

ONLINE BANKING PRIVACY POLICY

Effective Date:

Institution: Polish & Slavic Federal Credit Union ("PSFCU")

Online Services Covered: Online and Mobile Banking, and any related digital banking services offered by Polish & Slavic Federal Credit Union

Article 1 — Purpose and Scope

- I. Purpose.** PSFCU, a federal credit union, respects the privacy of its members and other users of its online and mobile banking services. This Online Banking Privacy Policy explains how we collect, use, disclose, protect, retain, and otherwise handle information when you access or use our online banking platform, mobile banking application, website, electronic communications, digital account-opening tools, remote deposit capture, bill payment, person-to-person payment features, alerts, electronic statements, card controls, loan applications, and other digital financial services that we make available from time to time.
- II. Relationship to Other Notices.** This Policy supplements our federal consumer privacy notice and any other privacy, data-security, electronic-signature, account, membership, card, loan, or online banking agreements applicable to your relationship with us. If this Policy conflicts with a more specific notice or agreement that applies to a particular product, service, transaction, or feature, the more specific notice or agreement controls for that product, service, transaction, or feature.
- III. Applicability.** This Policy applies to information collected through the Online Services and through related electronic communications. It does not apply to websites, applications, products, or services operated by unaffiliated third parties, even if they are accessible through or connected to the Online Services, except to the extent we expressly state otherwise.
- IV. Membership and Account Context.** Because PSFCU is a financial institution, much of the information collected through the Online Services may be financial information, transaction information, account information, or other nonpublic personal information. We handle that information in accordance with applicable federal privacy, consumer protection, and information-security requirements governing federal credit unions and financial institutions.

Article 2 — Information We Collect

- I. Information You Provide to Us.** We may collect information that you provide directly to us when you enroll in, access, or use the Online Services, including:
 - A. Identity and Contact Information.** Name, address, email address, telephone number, date of birth, Social Security number, taxpayer identification number, government-issued identification information, membership number, account number, username, password, security questions, authentication credentials, and other identifying information.

- B. Account and Financial Information.** Deposit account information, loan information, card information, payment instructions, transfer instructions, transaction history, balances, statements, payee information, income information, employment information, and other financial or credit-related information.
 - C. Application and Verification Information.** Information submitted in connection with membership applications, account-opening requests, loan applications, service requests, fraud investigations, identity verification, beneficial ownership review, eligibility confirmation, or other compliance procedures.
 - D. Communications and Support Information.** Messages, chat content, call-back requests, complaint information, dispute information, online forms, service tickets, uploaded documents, images, signatures, and other communications you send to us through or in connection with the Online Services.
 - E. Device Permissions and Feature Content.** Information provided through device-enabled features, including camera access for mobile deposit, location access where enabled, contacts or payee information where permitted, biometric login settings maintained by your device, and notification preferences.
- II. Information Collected Automatically.** When you access or use the Online Services, we may automatically collect certain information about your device, browser, network, and usage activity, including:
- A. Device and Browser Information.** Device type, operating system, browser type, mobile carrier, device identifiers, advertising identifiers where applicable, screen resolution, language settings, and application version.
 - B. Log and Security Information.** Internet protocol address, access dates and times, session duration, pages or screens viewed, referring and exit pages, authentication events, failed login attempts, device fingerprinting signals, fraud indicators, error logs, and system activity.
 - C. Usage Information.** Features used, transactions initiated, alerts configured, search activity within the Online Services, navigation paths, preferences, and interactions with content, messages, forms, or tools.
 - D. Location Information.** Approximate location inferred from network information and, where you authorize it, more precise location information from your device, including location information used for fraud prevention, branch or ATM locator features, transaction monitoring, and security alerts.
- III. Information from Third Parties.** We may receive information about you from third parties, including:
- A. Consumer Reporting and Verification Sources.** Consumer reporting agencies, identity verification providers, fraud-prevention services, public records sources, sanctions-screening providers, and similar compliance or risk-management sources.

