PROTECT

Your Business from Scams

Fraud attempts have become increasingly sophisticated, and we want to ensure you have the information you need to protect your business or organization. Below are the primary schemes we are seeing:

Business Email Compromise (BEC)

Fraudsters are impersonating company executives, vendors, or employees using email accounts that appear legitimate. These messages often request changes to payment instructions, urgent wire transfers, or sensitive information. What to do:

- ✓ Always verify payment-related requests using a known, trusted phone number.
- ✓ Review email addresses carefully for subtle misspellings.
- ✓ Enable multifactor authentication (MFA) where possible.

Counterfeit Currency

Several businesses have reported receiving high-quality counterfeit bills, especially in higher denominations. What to do:

- ✓ Train staff on security features of U.S. currency.
- ✓ Examine bills using multiple detection methods (touch, look, tilt).
- ✓ When in doubt, do not accept the bill and contact law enforcement.

Fraudulent ACH or Wire Instructions

Scammers may send altered invoices or payment instructions that direct funds to fraudulent accounts. These often come through email or appear to be updates from known vendors. What to do:

- ✓ Confirm all changes to account or routing information using previously verified contact information.
- ✓ Implement dual-control procedures for ACH and wire approvals.
- ✓ Monitor accounts regularly for unusual activity.

How We Can Help

Our team at Katahdin Trust is here to support your fraud-prevention efforts. If you receive a suspicious communication or have questions about protecting your accounts, please contact us immediately. Acting quickly can help minimize or prevent losses.

1-855-331-3221
(207) 521-3221

20 Katahdin Lane
Houlton, ME 04730

info@katahdintrust.com

Katahdin Trust Company