delete, or obtain copies of personal information; opt out of sale, sharing, or targeted advertising; limit certain uses of sensitive information; and appeal a denied request. The scope of these rights and applicable exemptions varies by state.

Where required, Fyntiq will honor valid opt-out preference signals and provide a Do Not Sell or Share My Personal Information control. Certain information processed in connection with financial products may be exempt from some state privacy-law provisions, while other personal information remains subject to those laws.

21. California Privacy Notice

21.1 Categories collected

During the preceding 12 months, Fyntiq may have collected identifiers; customer-record information; protected classification information; commercial information; internet or electronic-network activity; geolocation information; audio, electronic, or visual information; professional or employment information; inferences; sensitive personal information; and financial information.

21.2 Sources and purposes

We collect information from you, your devices, transaction participants, financial partners, identity and fraud providers, public records, service providers, merchants, advertising platforms, and other sources described in this Policy. We use the information for the purposes described in Sections 4 and 5.

21.3 Categories disclosed

We may disclose the categories above to the recipients described in Section 6.

21.4 California rights

Subject to applicable exemptions, California residents may request access, correction, deletion, information concerning collection and disclosure, opt-out of sale or sharing, limitation of certain uses of sensitive personal information, and freedom from discriminatory treatment. Where required, Fyntiq will honor valid opt-out preference signals.

22. European Economic Area, United Kingdom, and Switzerland

Where applicable, individuals in these regions may have rights to access, correction, erasure, restriction, objection, portability, withdrawal of consent, information about international transfers, and complaint to a supervisory authority. You may object to direct marketing at any time.

Fyntiq has not appointed a Data Protection Officer, EU representative, or UK representative at this time. We will appoint such representatives or officers if required by applicable law and update this Policy accordingly.

23. Marketing Communications

You may opt out of promotional emails by using the unsubscribe link in the message, manage push notifications through your device or app settings, and stop promotional SMS messages by following the instructions in the message.

Even after opting out of promotional communications, we may continue sending transaction notices, security alerts, legal disclosures, statements, support communications, account notices, and other nonmarketing messages.

24. Children and Minors

The standard Fyntiq Wallet Services are intended for individuals who are at least 18 years old. We do not knowingly permit a person under 18 to establish a standard account independently.

Fyntiq may offer a separate minor or family product with verified parental or legal-guardian consent. Any such product will be subject to additional terms and privacy disclosures. If you believe a minor has submitted information without authorization, contact privacy@fyntiq.com.

25. Account Closure, Death, and Incapacity

Closing an account does not require Fyntiq to immediately delete all personal information. We may retain information needed to complete transactions, release funds, resolve disputes, prevent fraud, comply with financial laws, respond to estate representatives, address incapacity or guardianship, handle unclaimed property, or preserve legal claims.

We may request court orders, death certificates, probate records, guardianship documents, powers of attorney, or other evidence before disclosing account information or releasing funds.

26. Non-Custodial Wallet and Blockchain Limitations

Fyntiq Wallet uses non-custodial wallet infrastructure. Fyntiq support does not have access to your four-digit security PIN and will not ask you to disclose it. Fyntiq does not ask for private keys, recovery phrases, or other secret wallet credentials.

Public blockchain information may be visible to anyone and may remain permanently available. Fyntiq may be unable to alter, suppress, or delete information written to a blockchain. Privacy rights may therefore be limited with respect to immutable blockchain records.

27. Third-Party Links and Services

The Services may contain links to third-party websites, applications, merchants, or services. This Privacy Policy does not govern a third party's independent privacy practices. Review the applicable third-party privacy notice before providing personal information.

28. Changes to this Privacy Policy

We may update this Privacy Policy to reflect changes to the Services, our practices, partners, features, law, regulation, security, or operations. We will post the updated Policy and revise the Last Updated date. Where required, we will provide advance notice or obtain consent before a material change takes effect.

29. Contact Us

For privacy questions or requests:

Fyntiq Technologies LLC
Attn: Privacy
5830 E 2nd Street, Suite 7000
Casper, Wyoming 82609
United States

Email: privacy@fyntiq.com

For general customer support: support@fyntiq.com