



**MILESTONE
BANK**
Formerly LCA Bank

MILESTONE BANK

Online Security Disclosure

Effective Date: June 16, 2026 • Last Reviewed: June 16, 2026

Purpose and scope. This Online Security Disclosure (this “Disclosure”) describes the principal measures Milestone Bank uses to help protect your information and your accounts when you access our Website and online services, and the responsibilities you accept when you use them. This Disclosure is incorporated by reference into, and supplements, the Milestone Bank *Website – Terms and Conditions of Use* and any account agreement or service-specific terms between you and Milestone Bank. If there is a conflict between this Disclosure and a signed account agreement, the account agreement controls. This Disclosure does not modify your rights under applicable law.

1. How Milestone Bank protects your information

1.1 Encryption in transit and at rest

Milestone Bank uses Transport Layer Security (TLS) to encrypt information transmitted between your browser and our Website and online portals. We use industry-standard encryption to protect sensitive customer information at rest within systems we control. We periodically review and update the cryptographic protocols and ciphers we support consistent with our information security program and prevailing industry guidance.

1.2 Authentication and access controls

Access to your Milestone Bank account requires authentication. Depending on the service and the risk profile of a given login or transaction, Milestone Bank may require:

- a password meeting minimum complexity and length requirements;
- multi-factor authentication using a one-time code delivered to a registered device or generated by an authenticator application;
- device recognition and binding to known devices;
- risk-based or step-up authentication for higher-risk activity, such as adding a new payee, initiating a wire, or changing contact information; and
- additional verification or a temporary hold for any activity Milestone Bank determines, in its reasonable judgment, presents elevated risk.

310 South Main St. Suite 900, Salt Lake City, UT 84101
Phone: 800-800-8098 • www.milestonebank.com
Member FDIC



**MILESTONE
BANK**
Formerly LCA Bank

You are responsible for keeping the email address, mobile telephone number, and other contact information associated with your account current so that Milestone Bank can deliver authentication codes and security notifications.

1.3 Monitoring, logging, and fraud detection

Milestone Bank logs and monitors access to its online services, including login attempts, transaction activity, and administrative changes, for the purposes of detecting fraud, investigating security incidents, complying with applicable law, and improving the security of our services. This monitoring may include automated risk scoring of transactions and may result in additional verification steps or the suspension of activity we reasonably believe to be unauthorized.

1.4 Session management

Our online portals are configured to terminate sessions after a period of inactivity. You should also log out of your session and close your browser when you are finished using the Website, particularly when using a shared or public device. Milestone Bank may also terminate any session that we reasonably believe to be compromised.

1.5 Vendor and third-party oversight

Milestone Bank uses third-party service providers to support certain online services, including, but not limited to, account statements, equipment financing, commercial banking, SBA lending, asset-based lines of credit, and consumer debt-settlement servicing. We conduct due diligence and ongoing oversight of these providers consistent with applicable banking regulations and interagency guidance on third-party relationships, including review of their information-security programs and incident-response capabilities.

1.6 Incident notification

If Milestone Bank determines that a security incident has occurred that affects your account or your personal information, we will provide notice to you in accordance with applicable federal and state law (including, where applicable, the Gramm-Leach-Bliley Act, the FTC Safeguards Rule, the federal banking agencies' Computer-Security Incident Notification Rule, and state breach-notification statutes) and our information-security program. Where required, we will also notify our regulators and other parties as the law directs.

2. Your responsibilities

You play an essential role in protecting your account. By using our Website and online services, you agree to:

310 South Main St. Suite 900, Salt Lake City, UT 84101
Phone: 800-800-8098 • www.milestonebank.com
Member FDIC



**MILESTONE
BANK**
Formerly LCA Bank

- **Protect your credentials.** Keep your username, password, security questions, one-time codes, and any device used to receive authentication codes confidential. Do not share them with anyone, including family members, employees, or any person who claims to represent Milestone Bank.
- **Use strong, unique credentials.** Choose a password that is not used for any other account, and change it promptly if you suspect it has been compromised. Where Milestone Bank offers passkeys or authenticator-app sign-in, we encourage you to use them in place of SMS-based codes.
- **Secure your devices.** Keep operating systems, browsers, and security software current. Use reputable anti-malware software where appropriate. Do not access your Milestone Bank account from a device or network you do not trust.
- **Verify before you log in.** Confirm that the address bar displays the expected domain (for example, milestonebank.com or a service-provider domain we have disclosed to you) and that the connection is secured by HTTPS before entering any credentials.
- **Use secure messaging for confidential communications.** Use the secure messaging feature within our online portals for confidential or account-specific communications, rather than email or text message.
- **Keep your contact information current.** Maintain a working email address and mobile telephone number on file so we can deliver authentication codes and security notifications.
- **Review your statements promptly.** Review your account statements, electronic notices, and transaction history regularly. Report any unauthorized or suspicious activity to Milestone Bank without delay. For consumer accounts subject to Regulation E, your liability for unauthorized electronic fund transfers depends on how promptly you notify us.
- **Honor any agreed security procedure.** For commercial accounts, comply with the security procedures established between you and Milestone Bank in writing. Under Article 4A of the Uniform Commercial Code, a commercially reasonable security procedure that you have agreed to may affect the allocation of loss from unauthorized payment orders.

3. How Milestone Bank will (and will not) communicate with you

Milestone Bank will never request the following by email, text message, or unsolicited telephone call: your password, your full account number, your full Social Security number or a one-time authentication code.

If you receive a communication that appears to come from Milestone Bank and asks for any of these items, treat it as a fraud attempt. Do not respond, do not click any links, and do not call any telephone

310 South Main St. Suite 900, Salt Lake City, UT 84101
Phone: 800-800-8098 • www.milestonebank.com
Member FDIC



**MILESTONE
BANK**
Formerly LCA Bank

number provided in the message. Instead, contact Milestone Bank using the contact information published on milestonebank.com.

Milestone Bank may legitimately contact you to verify a transaction we believe to be suspicious. In that case, our representative will provide information identifying the transaction and will not ask you to disclose your full credentials.

4. Reporting fraud, unauthorized access, or a security concern

If you suspect that your credentials, your device, or your account has been compromised, or that you have been the target of a phishing, smishing, vishing, or other fraud attempt involving Milestone Bank, contact us immediately. Prompt reporting is important to limit potential loss and, for consumer accounts, may affect your liability under Regulation E.

Customer Care Team – fraud and security reporting:

- Telephone: 888-542-5302
- Email (non-confidential reports only): CustomerSupport@milestonebank.com
- Mail: Milestone Bank, 310 S. Main Street, Suite 900, Salt Lake City, Utah 84101, Attention: Customer Care Team

Security researchers and responsible disclosure. Milestone Bank welcomes reports of suspected security vulnerabilities affecting our Website or online services. Researchers may submit reports to italerts@milestonebank.com. Please do not test against production accounts, access or modify customer data, or perform denial-of-service testing. Milestone Bank will acknowledge good-faith reports and will not pursue legal action against researchers who act in accordance with this paragraph.

5. Third-party access to your account

You may choose to share your Milestone Bank credentials or account data with a third-party financial-management application, data aggregator, or other service. If you do so:

- you are responsible for evaluating the security and reliability of that third party;
- access by that third party using your credentials may be considered authorized for purposes of this Disclosure and applicable law; and
- Milestone Bank is not responsible for losses that result from a third party's acts, omissions, or security failures, except to the extent applicable law allocates that loss to Milestone Bank.

Where Milestone Bank offers a more secure mechanism for sharing data with a third party (for example, a token-based data-access program), we encourage you to use that mechanism in place of sharing your credentials.

310 South Main St. Suite 900, Salt Lake City, UT 84101
Phone: 800-800-8098 • www.milestonebank.com
Member FDIC



**MILESTONE
BANK**
Formerly LCA Bank

6. Updates to this Disclosure

Milestone Bank may update this Disclosure from time to time to reflect changes in our security practices, technology, or applicable law. We will post the updated Disclosure on milestonebank.com and will indicate the effective date above. Material changes will be communicated to you in accordance with applicable law and your account agreement.