FRAUD PREVENTION

Best Practices to Safeguard Your Business

First Commonwealth Bank
MEMBER FDIC

Treasury Management

One of the best ways to prevent fraud is to educate yourself and your employees. These best practices are a resource to help recognize potential fraud, safeguard your businesses financial data and provide guidance towards developing a comprehensive fraud prevention program that is appropriate for your business. If you suspect fraud, please contact our Treasury Management Department at 724-463-5857.

Internal Policies and Procedures

Educating your employees and establishing sound procedures is your first line of defense to mitigate fraud.

Education and Training:

- ☐ Educate employees, partners and vendors on the importance of safeguarding sensitive information
- ☐ Establish training to build awareness of social engineering, phishing, acceptable use, business email compromise, identity theft and fraud.
- ☐ Ensure employees follow established procedures
- ☐ Ensure your staff understands they have the most important role in preventing fraud losses
- ☐ Make information about fraud easily accessible and update fraud training regularly

Separation of Duties for Employees:

- ☐ Control access to systems and information based on position and job function
- ☐ Cross-training and job rotation to reduce collusion risk
- ☐ Implement Dual Controls for transaction initiation
- ☐ Separate accounts receivables and accounts payables functions

Procedures:

- ☐ Use separate communication channels to validate payment requests
- ☐ Ensure payment requests from customers and internal employees, particularly senior employees are legitimate
- ☐ Validate requests from vendors to change payment instructions or unusually large payments
- ☐ Verify payment instructions from employees that are inconsistent with historical patterns

Authorities:

- ☐ Review and update signature cards regularly
- ☐ Update access privileges, particularly when roles change
- ☐ Give financial access only to employees who need it

Online Management

While technology has allowed businesses of all sizes to conduct business more efficiently, keeping your financial information protected is more important than ever.

Systems:

- ☐ Keep your operating systems, software, anti-virus and malware protection up-to-date
- ☐ Use caution when clicking links and downloading attachments, particularly from unknown senders
- ☐ Use encryption software when emailing confidential information
- ☐ Use a dedicated computer for your online banking activities with no other internet or email access
- ☐ Limit employee access to only those systems and applications required to perform their duties.
- ☐ Use security tokens, out-of-band or strong authentication for payment applications
- ☐ Implement and monitor intrusion detection and intrusion prevention systems

Controls:

- ☐ Require unique User IDs accompanied with complex passwords made up of letters, numbers and special characters.
- ☐ Truncate all but the last 4 digits of account numbers in both internal and external communications
- ☐ Require dual approvals from separate workstations to authorize transactions (ACH, Wires, etc.)
- ☐ Limit employee access privileges and system administrative rights and remove access for terminated employees
- ☐ Establish user entitlements to control online banking activities
- ☐ Implement company transaction limits, user transaction limits and daily processing limits
- ☐ Activate notification / alert features in online banking applications
- ☐ Monitor and reconcile all accounts daily

WE ARE HERE TO HELP

First Commonwealth is here to help you build for the long term by bringing you solutions, resources, and expertise that help your business succeed. To learn more about how we can bring ideas, insight and solutions please visit your local office or visit us online at www.fcbanking.com

FRAUD PREVENTION

Best Practices to Safeguard Your Business

First Commonwealth Bank
MEMBER FDIC

Treasury Management

Controlling Your Risk

Ongoing monitoring of your systems, controls and activities are essential component of your overall fraud prevention strategy to help recognize risks and mitigate potential fraud.

Planning and Monitoring:

- ☐ Conduct periodic audits of systems, policies, procedures and banking activities.
- ☐ Audits should be conducted both scheduled and at random to ensure compliance
- ☐ Evaluate computer network, firewall and other security/intrusion detection systems to ensure they are up-to-date
- ☐ Review downstream processes for cyber-security and fraud mitigation opportunities
- ☐ Test employee's knowledge of and adherence to fraud mitigation policies and procedures
- ☐ Work with your internal technology, audit and risk management partners on other ways to mitigate risks
- ☐ Partner with external auditors to conduct comprehensive annual reviews of systems, policies and procedures to identify areas of improvement
- ☐ Develop and regularly test a response plan for disaster recovery, business continuity and incident response that includes defined responsibilities and notification procedures

Additional Key Measures to Mitigate Risk:

- ☐ Review your **Business Insurance Coverage** and ask about specific coverage for data breaches, system failures and intellectual property rights.
- ☐ Implement a "clean desk" policy that ensures all sensitive internal and customer information is securely filed.
- ☐ Be selective with your business partners, particularly those who may have access to sensitive information, e.g. accounting firms, check printing companies, document storage facilities, online/cloud based services, etc.
- ☐ Remove signatures of executives and other key personnel from public documents, annual reports, customer notifications, social media, etc. to prevent illegal signature scanning and use

Fraud Prevention Services

First Commonwealth offers a variety of services to compliment your overall fraud prevention program.

Online Treasury Management and Mobile Treasury Management
Single point of access to help your business manage accounts, manage working capital, originate payments and monitor your account activities.

Account Reconcilement Plans
Detailed reporting to help reconcile payments and deposits against your account. Account Reconcilement is often paired with Check Positive Pay to maximize fraud protection.

Check Positive Pay
Monitor your check disbursements and identify suspect check items by providing a list of check items that First Commonwealth will match against items presented for payment.

ACH Filter
Reduce the risk of unauthorized ACH debits and potential payment fraud by allowing you to review and make payment decisions on ACH transactions that don't meet your pre-established criteria

Debit Block
Block all ACH debits against your account so that any ACH debits are automatically returned to the originating bank

What to Do If You Suspect Fraud

If you suspect you have experienced fraud, there are important some steps you can take to help mitigate any future risk.

- ☐ Contact First Commonwealth's Treasury Management Department at **724-463-5857**
- ☐ Contact your law enforcement agencies
- ☐ File a complaint, regardless of monetary loss, at IC3.gov
- ☐ Enroll in First Commonwealth's Fraud Protection services
- ☐ Consider changing your account numbers
- ☐ Consider updating system credentials and user/ID passwords for your banking applications

WE ARE HERE TO HELP

First Commonwealth is here to help you build for the long term by bringing you solutions, resources, and expertise that help your business succeed. To learn more about how we can bring ideas, insight and solutions together to grow your business, please contact your Treasury Management Officer or visit us online at https://www.fcbanking.com/business/treasury-management-solutions/