

ALLFI

PRIVACY POLICY

Wireless, Mobile Wallet, Debit Card, Payment and Digital Services

Effective date: September 3, 2026

IMPORTANT PRIVACY NOTICE. This Privacy Policy explains how ALLFI collects, uses, discloses, retains, and protects personal information across its wireless, mobile-wallet, payment, card-related, website, application, and other digital services. Certain products are also governed by separate bank, cardholder, financial-privacy, CPNI, E-Sign, or product-specific notices. Those notices control for the specific regulated product or information they cover.

1. Scope and Relationship to Other Privacy Notices

This Privacy Policy applies to the ALLFI-branded websites, mobile applications, wireless services, mobile wallet, payment and money-movement features, debit-card program administration, customer support, and related services that link to or reference this Policy (collectively, the "Services"). "ALLFI," "we," "us," and "our" mean the ALLFI legal entity identified in the applicable enrollment flow, order confirmation, account screen, or customer agreement and its affiliates acting for the applicable Service.

Some Services are provided in whole or in part by regulated or independent third parties. If your Service includes a bank-issued debit card or card account, the issuing bank identified in your Cardholder Agreement (currently Cross River Bank, Member FDIC) provides a separate privacy notice for information it collects or controls. Wireless network services may be supplied by one or more underlying carriers, and those carriers may have separate privacy obligations when they independently control information. Optional third-party services, such as remittances, securities, precious-metals, telehealth, gift-card, rewards, travel, or marketplace services, may also have separate privacy notices.

This Policy supplements, and does not replace, any legally required Financial Privacy Notice, CPNI notice or approval, bank privacy notice, biometric notice and consent, or other product-specific disclosure. Mandatory law and the applicable regulated-provider notice control over any inconsistent provision.

2. Personal Information We Collect

The information we collect depends on the Services you use, how you interact with us, and applicable legal and regulatory requirements. We may collect the following categories.

2.1 Identifiers and account information.

Name, postal address, email address, telephone number, date of birth, username, account identifiers, customer or device identifiers, tax or government identifiers when required, and information used to establish or administer your account.

2.2 Financial and transaction information.

Bank-account information, payment-card information, account balances, wallet balances, transaction and payment history, funding sources, beneficiary or recipient information, merchant information, transfer instructions, refunds, reversals, chargebacks, and related records.

2.3 Identity verification and compliance information.

Government-issued identification, identity-verification results, tax information, sanctions-screening information, fraud and risk signals, and, where used, selfie, liveness, or biometric-related information. When law requires separate biometric notice, consent, or retention terms, we or the applicable verification provider will provide them before collecting covered biometric identifiers or biometric information.

2.4 Wireless service information and CPNI.

Wireless account information and Customer Proprietary Network Information (CPNI), which may include the quantity, technical configuration, type, destination, location, and amount of use of telecommunications services, call-detail and usage information, service features, roaming information, and information contained in bills relating to telecommunications service.

2.5 Device, network, and application information.

IP address, device model, operating system, browser type, app version, mobile advertising or device identifiers, diagnostic logs, crash data, security events, network information, cookie or SDK identifiers, and information about how you use the Services.

2.6 Location information.

General or precise location may be collected when necessary to provide wireless or location-enabled features, comply with emergency-service obligations, prevent fraud, verify transactions, support network operations, or provide a feature you request. Device or application permissions may provide additional controls.

2.7 Communications and support information.

Customer-service calls and messages, support tickets, complaint and dispute records, surveys, feedback, and other communications with us. Calls may be monitored or recorded where permitted by law and after any required notice or consent.

2.8 Information from partners and other sources.

Information may be received from financial institutions, card networks, payment processors, money-transfer providers, wireless carriers, identity and fraud providers, consumer reporting or public-record sources where legally permitted, merchants, employers or program sponsors, and other persons involved in a transaction or Service.

