First Commonwealth Bank
Time to be first.



FRAUD MITIGATION & PROCEDURAL PROCESSES TO MITIGATE RISK

KATE NELSON - TREASURY MANAGEMENT CONSULTANT

BRETT CUNNINGHAM - TREASURY MANAGEMENT CONSULTANT

BRETT CUNNINGHAM

TREASURY MANAGEMENT CONSULTANT

EXPERIENCE

- Treasury Management Consultant serving Middle Market Companies in Northern Ohio for 10+ years. Experience with companies as large as $500M to $1B and assisting with all a wide range of Treasury Management solutions & integrations.
- Strategic advisor for complex solutions such as Payment Manager, Receivables Manager, Cash Flow Analysis, lockbox, safe vantage and many more.
- Consultant and advocate for optimal procedures to mitigate all types of risk to companies. Knowledgeable on current fraud trends, services, and awareness that threaten the landscape today.

KATE NELSON

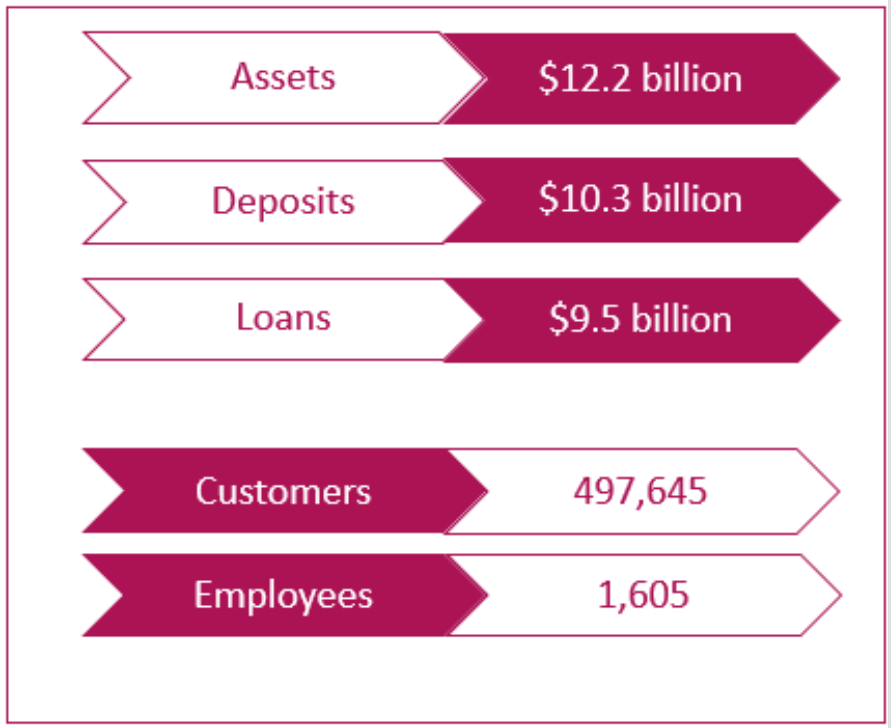
TREASURY MANAGEMENT CONSULTANT

Experience

- 26 years of banking experience
- 16 years dedicated to Treasury Management
- Supports the depository and electronic banking needs of public entities, and business clients throughout Ohio
- Serves a diverse client base, including Counties, Cities, Municipalities, School Districts, Libraries, and Sewer & Water Authorities
- Provides treasury management expertise to middle market, commercial real estate, and small business clients

FIRST COMMONWEALTH BANK

CORPORATE PROFILE



WHO WE ARE

First Commonwealth Financial Corporation (NYSE: FCF), currently has 126 community banking offices in 30 counties throughout western and central Pennsylvania and throughout Ohio, as well as commercial lending operations in Pittsburgh, Pennsylvania, and Canton, Cleveland, Columbus and Cincinnati, Ohio.

WHY WE EXIST

To improve the financial lives of our neighbors and their businesses.