- B. Payment and Transaction Participants.** Payment networks, card processors, bill payment providers, person-to-person payment providers, merchants, other financial institutions, automated clearing house participants, check processors, wire-transfer participants, and other transaction counterparties.
 - C. Service Providers.** Technology vendors, online banking providers, mobile application providers, core processors, cloud-hosting providers, analytics providers, cybersecurity providers, digital communication vendors, and other service providers that support our Online Services.
 - D. Affiliates, Partners, and Joint Marketing Participants.** Entities with which we may have permissible relationships, subject to applicable law and our privacy notices.
 - E. Governmental, Law-Enforcement, and Regulatory Sources.** Federal, state, and local agencies, law-enforcement authorities, regulators, courts, and other lawful authorities.
- IV. Sensitive Information.** Depending on the Online Services you use, we may collect sensitive information, including Social Security number, government identification information, financial account information, authentication credentials, precise location information where enabled, and information contained in uploaded documents. We use and disclose sensitive information only as permitted by law and as reasonably necessary for the purposes described in this Policy.

Article 3 — How We Use Information

- I. Providing and Administering Online Services.** We use information to provide, maintain, improve, and administer the Online Services, including to:
 - A.** authenticate users and authorize access;
 - B.** process transactions, transfers, payments, deposits, withdrawals, applications, and service requests;
 - C.** maintain account records, transaction histories, preferences, alerts, and electronic statements;
 - D.** provide member support, respond to inquiries, and resolve disputes;
 - E.** operate digital tools, calculators, forms, messaging features, and account-management functions; and
 - F.** deliver notices, confirmations, statements, disclosures, alerts, and other communications.
- II. Security, Fraud Prevention, and Risk Management.** We use information to protect members, accounts, systems, and the credit union, including to:
 - A.** verify identity and eligibility;
 - B.** detect, prevent, investigate, and respond to fraud, unauthorized access, account takeover, suspicious activity, cybersecurity events, and other unlawful or harmful activity;
 - C.** monitor system integrity, availability, and performance;

- D. enforce security controls, authentication requirements, access restrictions, and account-protection measures; and
- E. conduct audits, testing, incident response, vulnerability management, and other risk-management activities.

III. Compliance and Legal Obligations. We use information to comply with applicable legal, regulatory, supervisory, tax, accounting, audit, recordkeeping, reporting, dispute-resolution, and law-enforcement obligations, including obligations relating to anti-money laundering, sanctions screening, consumer protection, electronic fund transfers, credit reporting, lending, deposit accounts, and regulatory examinations.

IV. Product, Service, and Operational Improvement. We may use information to evaluate, develop, test, improve, personalize, and enhance our products, services, systems, communications, and member experience, including by analyzing Online Services usage, member preferences, technical performance, and service quality.

V. Marketing and Member Communications. We may use information to provide information about products, services, promotions, financial education, events, and other offerings that may be of interest to you, subject to applicable opt-out rights and communication preferences. We do not use online banking authentication credentials for marketing purposes.

VI. Aggregated and De-Identified Information. We may create, use, and disclose aggregated, anonymized, or de-identified information for analytics, reporting, service improvement, security, regulatory, and business purposes, provided that such information does not reasonably identify you.

Article 4 — How We Disclose Information

I. Disclosure to Service Providers. We may disclose information to service providers that perform services for us or on our behalf, including providers of:

- A. core processing and account systems;
- B. online banking and mobile banking technology;
- C. payment processing, card processing, bill payment, person-to-person payment, and remote deposit capture;
- D. identity verification, fraud prevention, cybersecurity, authentication, and risk monitoring;
- E. cloud hosting, data storage, software, analytics, and technology support;
- F. statement production, electronic communications, mail, email, text messaging, and call center support;
- G. collections, legal, audit, compliance, and consulting services; and
- H. other operational services.

II. Service Provider Safeguards. We require service providers to use information only for authorized purposes, maintain appropriate confidentiality and security safeguards, and

comply with applicable legal and contractual requirements. Service-provider access to information is limited to what is reasonably necessary for the relevant service or function.

III. Disclosure for Transactions and Account Services. We may disclose information as necessary to process, administer, confirm, dispute, reverse, or investigate transactions and account activity, including disclosures to merchants, payment networks, other financial institutions, payment processors, clearinghouses, card associations, check processors, billers, payees, and transaction counterparties.

IV. Disclosure to Affiliates and Joint Marketing Partners. We may disclose information to affiliates and joint marketing partners as permitted by law and as described in our federal consumer privacy notice. Current affiliate and joint marketing information is as follows: TruStage and LPL Financial.