3. How We Use Personal Information

We may use personal information to:

- open, maintain, service, secure, and close accounts and provide the Services you request;
- process wallet activity, payments, transfers, debit-card transactions, refunds, cash access, remittances, and other financial transactions;
- activate and support wireless voice, messaging, data, roaming, Wi-Fi calling, SIM or eSIM, number-porting, device, and account features;
- verify identity, conduct customer due diligence, screen for sanctions or prohibited activity, detect and prevent fraud, and satisfy anti-money-laundering, payment-network, banking, and other compliance obligations;
- authenticate customers, protect accounts, investigate suspicious activity, prevent SIM-swap and port-out fraud, and maintain the security and integrity of our systems and networks;

- provide customer support, investigate complaints, resolve errors and disputes, and communicate about transactions, account changes, security events, outages, policy changes, and other service matters;
- improve, test, troubleshoot, personalize, and analyze the Services and develop new features;
- market ALLFI products or conduct joint marketing where permitted by law and consistent with the Financial Privacy Notice, CPNI rules, and your communication choices;
- comply with legal process, regulatory obligations, court orders, law-enforcement requests, tax requirements, recordkeeping duties, and legal claims; and
- complete or evaluate a merger, financing, restructuring, asset transfer, acquisition, sale, or other corporate transaction, subject to applicable law and confidentiality protections.

4. How We Disclose Personal Information

We may disclose personal information to the following categories of recipients, subject to applicable law and the limitations described in this Policy:

4.1 Financial institutions and regulated providers.

Issuing banks, custodial or settlement institutions, money transmitters, remittance providers, payment processors, card networks, ACH operators, and other regulated providers when needed to provide a financial Service or comply with law.

4.2 Wireless carriers and communications providers.

Underlying carriers, roaming partners, messaging providers, number-portability providers, emergency-service providers, device and SIM/eSIM providers, and other telecommunications vendors needed to provide wireless Service.

4.3 Service providers and contractors.

Cloud, hosting, cybersecurity, identity-verification, fraud-prevention, customer-support, analytics, document-delivery, communications, billing, collection, professional-services, and other vendors that perform services for us.

4.4 Transaction participants.

Merchants, recipients, senders, employers, program sponsors, funding-source providers, and other parties involved in a transaction or feature you request.

4.5 Government, regulatory, and legal recipients.

Regulators, courts, law-enforcement agencies, tax authorities, sanctions authorities, and other persons when disclosure is required or permitted by law, legal process, or to protect rights, safety, security, or property.

4.6 Corporate transaction recipients.

Potential or actual purchasers, investors, financing sources, successors, advisers, or other parties to a corporate transaction, subject to appropriate confidentiality and legal restrictions.

4.7 At your direction or with your consent.

We may disclose information when you direct us to do so, consent to the disclosure, or use a feature that necessarily requires disclosure to another person or service.

For nonpublic personal financial information, ALLFI does not share information with affiliates for their everyday business purposes or marketing, and does not share with nonaffiliates for their own marketing, except as permitted by law or with your direction or consent. The Financial Privacy Notice and any bank-specific privacy notice provide additional details and control if they differ.

5. Financial Privacy and Nonpublic Personal Information

Federal financial-privacy law may apply to nonpublic personal information (NPI) collected in connection with consumer financial products or services. Where applicable, ALLFI provides an initial, annual, or revised Financial Privacy Notice as required. A separate bank privacy notice may also apply to a bank-issued product.

5.1 Financial information we may collect.

Financial NPI may include Social Security number, income, account balances, payment history, credit history, credit scores, transaction history, checking-account information, wire-transfer instructions, and other information collected in connection with a financial product or service.

5.2 Financial sharing summary.

Reason we may share financial NPI	Does ALLFI share?	Can you limit?
For everyday business purposes, such as processing transactions, maintaining accounts, responding to legal investigations, or reporting as permitted by law	Yes	No
For ALLFI's own marketing purposes	No	We do not share
For joint marketing with other financial companies	No	We do not share
For affiliates' everyday business purposes, information about transactions and experiences	No	We do not share
For affiliates' everyday business purposes, information about creditworthiness	No	We do not share
For affiliates to market to you	No	We do not share
For nonaffiliates to market to you	No	We do not share

5.3 Your federal financial-privacy choices.

Federal law gives consumers the right to limit certain types of financial-information sharing, but not all sharing. If ALLFI begins a type of sharing that requires an opt-out right, we will provide the notice, method, and reasonable opportunity to opt out required by law before the sharing occurs. You may contact us using Section 16 for questions about financial privacy.