COMMUNITY INVOLVEMENT

In 2022, we provided more than $51 million in Community Development Investments, nearly 600 hours of financial education classes in our communities and 11,000 employee volunteer hours. We also provided $467 million in mortgage loans including $17 million in First@Home loans, making homeownership possible for more of our neighbors

DIVERSITY

We are on a journey to build a diverse workforce and an inclusive work environment. We value the perspectives of every one of our employees with intentional care given to those who might feel less represented based on their gender, race, age, abilities, sexual orientation and life experiences. Our company is more diverse today than a year ago, and our commitment is to keep getting better for ourselves, our partners and our communities.

WE APPRECIATE YOUR PARTNERSHIP

We are committed to helping you achieve your goals and will work hard to earn your trust. We are excited for the opportunity to continue to build upon our partnership to ensure your continued financial success.



2025 PBC Top 100 Organizations



AGENDA

- **FRAUD TRENDS**
  - 2026 AFP SURVEY RESULTS
- **MITIGATING RISK**
  - INTERNAL CONTROLS/PROCESS
  - CUSTOMER & VENDOR HANDLING
  - INTERNAL BUSINESS PROCEDURES
  - BANK OFFERINGS
- **BEST PRACTICES**

TYPES OF FRAUD



CHECK FRAUD

Any efforts to obtain money illegally using paper or digital checks.



BUSINESS EMAIL COMPROMISE (BEC) & MASQUERADING

This technique is employed to assume control of a C-level executive's email address to con lower-level employees and/or even banking staff into scheduling fraudulent wires. And while these attacks are waged against a banking institution's commercial customers, not the institution itself, banking institutions should be on high-alert for this emerging scheme.



ACH FRAUD

When an account is accessed for unauthorized ACH payments or withdrawals.



WIRE FRAUD

Financial fraud involving the use of telecommunications or information technology.



SPIDERWARE

Software program that travels the web locating and indexing websites for search engines.



SPYWARE

Spyware can capture information like Web Browsing habits, e-mail messages, usernames and passwords and credit card information. The software can then transmit to another person's computer using the internet.



MALWARE

Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.



RANSOMWARE

Ransomware is a form of malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment.



VOICE-PHISHING/VISHING

Scams happen over the phone, voicemail or VoIP (Voice over Internet Protocol) calls. Computer systems
can create audio that sounds like a particular person speaking, giving the impression that a trusted individual is making a request.

ADDITIONAL RESOURCES

https://blog.totalprosource.com/5-common-malware-types

https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/spoofing-and-phishing

https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html

MARKET FACTORS: FRAUD & RISK MITIGATION

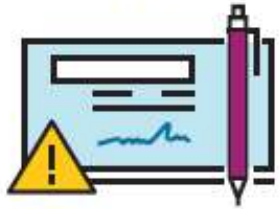
KEY FINDINGS

Adoption of AI for fraud prevention remains limited, despite recognized benefits



Few organizations (17%) report using AI to combat payments fraud. While adoption is higher among large organizations – i.e., those with annual revenue of at least $1 billion – most respondents cite immaturity of technology, cost and reliance on existing controls or banking partners as reasons for limited use, despite reported benefits such as improved detection and efficiency.

Checks continue to be the payment method most frequently impacted by fraud



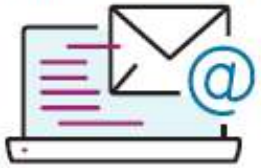
Despite declining fraud activity via their use, checks continue to be the most-often targeted method for fraud, reported by 58% of organizations in 2025 – outpacing fraud via ACH debits (30%) and wire transfers (25%). Check usage continues to be widespread; 68% of companies use checks for vendor payments because vendors require payment via checks. That is a 16% increase from 2024. Nearly three-quarters (72%) of organizations plan to continue using checks for the foreseeable future.

