Customer Information & Cybersecurity Awareness

AmeriFirst Bank | Rev. 2026-10

At AmeriFirst Bank, we take safeguarding customer information seriously. You can help protect your personal and financial information by securing your accounts, recognizing scams, and reporting suspicious activity promptly.

Protect your information when communicating

Do not disclose passwords, PINs, or sign-in verification codes in response to an unexpected call, email, or text. Do not approve a login you did not initiate. Caller ID, logos, and familiar voices can be faked. If someone claims to represent AmeriFirst Bank, end the contact and call a trusted bank number before sharing information or following instructions.

When you initiate contact through a verified bank channel, the bank may need information to identify you or handle your request. To access online banking, use the official banking app or type **my.amerifirstbank.com** directly into your browser. Do not use links or phone numbers from suspicious messages.

Do not send account numbers, Social Security numbers, identification documents, or other confidential information through regular email. Regular email may not provide the protection needed for sensitive information. Contact a bank employee through a trusted channel for access to our secure email portal.

Secure your passwords and sign-in methods

Use long, unique passwords or passphrases. Use a different password for each account, especially email and banking. A reputable password manager can generate and securely store passwords. Follow each service's requirements; change passwords promptly if they are exposed, reused on a compromised service, or suspected stolen.

Enable multi-factor authentication (MFA). Use it wherever available. Where supported, a passkey or security key offers phishing-resistant sign-in. An authenticator app is another option. Keep recovery details current and store backup recovery codes securely.

Protect your email account. Email can be used to reset other account passwords. Review login alerts, recovery details, connected apps, and forwarding rules. If compromised, use the provider's official recovery process, change the password, and sign out other sessions.

Monitor your money and identity

Review transactions frequently and statements promptly; report unfamiliar activity immediately. Enable transaction and login alerts where available. Check credit reports through **AnnualCreditReport.com**. Consider a free credit freeze with each of the three national credit bureaus - Equifax, Experian, and TransUnion - to help prevent new-account identity theft. A freeze does not stop misuse of existing accounts.

Recognize Scams Before You Act

Phishing, texts, calls, and QR codes

Scammers may claim there is a suspicious transaction, overdue toll, delivery problem, refund, or account restriction. They may pressure you to act immediately or keep the conversation secret. Professional wording and correct personal details do not prove a message is genuine.

Check independently. Do not open unexpected attachments, scan unexpected QR codes, or use links in suspicious messages. Open the organization's official app or a saved bookmark, or type its known website address yourself. Verify unusual requests through a separate trusted channel, even when they appear in a familiar email conversation.

Do not rely only on appearances. A padlock or HTTPS means the connection is encrypted; it does not prove the business is legitimate. A familiar security image, sender name, or caller ID is not enough to verify identity. Inspect the full website address.

Be alert to AI impersonation. Criminals can imitate voices, create realistic videos, and write convincing messages. Call family members or coworkers back at a known number. Consider a family verification phrase for emergency requests.

Protect your money from impersonators

Do not move money to a supposed "safe account" to protect it. Treat instructions to withdraw cash for collection, buy gift cards or cryptocurrency, install remote-access software, or share your screen during banking as serious warning signs. Stop and contact the bank independently. Do not send money because someone promises a refund, prize, investment return, or recovery of money already lost.

Extra safeguards for business customers

Periodically assess online banking risks and review user access. Give each person an individual login and only the access needed for their role. Remove access promptly when duties change or employment ends. Use separate payment initiation and approval where available, and review payment limits and alerts with the bank.

Verify new or changed vendor, payroll, ACH, and wire instructions by calling an independently verified number. Do not rely solely on an email, an invoice, or a phone number supplied with the change request. Require a second authorized person to approve payment changes and reconcile activity promptly.

Protect your devices and important files

Install operating system, browser, app, and security updates promptly. Use supported security software where appropriate. Install apps from trusted sources and review permissions. Enable screen locks and device encryption, and avoid shared or public computers for sensitive transactions.

On any network, use the official app or verify the website address and HTTPS connection. Never ignore certificate warnings. Ransomware can lock files and demand payment. Keep backups separate from your working device, such as a disconnected external drive or protected cloud backup with recovery history, and test that files can be restored. Securely erase devices before disposal and shred sensitive paper records.

Act Quickly if Something Does Not Look Right

If money or banking access is at risk

Contact AmeriFirst Bank immediately. Tell us if you shared banking credentials, gave someone a verification code, approved an unfamiliar sign-in, installed remote-access software, or sent money because of a suspected scam. Ask whether a payment can be stopped or recovered. Recovery is not guaranteed; do not wait to report the incident.

Call **1-800-298-1763** or your branch. Use a trusted number from your statement, debit card, or the bank's official website. Do not use contact details supplied by a suspected scammer. Do not send sensitive information through ordinary email.

Branch	Phone
Union Springs	334-738-2060
Vaughn Road / Montgomery	334-409-2980
Prattville	334-358-0351
Lee County	334-821-1329
Escambia County	251-296-5356
Point Clear	251-973-3232

If a device or account may be compromised

If you suspect malware or ransomware, disconnect the affected device from Wi-Fi and wired networks. For a business device, notify your IT or security contact immediately and follow the incident-response plan. Use another trusted device to contact the bank and secure affected accounts. Do not continue banking on the affected device until it has been checked.

Use the provider's official recovery instructions to change affected passwords, revoke unfamiliar access, and review security settings. Keep relevant messages, screenshots, receipts, and transaction details. Do not pay someone who unexpectedly offers to recover your account or money.

Report fraud and find recovery help

These addresses are provided as plain text. Type them into your browser:

ReportFraud.ftc.gov - Report scams to the Federal Trade Commission.
IdentityTheft.gov - Report identity theft and get a recovery plan.
IC3.gov - Report internet-enabled crime to the FBI.
consumer.ftc.gov - Consumer scam and online-security guidance.
AnnualCreditReport.com - Access your credit reports.
amerifirstbank.com - Official AmeriFirst Bank website.
my.amerifirstbank.com - AmeriFirst Bank online banking sign-in.

Contact the bank first when your money or banking access is at risk. Filing an online fraud report does not notify the bank.