6. Wireless Privacy and Customer Proprietary Network Information (CPNI)

Federal telecommunications law provides special protection for CPNI. ALLFI and any telecommunications carrier subject to those rules have a duty to protect the confidentiality of CPNI.

6.1 Permitted uses.

We may use or disclose CPNI without additional customer approval when permitted by law, including to provide and bill for the telecommunications service you request, protect users and the network, prevent fraud or unlawful use, provide emergency services, or perform other activities specifically authorized by telecommunications law.

6.2 Marketing and other uses requiring approval.

When federal law requires customer approval before CPNI may be used, disclosed, or accessed for marketing or another purpose, we will provide a separate notice describing the CPNI involved, the intended use and recipients, your right to approve or deny access, and the steps to make that choice. Approval or denial remains effective until you revoke or limit it. Denying CPNI marketing approval will not affect the telecommunications services to which you already subscribe, except for consequences directly resulting from our inability to use CPNI for the optional purpose.

This Privacy Policy is not itself a request for CPNI marketing approval. Any required solicitation for CPNI approval will be presented separately and in proximity to the request for approval.

6.3 CPNI security and account authentication.

We use authentication and account-protection measures designed to prevent unauthorized access to CPNI. We may require passwords, one-time codes, secure device or application authentication, identity checks, or other methods before disclosing CPNI or making sensitive account changes. We may send security notifications when account credentials, authentication methods, addresses, SIM/eSIM, or other sensitive account information changes, as required or permitted by law.

6.4 SIM-swap and port-out protection.

For wireless Services subject to FCC requirements, we use secure customer-authentication methods and fraud controls for SIM/eSIM changes and number-porting requests, and we train relevant personnel to identify and respond to suspected SIM-swap or port-out fraud. Specific procedures may vary based on the Service and applicable law.

6.5 CPNI choices and records.

You may revoke or limit a CPNI approval using the method stated in the applicable CPNI notice or by contacting us. We retain records of CPNI approvals and notices for the period required by applicable FCC rules. We also provide breach notifications and make regulatory reports when required by law.

7. Cookies, SDKs, Analytics, and Similar Technologies

Our websites and applications may use cookies, software development kits (SDKs), local storage, pixels, device identifiers, analytics tools, and similar technologies to operate the Services, remember settings, authenticate users, detect fraud, measure performance, diagnose problems, and understand usage.

Browser and device settings may allow you to limit some technologies. Where applicable law requires recognition of an opt-out preference signal, such as Global Privacy Control, we will process the signal for the browser or device from which it is sent. Some essential security, authentication, fraud-prevention, or service-delivery technologies cannot be disabled without affecting the Services.

Certain analytics or advertising disclosures may be treated as a 'sale,' 'sharing,' or targeted advertising under some state privacy laws even when no money is exchanged. If ALLFI engages in activity that triggers such a right, we will provide the legally required notice and opt-out mechanism. Financial NPI and CPNI remain subject to their separate federal restrictions.

8. Communications and Marketing Choices

We and service providers acting for us may send account, transaction, fraud, security, receipt, servicing, collection, outage, network, legal, and other transactional communications by email, text, push notification, in-app message, mail, or telephone using the contact information you provide.

Promotional email, text, or telephone communications are sent only as permitted by law and any applicable consent. You may use the unsubscribe or opt-out instructions in a promotional message or contact us to update your choices. Marketing choices do not prevent transactional, security, fraud, legal, or other non-marketing communications needed to provide or protect the Services.

9. Sensitive Personal Information

Some Services require sensitive information, such as government identifiers, account credentials, financial account information, precise location, or identity-verification data. We use and disclose sensitive personal information only as reasonably necessary to provide requested Services, verify identity, secure accounts, prevent fraud, comply with law, or for another purpose you authorize. Where state law provides a right to limit certain uses of sensitive personal information, we will honor that right to the extent it applies.

