Protect Your Business Payments

A fraud-prevention checklist for ACH, wires, checks, and online banking. Share this sheet with everyone who initiates, approves, or reconciles payments.

Before sending money or changing instructions

Verify new or changed payment details independently. Call your vendor, employee, or other payee at a number already on file or independently verified. Do not use a new number from the change request, and do not rely on an email reply. A real email account or invoice can be compromised.

Require a second authorized review. Separate payment initiation and approval where available. Have another authorized person confirm payment changes, payee information, amounts, and approvals. Do not let an urgent executive request bypass your procedures.

Review payment protections with the bank. Ask about available approval controls, payment limits, alerts, and check or ACH fraud-prevention services. Configure controls to match your business risks; availability depends on your services and agreements.

Secure access and monitor activity

Give each user an individual login. Limit access to job duties, review it regularly, and remove it promptly when duties or employment change. Use long, unique passwords and multi-factor authentication. Never share credentials or sign-in codes.

Use trusted, updated devices. Protect business email and banking devices, install security updates, and verify unexpected support requests. Do not grant remote access at an unknown caller's direction or use shared/public computers for banking.

Review transactions every business day. Reconcile activity promptly, inspect check images and payee details, and follow up on unexpected payments or changed account information. Keep contact details and alerts current. Know the review and reporting deadlines in your account and service agreements.

Suspect fraud? Call immediately.

AmeriFirst Bank: 1-800-298-1763
Report suspicious access, payment instructions, or transactions promptly. Ask whether a payment can be stopped or recalled; recovery is not guaranteed. Notify your own IT/security contact if business email or devices may be compromised. Preserve relevant messages and payment records.

Business accounts generally do not have the same federal electronic-transfer protections as consumer accounts. Prompt review and reporting matter.

Bank website: amerifirstbank.com | **Online banking: my.amerifirstbank.com**
Internet-crime reporting: IC3.gov - reporting online does not notify the bank.