

CardOnline Privacy Policy

Personal and Business Accounts

Version 1.0 | Effective date: **04 December 2024**

Operated by Online Finance Limited, New Zealand

IMPORTANT

This Privacy Policy explains how Online Finance Limited, operating the CardOnline brand, collects, uses, stores, discloses and protects personal information when you visit CardOnline.io, apply for or use a CardOnline Account, use CardOnline Cards or related Services, communicate with us, or otherwise interact with CardOnline. It should be read together with the CardOnline Terms of Service and other policies referred to in those Terms.

1. About CardOnline and this Privacy Policy

1.1 CardOnline is a brand operated by ONLINE FINANCE LIMITED, a New Zealand company with NZBN 9429053282101 and Financial Service Provider registration FSP1011411. Our registered address is Suite 1298 Unit A Level G, 26 Hobson Street, Auckland 1010, New Zealand.

1.2 This Privacy Policy applies to personal information handled by CardOnline in connection with CardOnline.io, Personal and Business Accounts, onboarding, KYC/KYB, USDT funding, Cards, Card Top-Ups, transaction and account management, Telegram functionality, support and related services (together, the "Services").

1.3 We handle personal information in accordance with the New Zealand Privacy Act 2020 and, where applicable, the Biometric Processing Privacy Code 2025 and other applicable privacy laws or codes.

1.4 "Personal information" generally means information about an identifiable individual. For Business Accounts, this may include information about directors, beneficial owners, Authorised Administrators, Authorised Cardholders, employees, contractors and other individuals associated with the Business Customer.

2. Personal information we collect

2.1 The information we collect depends on how you interact with CardOnline and which Services you use. It may include:

- identity and contact information, including legal name, date of birth, nationality or country, residential or business address, email address, telephone number and other contact details;
- government identification and verification information, including passport, driver licence or other identification documents, document numbers, issuing country, expiry information and verification results;
- photographs, selfie/liveness information and biometric-related information used for identity verification, fraud prevention, duplicate-identity detection and related compliance purposes;
- Business Account information, including company details, registration information, registered and operating addresses, directors, beneficial owners, key people, ownership and control information, and supporting corporate documents;
- account and authentication information, including login information, authentication events, account permissions, security settings and records relating to Authorised Administrators and Authorised Cardholders;
- financial, transaction and blockchain information, including CardOnline USDT Balance records, unique deposit addresses, blockchain transaction identifiers, deposit and Card Top-Up activity, Card transaction information, fees, refunds, reversals, disputes and chargebacks;
- compliance and risk information, including KYC/KYB results, AML/CFT and sanctions screening, blockchain/KYT information, fraud indicators, risk scores, source-of-funds or source-of-wealth information where required, and records of compliance reviews;

- device, technical and usage information, including IP address, browser and device information, operating system, timestamps, session information, security events, website activity and other technical information generated when using our Platform;
- communications and support information, including support tickets, emails, Telegram-related records where linked, complaints, enquiries and other communications with CardOnline;
- delivery information for Physical Cards, including delivery address, courier and tracking information; and
- marketing and website information, including cookie identifiers, referral information, campaign interactions and marketing preferences where applicable.

2.2 We do not intentionally collect more personal information than we reasonably need for the relevant purpose. We may request additional information where required for compliance, security, fraud prevention, service delivery, dispute handling or risk management.

3. How we collect personal information

3.1 We collect personal information directly from you when you register, complete onboarding, submit documents, fund or use your Account, order or use Cards, contact support, link supported services, complete forms or otherwise interact with CardOnline.

3.2 We may also collect personal information from other sources where permitted by law, including:

- Business Customers, Authorised Administrators, directors, beneficial owners, representatives or other persons who provide information about individuals associated with a Business Account;
- identity, KYC/KYB, AML, sanctions, fraud and compliance providers, including Didit;
- card issuers, programme managers, payment processors, payment networks, banks and other financial-service infrastructure providers;
- blockchains, blockchain analytics/KYT providers and publicly available blockchain records;
- public registers, company registries, sanctions lists, watchlists, insolvency records, regulatory databases and other public or commercial information sources;
- device, security, hosting, communications, website, analytics and advertising providers; and
- couriers and delivery providers in connection with Physical Cards.

3.3 Where CardOnline collects personal information about you indirectly, we will take reasonable steps to notify you where required by Information Privacy Principle 3A or another applicable rule, unless an exception applies. This Privacy Policy may form part of that notification where appropriate.