10. U.S. State Privacy Rights

Depending on where you live, and subject to legal exceptions and exemptions, you may have rights concerning personal information that is not governed exclusively by federal financial-privacy or telecommunications law. These rights may include the right to:

- confirm whether we process your personal information and obtain access to it;
- correct inaccurate personal information;
- delete personal information;
- obtain a portable copy of personal information;
- opt out of the sale of personal information, sharing for cross-context behavioral advertising, targeted advertising, or certain profiling where those rights apply;
- limit certain uses or disclosures of sensitive personal information;
- appeal a denial of a privacy request where state law provides an appeal right; and
- exercise privacy rights without unlawful discrimination.

We may need to verify your identity and authority before completing a request. An authorized agent may submit a request where permitted by law, but we may require proof of authorization and direct verification with you. We may deny or limit a request when an exception applies, including when information must be retained to complete a transaction, comply with law, protect security, prevent fraud, exercise legal rights, or satisfy another lawful purpose.

For California residents, applicable rights may include the rights to know, access, correct, delete, opt out of sale or sharing, limit certain uses of sensitive personal information, and receive equal service and pricing. Where legally required, ALLFI will disclose categories of personal information collected, sources, purposes, recipient categories, and applicable sale or sharing practices for the preceding period in this Policy or a state-specific notice.

11. Data Retention

We retain personal information for as long as reasonably necessary for the purposes described in this Policy, including to maintain an account or Service, complete transactions, protect against fraud, resolve disputes, enforce

agreements, and comply with banking, payment-network, anti-money-laundering, tax, telecommunications, CPNI, legal-hold, regulatory, and recordkeeping requirements. Retention periods vary by information type and Service.

When information is no longer reasonably needed, we delete, de-identify, anonymize, or otherwise dispose of it in accordance with applicable law and our retention procedures, unless a longer retention period is required or permitted.

12. Information Security

We maintain administrative, technical, and physical safeguards designed to protect personal information against unauthorized access, acquisition, use, alteration, disclosure, or destruction. Safeguards may include access controls, authentication, encryption or tokenization where appropriate, network and application security, monitoring, incident-response procedures, employee training, vendor controls, and secure development practices.

No security system can eliminate all risk. You are responsible for protecting your credentials, device, and authentication methods and for notifying us promptly if you suspect unauthorized access, account takeover, SIM-swap, fraud, or other security issues.

13. Third-Party Services and Links

The Services may link to or integrate products and services provided by third parties. Their collection, use, and disclosure of information is governed by their own privacy notices and agreements when they act as independent controllers or providers. ALLFI is not responsible for the privacy practices of an independent third party merely because its service is available through a ALLFI application or website.

14. Children and Authorized Minor Users

The Services are not directed to children under 13 unless a specific product is expressly designed to permit use through a parent, legal guardian, or other authorized adult and is offered with the notices, consents, and controls required by law. Some products may permit an authorized minor user or companion cardholder under separate eligibility and account terms. The primary account owner or guardian is responsible for permissions and account controls applicable to that minor user.

We do not knowingly sell personal information of consumers under 16 or share it for cross-context behavioral advertising without the affirmative authorization required by applicable law.

15. Changes to This Privacy Policy

We may update this Privacy Policy to reflect changes in the Services, our practices, technology, legal requirements, or regulated-provider relationships. The effective date above identifies the current version. If a change materially affects how we use or disclose personal information in a manner that requires advance notice, consent, or a new opt-out opportunity, we will provide it as required by applicable law.

16. Contact Us and Exercise Privacy Rights

For privacy questions, financial-privacy questions, CPNI choices, or requests to exercise an applicable privacy right, contact ALLFI using one of the following methods:

Telephone	1-800-724-7231
Email	support@ALLFIservices.com
Website	www.myallfi.net

Please describe the nature of your request and the Service involved. If your request concerns a bank-issued card or account, we may direct you to the issuing bank's privacy-request process when the bank controls the relevant information. If your request concerns an underlying wireless carrier's independently controlled information, we may direct you to that carrier when appropriate.

Separate legally required notices, including a Regulation P Financial Privacy Notice, Cross River Bank privacy notice, CPNI notice or approval, E-Sign consent, and product-specific privacy disclosures, remain part of the applicable customer documentation.