V. Disclosure for Legal, Regulatory, and Safety Purposes. We may disclose information:

- A. to comply with subpoenas, court orders, legal process, regulatory requests, examination requirements, and governmental inquiries;
- B. to law-enforcement authorities, regulators, courts, and other lawful authorities;
- C. to protect the rights, property, security, and safety of PSFCU, our members, our employees, our systems, or others;
- D. to investigate or respond to fraud, suspicious activity, cybersecurity events, disputes, unauthorized transactions, or potential violations of law or agreements; and
- E. as otherwise required or permitted by applicable law.

VI. Disclosure in Corporate or Structural Transactions. If PSFCU participates in a merger, consolidation, purchase and assumption transaction, conservatorship, liquidation, receivership, reorganization, transfer of assets, or similar transaction, information may be disclosed or transferred as permitted by law and subject to applicable supervisory, regulatory, and contractual requirements.

VII. No Sale of Member Information. PSFCU does not sell member nonpublic personal information. If state privacy law uses a definition of “sale,” “sharing,” or “targeted advertising” that may apply to certain online identifiers, analytics, or advertising technologies, our practices and any available state-specific rights are described in Article 13 and in PSFCU Privacy Notice.

Article 5 — Cookies, Analytics, Tracking Technologies, and Digital Advertising

I. Use of Tracking Technologies. We and our service providers may use cookies, pixels, tags, software development kits, local storage, session replay or screen analytics tools, device identifiers, log files, and similar technologies to operate the Online Services, authenticate users, remember preferences, measure performance, analyze usage, detect fraud, maintain security, and improve member experience.

II. Essential Technologies. Certain technologies are necessary for security, authentication, fraud prevention, transaction processing, accessibility, system performance, and core Online

Services functionality. If you disable these technologies, some Online Services may not function properly.

III. Analytics Technologies. We may use analytics technologies to understand how users interact with the Online Services, identify technical issues, improve functionality, and measure communications or feature performance. Analytics information may include device information, usage activity, browser information, approximate location, and interaction data.

IV. Advertising and Measurement Technologies. Where permitted by law and configured by PSFCU, we may use advertising or measurement technologies to evaluate outreach campaigns, measure engagement, and provide relevant communications. We do not permit advertising partners to access your online banking credentials or full account numbers.

V. Choices for Tracking Technologies. You may be able to manage cookies and similar technologies through your browser, device settings, application settings, or available preference tools. Your choices may vary by browser, device, and Online Service. Certain privacy signals, including browser-based opt-out signals, will be honored to the extent required by applicable law and technically feasible for the relevant Online Service.

VI. Third-Party Digital Services. Some Online Services may include content, features, or functionality provided by third parties. Those third parties may collect information directly from you or your device, subject to their own terms and privacy practices. We are not responsible for the privacy practices of unaffiliated third-party services.

Article 6 — Mobile Banking and Device Features

I. Mobile Application Information. If you use our mobile application, we may collect mobile device information, app usage information, device identifiers, operating system information, mobile carrier information, app version, crash logs, and related technical information.

II. Location Services. With your permission, our mobile application may collect precise location information to support features such as branch or ATM locators, fraud prevention, transaction monitoring, and security alerts. You may disable precise location collection through your device settings, but certain features may be limited or unavailable.

III. Camera and Image Access. With your permission, our mobile application may access your device camera, images, or files for features such as remote deposit capture, document upload, identity verification, or secure messaging attachments. Images submitted through these features may include checks, identification documents, signatures, account documentation, or other sensitive information.

IV. Biometric Login. If biometric login is available and you enable it, your biometric identifiers are generally stored and managed by your device or operating system provider, not by PSFCU. We may receive confirmation that authentication was successful, but we do not receive or store your underlying biometric template unless expressly disclosed in a separate notice.

v. Push Notifications and Alerts. If you enable alerts or push notifications, we may send account, transaction, security, marketing, service, or administrative messages to your device. Some

notifications may display information on your device screen depending on your device settings. You are responsible for configuring your device notification settings to protect your privacy.

VI. Device Security. You should protect your device, credentials, and authentication methods. If you believe your device, password, username, card, account, or Online Services access has been lost, stolen, compromised, or used without authorization, contact us immediately using the contact information in Article 16.

Article 7 — Security Safeguards

I. Administrative, Technical, and Physical Safeguards. We maintain a written information-security program designed to protect member information through administrative, technical, and physical safeguards appropriate to the sensitivity of the information, the nature of our operations, and applicable federal credit union requirements.

