Bank of Tennessee

Carter County Bank | Mountain Community Bank

CARTER COUNTY BANK AND MOUNTAIN COMMUNITY BANK ARE DIVISIONS OF BANK OF TENNESSEE MEMBER FDIC

The Treasurer's Security Checklist

This checklist can provide you with ideas on how to manage and mitigate your risk.

Over the past couple of years, the public's attention has been drawn to cases of corporate fraud involving very large, publicly traded businesses. However, small businesses aren't immune to the same scams the large companies have fallen victim to. According to the American Institute of Certified Public Accountants (AICPA), small and midsize companies suffer a greater share of fraud losses than do the largest companies.

1. CHECK FRAUD

- Utilize Payee Positive Pay
- Utilize Positive Pay/Reverse Positive Pay
- Purchase check stock from known vendors
- Use blank check stock
- Use a high security check printing system
- Know your bank's process for check destruction and procedures for check fraud detection
- Make sure your bank has invested in a duplicate detection system if you use Remote Deposit Capture

2. CARD FRAUD

- Review card report daily
- Set transaction limits for corporate card purchases
- Use chip card technology
- Require PIN authorization
- Verify that customer's ID is authentic

3. ACH FRAUD

- Institute ACH debit filters and blocks – requests that do not meet a preset criteria are rejected
- Segregate accounts and duties
- Monitor and reconcile transaction accounts daily
- Know your customers and vendors
- Protect sensitive information: mask and encrypt
- Ensure tokens are collected and credentials are changed after employees leave

4. WIRE FRAUD

- Confirm that the client is in the loop when a requested third-party wire transfer is inconsistent with the client's past activity
- Examine the content of all requests for spelling and grammatical errors and/or overly formal language
- Watch out for requests to change a client's phone number
- Avoid responding directly to new email correspondence; send your response to a known email address instead
- Confirm requests using the phone number you have on file before sending any forms out
- Establish recurring wire templates, and review them on a regular basis

5. GENERAL INTERNAL CONTROLS

- Institute dual controls and a separation of duties for payment processes
- Set up dedicated computers for conducting transaction with a bank or payment processor
- Restrict physical access to the payment processing computer (i.e. use a secure room or office)
- Reconcile bank accounts daily
- Separate bank accounts by operating function
- Address exemption items in a timely fashion
- Perform periodic internal/external audits
- Set up an employee hotline to report potential fraud
- Restrict/limit employee internet usage of the organization's network
- Establish a centralized risk management department
- Institute human review of payment transactions
- Purchase insurance coverage to minimize risk
- Educate staff on risk mitigation and conduct phishing tests
- Set up HR policies for employee hiring and departures
- Do not initiate any payment transactions based solely on email instructions

Treasury Management Department

Detra Cleven
Sr. Vice President
Treasury Mgmt Services
423.262.5486

Heather Steele
Treasury Mgmt Sales Officer
Middle Tennessee
615.321.9244

Rod Stent
Treasury Mgmt Sales Officer
Northeast TN / Western NC
423.262.4317

Elizabeth Cox
Treasury Services
Support Specialist
423.262.5487

**In the event you suspect fraud or identity theft, contact our Customer Care Department immediately at 866-378-9500 or customercare@bankoftennessee.com