4. Didit identity, business and compliance verification

4.1 CardOnline uses Didit as a third-party identity, business verification and compliance technology provider for parts of our onboarding and ongoing risk-control processes.

4.2 Depending on the applicable workflow, information processed through Didit may include identity and contact details, government identification documents, photographs or selfies, liveness information, biometric-related information, device and IP information, business information, directors, beneficial owners or other key people, and AML/sanctions or related screening information.

4.3 We may use Didit-supported processes for purposes including identity verification, business verification, document verification, liveness or face verification, duplicate-identity or duplicate-face detection, AML/sanctions screening, fraud detection and related compliance or risk controls, where those functions are enabled for CardOnline.

4.4 Didit may process information on CardOnline's behalf or otherwise as described in the notices and terms applicable to its services. CardOnline may receive verification results, match information, risk indicators, screening results and other information generated through those processes.

4.5 Use of biometric information for biometric processing is subject to applicable privacy requirements, including the Biometric Processing Privacy Code 2025 where it applies. CardOnline uses biometric processing for identity, security, fraud-prevention and related verification purposes, not for unrelated behavioural advertising.

5. Why we use personal information

5.1 We may use personal information to:

- create, verify, administer and secure Personal and Business Accounts;
- perform KYC, KYB, AML/CFT, sanctions, blockchain/KYT, fraud, identity and ongoing due-diligence checks;
- determine eligibility for the Services and satisfy legal, regulatory, card-programme and risk requirements;
- provide unique USDT deposit addresses, record deposits, maintain internal ledger balances and process supported Card Top-Ups;
- order, create, deliver, activate, manage, freeze, unlink or otherwise support Cards and related functionality;
- process and reconcile transactions, fees, refunds, reversals, disputes, chargebacks and account-closure activity;
- provide Telegram alerts or functionality where you choose to link Telegram;
- provide customer support, investigate complaints and communicate service, transaction, security, compliance and legal information;
- protect CardOnline, customers and third parties from fraud, misuse, cyber threats, prohibited activity and security incidents;
- maintain, test, troubleshoot, improve and develop the Platform and Services;
- perform accounting, reconciliation, audit, reporting, record-keeping and business administration;
- comply with law, regulatory obligations, court orders, lawful requests and dispute-resolution requirements;
- measure website performance and understand how our public website is used; and
- conduct marketing and measure advertising effectiveness where permitted by law and subject to applicable preferences or consent requirements.

6. KYC, KYB, AML/CFT, sanctions and fraud information

6.1 CardOnline operates compliance controls that may include identity and business verification, ongoing customer due diligence, AML/CFT monitoring, sanctions screening, blockchain/KYT screening, fraud controls and transaction monitoring.

6.2 These processes may involve automated tools, matching technologies, risk indicators or screening systems. Results may be reviewed by CardOnline personnel where appropriate. CardOnline may request further information or restrict Services where required by law, compliance obligations, security, fraud prevention, programme requirements or legitimate risk controls.

6.3 We may be legally restricted from disclosing certain compliance information, reports, investigations or reasons for particular restrictions.

7. Biometric information

7.1 Identity verification may involve a photograph or selfie, liveness check, facial comparison or other biometric processing through Didit or another approved provider.

7.2 We use biometric processing where reasonably necessary and appropriate for purposes such as verifying that an applicant is a real person, matching the person to an identity document, detecting duplicate or fraudulent applications, protecting Accounts and meeting compliance requirements.

7.3 Biometric samples, templates, results and related information may be held by the relevant verification provider and/or CardOnline depending on the technical workflow. We apply or require safeguards appropriate to the sensitivity of the information and do not retain biometric information longer than reasonably necessary for the relevant purpose or applicable legal requirements.

7.4 Where the Biometric Processing Privacy Code 2025 applies, CardOnline will handle biometric information in accordance with that Code, including applicable requirements concerning necessity, proportionality, safeguards, transparency, use, disclosure, access, correction, retention and disposal.

8. Blockchain and transaction information

8.1 Public blockchains are transparent by design. Blockchain addresses, transaction identifiers, token amounts, timestamps and related information may be publicly visible and may remain permanently recorded on the relevant blockchain.

8.2 CardOnline may associate blockchain information with an Account for deposit processing, reconciliation, compliance, fraud prevention, transaction monitoring and support purposes.