II. Security Measures. Our safeguards may include access controls, encryption, authentication controls, monitoring, logging, intrusion detection, vulnerability management, vendor oversight, employee training, physical security, incident response procedures, and other measures designed to protect information against unauthorized access, use, disclosure, alteration, or destruction.

III. Limitations. No information system, electronic communication, network, website, mobile application, or data transmission can be guaranteed to be completely secure. We therefore cannot guarantee that unauthorized access, interception, loss, misuse, or alteration will never occur.

IV. Member Responsibilities. You are responsible for maintaining the confidentiality of your username, password, multifactor authentication methods, device credentials, security codes, and other access credentials. You should use strong passwords, keep devices updated, avoid using public or unsecured networks for sensitive transactions, review account activity regularly, and promptly report suspected unauthorized activity.

V. Security Alerts and Communications. We may contact you regarding suspected fraud, security events, account activity, authentication changes, password resets, transaction verification, or other security matters. We will not ask you to provide your full password through email, text message, or an unsolicited telephone call.

Article 8 — Your Privacy Choices

I. Federal Consumer Privacy Choices. Your choices regarding our sharing of nonpublic personal information are described in our federal consumer privacy notice. Depending on our information-sharing practices, you may have rights to limit certain sharing with nonaffiliates, affiliates, or other parties as described in that notice.

II. Marketing Communications. You may opt out of certain promotional emails, text messages, or telephone solicitations by following the instructions provided in the communication or by contacting us using the information in Article 16. Even if you opt out of promotional communications, we may continue to send transactional, servicing, security, legal, and administrative communications.

III. Account Alerts and Notifications. You may manage certain account alerts, push notifications, and electronic communications through the Online Services, device settings, or by contacting us. Some notices may be required for account servicing, security, or legal compliance and may not be subject to opt-out.

IV. Cookies and Device Settings. You may manage certain cookies, location permissions, camera permissions, push notifications, and other device-based permissions through your browser or device settings. Disabling certain permissions may limit the availability or functionality of Online Services features.

V. Credit Reporting and Prescreened Offers. If we use consumer reports or prescreening programs in connection with credit offers, you may have choices under applicable consumer reporting laws. Additional information may be provided in our federal consumer privacy notice, credit disclosures, adverse action notices, prescreened offer notices, or other legally required notices.

VI. Joint Accounts. If you hold a joint account, choices made by one accountholder may apply to all accountholders on the account unless otherwise permitted by law or by our account procedures.

Article 9 — Access, Correction, and Account Information

I. Online Access. You may access and update certain profile, contact, security, alert, and account-preference information through the Online Services.

II. Correction Requests. If you believe information we maintain about you is inaccurate or incomplete, you may contact us using the information in Article 16. We may require verification of your identity and sufficient information to locate and review the relevant records.

III. Transaction Disputes. Disputes concerning electronic fund transfers, card transactions, billing errors, account errors, credit reporting, loan servicing, or other regulated matters may be subject to specific procedures, deadlines, notices, and rights described in applicable account agreements, periodic statements, disclosures, or notices. This Policy does not replace those procedures.

IV. Authentication and Verification. Before responding to a request to access, correct, update, or disclose information, we may require authentication and may decline to act on a request if we cannot verify identity, authority, or account ownership to our satisfaction.

Article 10 — Retention of Information

I. Retention Periods. We retain information for as long as reasonably necessary to provide Online Services, maintain accounts and records, comply with legal and regulatory obligations, resolve disputes, enforce agreements, prevent fraud, support security, conduct audits, and satisfy legitimate operational needs.

II. Retention Criteria. Retention periods may vary based on the type of information, account status, transaction history, product or service involved, legal requirements, regulatory expectations, litigation holds, fraud or security concerns, and operational requirements.

III. Deletion and De-Identification. When information is no longer required, we may delete, destroy, anonymize, de-identify, or aggregate it in accordance with our records-management and information-security procedures, subject to applicable law and operational constraints.

Article 11 — Children’s Privacy

I. General Rule. The Online Services are intended for use by members, joint accountholders, authorized users, applicants, and other individuals who are eligible to use our financial products and services. The Online Services are not directed to children under the age of 13.

II. Minor Accounts. We may collect information concerning minors in connection with youth accounts, custodial accounts, education accounts, joint accounts, authorized-user relationships, or other products or services permitted by law and our membership or account rules.

