Pelican
CREDIT UNION
P.O. Box 40088
Baton Rouge, LA 70835
1-800-351-4877
Fax: 225-408-6200
pelicancu.com

WEBSITE PRIVACY POLICY DISCLOSURE

Pelican Credit Union ("Pelican," "we," "us," or "our") provides this Website Privacy Policy Disclosure ("Disclosure") to explain how we collect, use, share, and protect information obtained through our public website, Online Banking, and Mobile Banking applications (collectively, "Digital Services"). This Disclosure supplements Pelican's Gramm-Leach-Bliley Act ("GLBA") Privacy Notice. If there is a conflict, the GLBA Privacy Notice you receive as a member governs our sharing practices required by federal law.

This Disclosure applies to visitors to Pelican's website and web pages we control; users of Pelican Online Banking; users of Pelican Mobile Banking applications and related features such as mobile deposit, card controls, alerts, and push notifications; and individuals who communicate with us through secure messages or other digital interactions. It does not apply to websites, applications, or services we do not control, even if they are linked from our Digital Services.

Definitions – "Digital Services" means Pelican's website, Online Banking, and Mobile Banking applications. "Personal Information" means information that identifies, relates to, or could reasonably be linked to you or your household. "You" and "your" mean a Pelican member or an authorized user of a member's account.

Information We Collect – Information you provide includes contact details such as your name, mailing address, email address, and phone number; Online and Mobile Banking credentials and related security information such as usernames and selected security questions and answers (never share your password with anyone); information submitted in applications, forms, or secure messages; and transaction or service instructions, including transfers, bill payments, stop payments, card controls, and account changes.

Information collected automatically includes technical data such as your IP address, device and browser type, operating system, language settings, device identifiers, and mobile advertising IDs (if available); usage data such as dates and times of access, pages viewed, features used, referring or exit pages, and links clicked; and security and authentication data such as successful or failed sign-in attempts, number of logins, and fraud-prevention signals.

Mobile app permissions may be requested—if you enable the related features—for access to the camera or photos (for Mobile Check Deposit), microphone (for optional voice features), location (for ATM or branch finder and fraud signals), contacts (for person-to-person payments, if offered), and biometric authentication (such as Touch ID or Face ID on your device). You can manage these permissions in your device settings, but some features may not function without the related permission.

How We Use Information – We use information to provide, operate, maintain, and improve our Digital Services and member support; authenticate users and protect against fraud, abuse, and security incidents; process your transactions, applications, and account requests; perform analytics and reporting to enhance performance and usability; communicate with you about accounts, services, security alerts, and service updates; and comply with applicable laws, regulations, legal processes, and our policies. We do not sell your personal information.

Cookies, Pixels, SDKs, and Similar Technologies – We use first-party and limited third-party technologies—such as cookies, pixels, local storage, and mobile SDKs—to enable essential functions including security and session management, to measure performance and usage, and to remember preferences. We do not store sensitive account numbers or passwords in cookies. You may limit cookies or identifiers in your browser or device settings, but some features may not work as intended. Our Digital Services currently do not respond to "Do Not Track" signals because no standard has been adopted.

Online & Mobile Banking Practices – We collect only the information needed to follow your instructions—such as transferring funds, paying bills, depositing checks, sending alerts, or submitting applications—and to maintain the security and performance of the Digital Services. We may compile statistics such as the number of times you log in, and we do not sell this information. For your protection, access Online or Mobile Banking by typing our URL or using our official app, log out when you are finished and close your browser or app—especially on shared devices—and keep your devices, operating systems, and apps up to date.

How We Share Information – We may share information with service providers that assist us with Digital Services, transaction processing, communications, analytics, or fraud monitoring, subject to confidentiality and security

obligations; with payment networks and other financial institutions to process your transactions or as permitted by law; and for legal or safety reasons to comply with laws, regulations, subpoenas, and lawful requests, to protect Pelican, our members, or the public, or to enforce agreements. We also share information at your direction or with your consent, including when you enable third-party features. We do not provide any third party the ability to read your Online or Mobile Banking password.

Email, SMS/Text, and Push Communications – Email and standard text messaging are not secure; do not send account numbers, Social Security numbers, passwords, or other confidential information by email or standard text. Use secure messaging within Online or Mobile Banking or call 1-800-351-4877. If you enroll in alerts, message and data rates may apply to SMS/text and push alerts, and you may manage your preferences in the Digital Services or your device settings. You may opt out of marketing emails using the unsubscribe link, but you will still receive important service and account messages.

Children's Privacy – Our Digital Services are not directed to children under 13, and we do not knowingly collect personal information from them online. If you believe a child under 13 has provided information to us, please contact us so we can delete it.

Third-Party Links and Embedded Content – Our Digital Services may link to or embed third-party content that we do not control. We are not responsible for the content, accuracy, security, or privacy practices of third parties. Your use of third-party sites or services is governed by their terms and policies, which you should review before providing information or enabling features. You access third-party sites at your own risk.

Security Practices – We maintain administrative, technical, and physical safeguards designed to protect your information, including Transport Layer Security (TLS) encryption for data in transit, multi-factor authentication options, network and application monitoring, role-based access controls with employee training, and regular backups with business continuity measures. No system can be guaranteed 100% secure, and you also play a critical role in protecting your accounts (see Section 15).

Service Availability – Digital Services may be unavailable at times due to maintenance, updates, or events beyond our control. We perform frequent backups and implement redundancy to help protect against loss or inadvertent alteration of data.

Data Retention & Accuracy – We retain information as needed to provide services; to meet legal, regulatory, and security obligations; to resolve disputes; and to enforce agreements. Please keep your contact details current in Online or Mobile Banking or by contacting us so we can reach you with important account information.

Member Security Tips (Best Practices) – Use strong, unique passwords or passphrases and enable multi-factor authentication where available; be cautious of phishing attempts and avoid clicking links or opening attachments in unexpected messages requesting personal or account information; keep anti-virus and anti-malware protection current and avoid untrusted downloads; type our website URL directly when signing in and verify the official app publisher before installing; log out after each session, especially on shared devices; monitor your accounts regularly and report unauthorized activity immediately; and, if you are a business member, periodically assess user access, password practices, and dual controls.

Your Rights & Responsibilities – Your rights and responsibilities for Online and Mobile Banking and electronic fund transfers are described in your Account Agreements and Disclosures, including the Electronic Fund Transfers disclosure. If you see suspicious activity or believe your credentials are compromised, contact us immediately at 1-800-351-4877.

Changes to This Disclosure – We may update this Disclosure periodically. When we do, we will revise the Effective date above and post updates within our Digital Services. Your continued use after an update indicates your acknowledgment of the revised Disclosure.

How to Contact Us – For questions about this Disclosure or your digital privacy, contact Pelican Credit Union at 1-800-351-4877.