8.3 We may use blockchain analytics or KYT providers to assess transaction and wallet risk, including links to sanctions, fraud, theft, scams, ransomware, darknet activity or other risk indicators.

9. Business Accounts and information about other people

9.1 A Business Customer may provide CardOnline with personal information about directors, beneficial owners, Authorised Administrators, Authorised Cardholders, employees, contractors or other associated individuals.

9.2 The Business Customer must ensure it is authorised to provide that information and should make affected individuals aware that their information may be provided to and processed by CardOnline, subject to applicable law.

9.3 CardOnline may contact or notify an affected individual directly where reasonably necessary or where required by applicable privacy law, including requirements relating to indirect collection.

10. When we disclose personal information

10.1 We may disclose personal information where reasonably necessary for the purposes described in this Privacy Policy, including to:

- Ddidit and other identity, KYC/KYB, AML, sanctions, fraud and compliance providers;
- card issuers, programme managers, payment processors, Visa or other payment networks, banks and related financial infrastructure providers;
- blockchain infrastructure and blockchain analytics/KYT providers;
- hosting, cloud, cybersecurity, software, communications, email and technical service providers;
- Telegram or other communication platforms where you choose to link or use those services;
- third-party website platform providers and providers supporting our public website, and analytics or advertising providers where applicable;
- couriers and delivery providers for Physical Cards;
- professional advisers, auditors, insurers, contractors and service providers who reasonably require the information to perform services for CardOnline;
- government agencies, regulators, law-enforcement bodies, courts, tribunals, dispute-resolution schemes or other persons where disclosure is authorised or required by law; and
- a purchaser, successor, affiliate, financier or adviser in connection with a bona fide corporate transaction, restructuring, financing, merger, sale or transfer, subject to appropriate confidentiality and legal requirements.

10.2 We do not sell personal information to advertisers as a standalone product.

11. Overseas processing and disclosure

11.1 CardOnline uses technology and service providers that may process or store personal information outside New Zealand. The countries involved may vary depending on the provider, infrastructure and Service used.

11.2 Where CardOnline discloses personal information to an overseas person or entity, we will take steps required by Information Privacy Principle 12 or other applicable law. Depending on the circumstances, this may include satisfying ourselves that the recipient is subject to the New Zealand Privacy Act, is required to provide comparable safeguards, is located in a jurisdiction with comparable privacy protections, or obtaining the individual's informed authorisation where required.

11.3 Some service-provider arrangements may involve information being processed on CardOnline's behalf rather than disclosed for the provider's own purposes. CardOnline will use reasonable contractual, technical and organisational measures appropriate to the arrangement and information involved.

12. Cookies, analytics and advertising technologies

12.1 Our public website is operated using third-party website platform providers. third-party website platform providers and CardOnline may use cookies, local storage, pixels and similar technologies required for website functionality, security, session management and performance.

12.2 We may also use analytics, measurement and advertising technologies from time to time. These may include services such as Google Analytics, Google Ads and Meta Pixel where enabled. The particular technologies used may change as our website and marketing activities develop.

12.3 These technologies may collect or generate information such as IP address, device and browser information, cookie or advertising identifiers, pages viewed, interactions, referral source, approximate location derived from technical information, campaign information and conversion or advertising events.

12.4 We may use this information to understand website use, diagnose performance, measure campaigns, improve our website and Services, measure advertising effectiveness and, where permitted, deliver or measure relevant advertising or remarketing.

12.5 Where consent or a particular cookie control is required by applicable law, we will use appropriate notices or controls. You may also be able to manage cookies through your browser or device settings. Disabling some technologies may affect website functionality.

13. Telegram and other external platforms

13.1 If you choose to link Telegram or another supported third-party communication service, CardOnline may transmit selected alerts, Card or Account information and related identifiers to the linked service as necessary to provide the requested functionality.

13.2 Telegram and other external platforms operate independently and have their own privacy practices. You are responsible for linking the correct account and securing access to it.

14. Communications and marketing

14.1 We may use your contact details to send transaction, security, compliance, legal, support and other service-related communications necessary to operate your Account or provide the Services.

14.2 We may send marketing communications where permitted by law. Marketing communications will include applicable unsubscribe or preference-management options. Unsubscribing from marketing does not prevent us from sending necessary service, security, legal or compliance communications.

