Business Fraud Prevention Checklist

Fraud can pose a significant threat to businesses of all sizes. This comprehensive checklist is designed to help your business proactively prevent, detect, and mitigate potential fraud risks. Use this guide as a tool for internal review and continuous improvement. Regular audits are recommended to be conducted using this checklist to maintain your vigilance against fraud. Partner with a **Central Bank Business Banker** to help find the products and solutions that will help you in fraud prevention.

✓ Employee Training and Awareness

- ❑ Establish a culture of integrity by fostering an environment where ethical conduct is prioritized and supported.
- ❑ Develop a *Fraud Response Plan* to ensure all fraudulent situations are handled effectively and efficiently when reported.
- ❑ Create a whistleblower policy allowing employees an anonymous reporting channel of potential fraud and that will investigate their reports in a timely manner.
- ❑ Conduct regular fraud awareness training to all your employees on common fraud schemes, red flags, and how to report fraud.
- ❑ Communicate the consequences of fraud by sharing the policies and reinforce the importance of ethical behavior.
- ❑ Update your training on a regular basis to stay up-to-date on the latest fraudulent activity.

✓ Regulatory and Law Compliance

- ❑ Maintain adequate documentation of all fraudulent activity.
- ❑ Stay up-to-date on fraud prevention laws and regulations.
- ❑ Ensure compliance with industry standards when reporting fraud.

✓ Internal Controls and Procedures

- ❑ Maintain clear documentation for all financial processes.
- ❑ Appoint a *Fraud Risk Manager* to oversee fraud prevention efforts.
- ❑ Limit access to sensitive information/systems, ensuring only essential personnel have access (bank accounts, BusinessLink, etc.)
- ❑ Utilize system-based controls to reduce manual intervention and errors.
- ❑ Enforce dual approval for payments, requiring two or more employees to authorize payments.
- ❑ Regularly review role assignments and duties to prevent employees from accumulating excessive control.
- ❑ Immediately remove privileges for terminated employees.
- ❑ Conduct surprise audits to verify compliance and detect irregularities.
- ❑ Hold regular accountability meetings to review key controls, fraud incidents, loss amounts, and case resolution times with senior leadership and management.
- ❑ Daily reconcile bank accounts and financial records for fraudulent activity and errors.
- ❑ Avoid using email to send confidential information, but if required, utilize an encryption software to protect sensitive information.

✓ Vendors and Suppliers

- ❑ Perform extensive checks on all vendors and suppliers (including background checks, as needed).
- ❑ Review contracts and payment terms ensuring all payment terms and contract details are transparent and verifiable. Seek legal advice when needed.
- ❑ Maintain an approved vendor and supplier list, only allowing payments to pre-approved vendors and suppliers.
- ❑ **NEVER accept payment requests via email or text message!**
- ❑ Require a second communication channel to validate payment related requests and/or change of payment instructions (especially when originated through email).
- ❑ Continuously monitor vendor and supplier performance and billing accuracy.

✓ Monitoring and Detection Systems

- ❑ Utilize automated fraud detection software that flags unusual transactions and activity.
- ❑ Conduct regular transaction reviews of high-risk transactions for anomalies.
- ❑ Use trusted firewall, anti-virus, encryption, and anti-malware software.
- ❑ Use caution when downloading software, downloading applications, opening email attachments, etc.
- ❑ Monitor for download requests from pop-up advertisements.
- ❑ Monitor employee's behavior using tools to detect unusual activities.
- ❑ If, at any point, you believe your cyber environment has been compromised, consult an external cyber forensics firm to complete a comprehensive review.
- ❑ Conduct regular testing for system vulnerabilities and resolve any discovered issues.
- ❑ Use multi-factor authentication for all system logins.
- ❑ Backup your data to an offsite, secure location, so you are still able to operate if an attack occurs.

✓ Financial Controls

- ❑ Monitor account balances and activity daily via BusinessLink and report any fraudulent activity immediately to a bank representative.
- ❑ Enable Alerts for transactions matching certain criteria, possible check suspected items, and possible ACH suspected items.
- ❑ Review and decision daily Check Positive Pay exceptions.
- ❑ Review and decision daily ACH Positive Pay exceptions.
- ❑ Utilize dual approval on ACH origination and Wire Transfer origination.
- ❑ Ensure each BusinessLink user's limits for above services are set appropriately.
- ❑ Incorporate security features into your check designs.
- ❑ Store blank checks and check printing equipment in a secured location with limited access, also limiting the working supply of checks removed from this area.
- ❑ Utilize BillPay to outsource and automate check printing, drastically reducing the need for physical checks.

This checklist serves as a foundational tool to safeguard your business from fraud. By focusing on these key areas, you can reduce the likelihood of fraud, protect your assets, and build a culture of accountability and integrity. For further guidance and support, please contact your **Central Bank**

REV 1-2025

MEMBER FDIC