BUSINESS FRAUD PREVENTION CHECKLIST

Revised 3/11/25

Safeguarding your business from fraud requires a proactive strategy. Partner with AbbyBank for regular reviews of your fraud prevention practices and access to the latest tools to keep your business secure.

ESSENTIAL PRACTICES

Employee Awareness & Training

- ☐ Educate staff on safeguarding sensitive info (account numbers, credit card details, personal data).
- ☐ Train employees to spot fraud tactics (phishing, scams, malicious links, attachments).
- ☐ Restrict access to secure areas and implement check-in/check-out for third-party vendors.
- ☐ Conduct annual training refreshers to reinforce best practices.

Securing Sensitive Information

- ☐ Limit personal email and internet use on computers with access to business online banking.
- ☐ Implement a "clean desk" policy to prevent unauthorized access to sensitive materials.
- ☐ Limit using email for sending confidential information; if necessary, use encryption software.

Yearly Reviews

- ☐ Meet with your insurance advisor to review policies and cybercrime coverage.
- ☐ Meet with your AbbyBank Business Banker to review online banking controls and security settings.

TECHNOLOGY & CYBERSECURITY MEASURES

Software & System Updates

- ☐ Keep operating systems, web browsers, and software (Microsoft, Adobe, etc.) updated.
- ☐ Install and maintain anti-virus, anti-malware, and firewall protections.
- ☐ Regularly back up data securely on separate servers.

AbbyBank

800-288-2229 • www.abbybank.com

TECHNOLOGY & CYBERSECURITY MEASURES

Hardware & Access Control

- [ ] Conduct audits to ensure only authorized personnel access critical systems.
- [ ] Review access permissions for networks and financial systems regularly.
- [ ] Restrict the use of USB drives to reduce the risk of malware.

Password Management

- [ ] Require strong, unique passwords with a mix of uppercase, lowercase, numbers, and symbols.
- [ ] Enable two-factor authentication where possible.
- [ ] Change passwords regularly and never write them down or share them.

Financial Transaction Controls

- [ ] Set approval thresholds for high-value transactions and require multiple authorizations.
- [ ] Utilize Positive Pay services to monitor and prevent fraudulent check and ACH transactions.
- [ ] Verify payment change requests with a call-back procedure.

Document Retention & Management

- [ ] Secure critical documents (checks, bank statements, employee records).
- [ ] Store records in a controlled environment with restricted access.
- [ ] Shred documents with cross-cut shredders or use a certified shred provider.
- [ ] Establish a document retention policy to store and destroy records securely after they are no longer useful.

FRAUD PREVENTION SERVICES & BEST PRACTICES

Enhancing Security with Banking Tools

- [ ] Implement check and ACH Positive Pay to identify and reject unauthorized transactions.
- [ ] Use encryption and tokenization for payment data security.
- [ ] Transition from check payments to ACH or wire transfers to minimize the risk of checking account fraud.
- [ ] Review check images online and reconcile the exceptions daily.

FRAUD PREVENTION SERVICES & BEST PRACTICES

Dual Control & Duty Segregation

- ☐ Ensure initiators and approvers use different workstations.
- ☐ Require dual approvals for ACH, wire transfers, and online banking transactions.
- ☐ Remove access privileges for employees who are no longer with the company.
- ☐ Limit employee access permissions and restrict administrative rights in online banking.

Monitoring Account Balances & Activity Daily

- ☐ Monitor account balances and activity daily to detect any irregularities.
- ☐ Immediately report suspicious activity to your bank and alert your users.
- ☐ Activate notification features within online banking to stay informed of account changes.

Disaster Preparedness & Fraud Response

- ☐ Develop a contingency plan for emergencies like cyberattacks, natural disasters, and power outages.
- ☐ Assign clear responsibilities for fraud prevention and incident response.
- ☐ Test security plans at least once a year to ensure effectiveness.
- ☐ If you suspect your cyber environment has been compromised, hire an external cyber forensics firm to conduct a thorough review.

We're serious about protecting your business and helping you manage the money you bring in using our cash management[1] tools. Contact an AbbyBank Business Banker to explore your options.

[1] *Subject to approval*

This checklist is intended for informational purposes only and does not provide legal advice. It does not address all aspects of the topics discussed. The content is meant to be used as a guide. For specific concerns, please consult with your attorney or fraud experts.