15. How we protect personal information

15.1 CardOnline uses reasonable technical, organisational and administrative safeguards appropriate to the nature of the information and the risks involved. These may include access controls, authentication, logging, role-based permissions, secure infrastructure, monitoring, vendor controls and operational security procedures.

15.2 No internet, blockchain, communications or information-storage system can be guaranteed to be completely secure. You must also protect your Account credentials, devices, email account, Telegram account, Card information and other authentication methods.

15.3 Where we use service providers to process personal information, we take reasonable steps appropriate to the relationship to address confidentiality, security and permitted use of the information.

16. Retention and deletion

16.1 We retain personal information for as long as reasonably necessary for the purposes for which it was collected and for legal, regulatory, AML/CFT, accounting, tax, fraud prevention, security, dispute, audit and record-keeping requirements.

16.2 Different categories of information may have different retention periods. Closing an Account does not necessarily result in immediate deletion because CardOnline may be legally required or reasonably entitled to retain certain records.

16.3 When personal information is no longer required, we will take reasonable steps to delete, anonymise or otherwise dispose of it, subject to legal requirements, technical limitations and legitimate retention needs. Information permanently recorded on a public blockchain cannot generally be deleted by CardOnline.

17. Access and correction rights

17.1 Subject to applicable law, you may request access to personal information CardOnline holds about you and request correction where you believe information is inaccurate, incomplete or misleading.

17.2 To make a privacy access or correction request, submit a ticket through the CardOnline support system available on the Website or in your CardOnline Account. We may need to verify your identity before acting on a request.

17.3 In some circumstances the law permits or requires us to withhold information or decline a request. Where applicable, we will explain the basis for doing so and any available rights of complaint.

17.4 Where information is held or controlled by an independent third party, we may direct you to that provider or assist with the request where appropriate and legally required.

18. Privacy breaches

18.1 CardOnline maintains processes for responding to suspected loss, unauthorised access, disclosure or other privacy or security incidents involving personal information.

18.2 Where a privacy breach is notifiable under the Privacy Act 2020 or another applicable law, CardOnline will notify the Office of the Privacy Commissioner and affected individuals as required by law.

19. Children and eligibility

19.1 CardOnline Services are intended for persons who satisfy the eligibility requirements stated in the Terms of Service and applicable onboarding requirements. We do not knowingly provide Accounts to persons who are not eligible to use the Services.

19.2 If we become aware that personal information has been provided in connection with an ineligible or unauthorised application, we may restrict the application and handle the information in accordance with applicable law, compliance requirements and this Privacy Policy.

20. Automated processing and risk decisions

20.1 CardOnline and its service providers may use automated systems to assist with identity verification, liveness checks, duplicate detection, sanctions and AML screening, blockchain/KYT analysis, fraud detection, transaction monitoring, security and other risk controls.

20.2 Automated results may contribute to an application, transaction or Account being flagged, delayed, restricted or referred for further review. CardOnline may request additional information or conduct manual review where appropriate, but some actions may need to occur immediately for legal, sanctions, fraud, security or third-party programme reasons.

21. Changes to this Privacy Policy

21.1 We may update this Privacy Policy to reflect changes in law, regulation, privacy requirements, our Services, technology, service providers, security practices or business operations.

21.2 We will publish the current version and effective date. Where a change materially affects how we handle personal information, we will provide additional notice where required by law or reasonably appropriate in the circumstances.

22. Contacting CardOnline about privacy

22.1 CardOnline is operated by:

- ONLINE FINANCE LIMITED

- FSP1011411
- NZBN 9429053282101
- Suite 1298 Unit A Level G, 26 Hobson Street, Auckland 1010, New Zealand
- Website: CardOnline.io

22.2 For privacy questions, access or correction requests, or concerns about how CardOnline has handled your personal information, please submit a ticket through the CardOnline support system available on the Website or in your CardOnline Account.

22.3 If you are not satisfied with how a privacy matter has been handled, you may have the right to complain to the New Zealand Office of the Privacy Commissioner or another applicable privacy regulator.

23. Relationship with the Terms of Service

23.1 This Privacy Policy forms part of CardOnline's contractual and privacy framework but does not limit any right or remedy that cannot lawfully be excluded under the Privacy Act 2020, the Biometric Processing Privacy Code 2025 or other applicable law.

23.2 If there is an inconsistency between this Privacy Policy and a mandatory privacy requirement, the mandatory requirement prevails. The CardOnline Terms of Service continue to govern use of the Services generally.