III. Parental or Guardian Inquiries. A parent, guardian, custodian, or other legally authorized person may contact us regarding information associated with a minor’s account, subject to verification of identity, authority, and applicable account ownership or access rules.

Article 12 — External Links and Third-Party Sites

I. External Services. The Online Services may allow you to access websites, applications, services, payment portals, merchant sites, financial tools, or content operated by unaffiliated third parties. Those third parties may have privacy, security, accessibility, and data practices that differ from ours.

II. No Control Over Third Parties. We do not control and are not responsible for the privacy or security practices of unaffiliated third parties. You should review the applicable third-party terms and privacy notices before providing information to or through those services.

III. Account Aggregation and Data Sharing at Your Direction. If you authorize a third-party financial application, data aggregator, or other external service to access your account information, that access may be governed by the third party’s terms, your authorization, and applicable law. We are not responsible for the third party’s use, storage, security, or redisclosure of information after you authorize access.

Article 13 — State-Specific Privacy Rights and Supplemental Notices

I. State Supplements. Certain state privacy laws may provide additional rights or notices for residents of particular states.

II. Scope of State Rights. State-specific rights may include, where applicable, rights to know, access, correct, delete, obtain a copy of, restrict, or opt out of certain uses or disclosures of personal information. These rights may be limited or unavailable where information is subject to federal financial privacy laws, maintained for compliance purposes, needed to provide financial services, or otherwise exempt under applicable law.

III. Requests Under State Law. If you submit a state privacy request, we may require information reasonably necessary to verify your identity, residency, authority, and relationship to the

account or information at issue. We may deny, limit, or decline requests as permitted by applicable law.

IV. Authorized Agents. If applicable state law permits requests through an authorized agent, we may require proof of the agent's authority and may require you to verify your identity directly with us.

v. Non-Discrimination. We will not unlawfully discriminate against you for exercising privacy rights available under applicable law.

Article 14 — International Use

I. United States Services. The Online Services are intended for use in the United States by eligible members and users of PSFCU. If you access the Online Services from outside the United States, you understand that information may be processed in the United States and may be subject to United States law.

II. Cross-Border Access Risks. Access to Online Services from outside the United States may be restricted, monitored, delayed, or unavailable due to security controls, sanctions requirements, fraud-prevention measures, local law, network conditions, or other operational considerations.

Article 15 — Changes to This Policy

I. Policy Updates. We may amend this Policy from time to time to reflect changes in our Online Services, technology, legal requirements, regulatory expectations, security practices, business operations, or information practices.

II. Notice of Changes. We will provide notice of material changes as required by law, which may include posting an updated Policy within the Online Services, sending an electronic notice, providing notice on statements or account communications, or using other legally permissible methods.

III. Continued Use. Your continued use of the Online Services after an updated Policy becomes effective constitutes acknowledgment of the updated Policy, subject to any consent requirements imposed by applicable law or by a separate agreement.

Article 16 — Contact Information

I. Privacy Contact. If you have questions about this Policy, our privacy practices, or your privacy choices, you may contact us as follows:

PSFCU

Attention: Compliance Department, Privacy
9 Law Drive, Fairfield, NJ 07921

Email: privacy@psfcu.net

II. Security and Unauthorized Activity. To report suspected unauthorized access, fraud, identity theft, lost or stolen credentials, compromised devices, or suspicious account activity, contact us immediately at:

contact@psfcu.net

III. Accessibility and Alternative Formats. If you need this Policy in an alternative format, please contact us at privacy@psfcu.net.

Article 17 — Federal Consumer Privacy Notice Coordination

- I. Nonpublic Personal Information.** We collect, use, and disclose nonpublic personal information as described in our federal consumer privacy notice, which explains our categories of information collected, categories of information disclosed, categories of parties to whom information may be disclosed, and available privacy choices.
- II. Consistency With Federal Credit Union Requirements.** Our privacy and information-security practices are designed to comply with applicable requirements for federal credit unions, including requirements concerning the privacy of member financial information, safeguarding of member information, vendor oversight, and confidentiality of records.
- III. Annual and Revised Notices.** Where required, we provide initial, annual, revised, or other privacy notices through methods permitted by law, including electronic delivery where you have consented or where otherwise permitted.
- IV. Opt-Out Implementation.** If you exercise an available federal privacy opt-out right, we will implement your choice within the time required by law and will apply it according to the scope and limitations described in the applicable privacy notice.