MapleMark BANK

SECURITY INFORMATION

REVISED

March 2026

If you are concerned that your account has been compromised, please contact Customer Service at 866-698-5760 (Monday–Friday 9am–5pm CST)

HOW DO WE KEEP YOUR DATA SAFE & CONFIDENTIAL?

MapleMark Bank pursues information security with the same commitment to excellence we apply to understanding our clients' financial needs. We strictly limit information sharing and employ layered administrative, technical, and physical safeguards designed to protect your information and maintain confidentiality.

Our security program is aligned with applicable federal standards and focuses on identifying, prioritizing, monitoring, and testing controls to address both existing risks and emerging threats. We also oversee third-party service providers to help ensure appropriate security protections.

CARD SAFETY & SECURITY

Chip Technology

Chip-enabled cards use dynamic authentication, making them significantly harder to counterfeit or copy.

If you notice suspicious card activity, contact us immediately using the number on the back of your card or call 866-698-5760.

MOBILE & ONLINE BANKING SECURITY

- Only enrolled devices may access your accounts; no account data is stored on your device.
- Online access is protected by username and password; clients are encouraged to use strong, unique passwords.
- Multi-factor authentication is required for certain activities such as device registration or password resets.
- Biometric login (Touch ID or Face ID) may be enabled on supported devices.
- Encryption protects data transmitted between your device and MapleMark systems.
- Automatic session timeouts help prevent unauthorized account access.
- Custom security alerts help you monitor balances, transactions, and payments.
- Electronic statements reduce fraud risk; MapleMark Bank never emails statements or attachments.

FRAUD MONITORING & DETECTION

Our fraud monitoring systems continuously analyze transaction activity to identify unusual patterns or suspicious behavior, allowing us to respond quickly to potential threats.

COMMERCIAL CUSTOMER SAFEGUARDS

- User-specific permissions and access controls
- Multi-factor verification for logins and payments
- Alerts for higher-risk activities
- Positive Pay and ACH Blocks/Filters
- Dual approval and transaction limits
- Secure data transmission methods and activity monitoring

Fraud risk management is a shared responsibility, and we partner closely with our commercial clients to address evolving threats.

ABOUT MAPLEMARK'S CYBERSECURITY PROGRAM

- Antivirus and endpoint protection
- Network firewalls and monitoring
- Intrusion prevention and detection
- Data loss prevention and backup controls
- Redundant systems and resiliency planning
- Ongoing security awareness training and governance oversight

WHAT YOU CAN DO

Remain vigilant against common fraud tactics such as phishing, smishing, vishing, ransomware, malicious pop-ups, and business email compromise. Do not share personal or login information in response to unsolicited communications and keep your devices and software up to date.

LEARN MORE

FDIC – Cybersecurity for Consumers:
https://www.fdic.gov/consumers/assistance/protection/idtheft.html

FDIC – Cybersecurity for Businesses: https://www.fdic.gov/regulations/resources/cybersecurity/

Federal Trade Commission – Online Security: https://www.consumer.ftc.gov/topics/online-security

FTC OnGuardOnline: https://www.consumer.ftc.gov/features/onguardonline