Payments fraud remains widespread; over three-quarters of surveyed organizations experienced either attempted or actual fraud attacks in 2025



Payments fraud remains widespread; over three-quarters of surveyed organizations experienced either attempted or actual fraud attacks in 2025

Business email compromise (BEC) is the most prevalent fraud vector



BEC affected 74% of organizations in 2025, representing a significant increase from 2023 and 2024. Fraudsters primarily impersonate vendors or executives to request changes to payment instructions, making email the dominant channel for payments fraud regardless of organization size. Additionally, 39% of organizations continue to receive genuine emails that have been intercepted by fraudsters.

Treasury plays a central role in payments fraud detection, reporting and recovery



Treasury is most frequently cited as the business unit discovering both attempted fraud (83%) and actual fraud (55%), underscoring its critical risk management role in monitoring bank activity, managing controls and coordinating recovery efforts – often in close collaboration with Accounts Payable and banking/vendor partners.

Payments fraud impacts U.S. businesses of all revenue categories with varying consequences



Nearly half of organizations (48%) with annual revenue less than $1 billion that experienced payments fraud in 2025 incurred a loss, and 24% of these companies were unsuccessful in recouping any funds lost. Two-thirds (66%) of larger organizations with annual revenue of at least $1 billion faced a financial loss due to fraud, and 19% were unable to recoup funds lost.

Smaller organizations experience payments fraud less frequently, but when fraud succeeds, they are far more likely to absorb the full financial loss. While larger organizations face more frequent attacks, they recover those losses more effectively due to stronger detection, escalation and recovery infrastructure.

Source: 2026 AFP Payments and Fraud Control Survey Report

MARKET FACTORS: FRAUD & RISK MITIGATION

PAYMENT METHODS IMPACTED BY FRAUD

Checks and ACH Debits Remain Most Susceptible to Payments Fraud

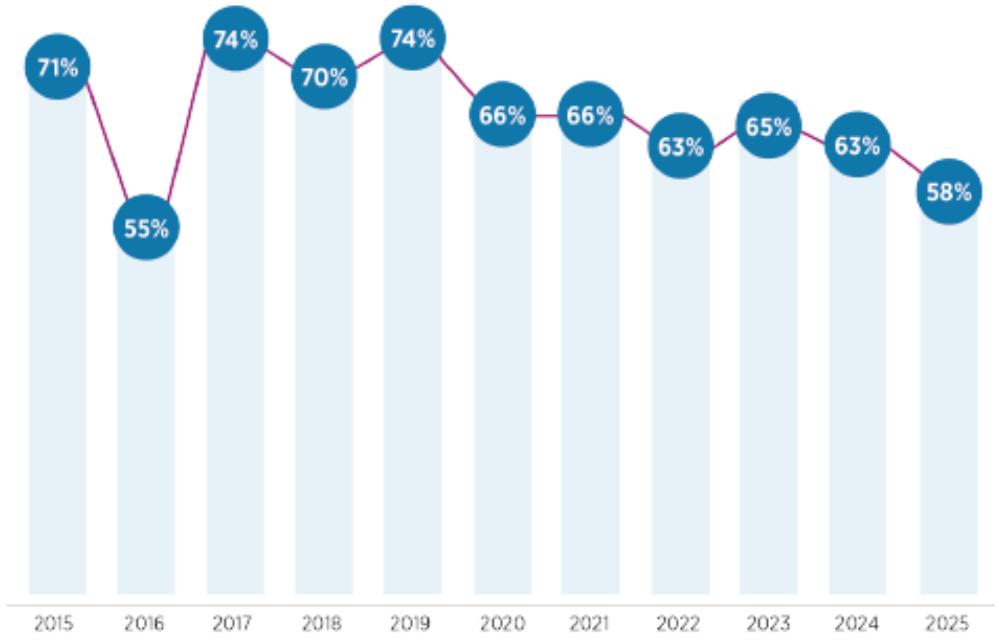
In 2025, checks and ACH debits remained the payment methods most impacted by fraud activity. Checks were the most frequently reported payment method subject to fraud (58% of organizations), followed by ACH debits (30%) and wire transfers (25%). Corporate/commercial credit cards (21%) and ACH credits (18%) accounted for a secondary tier of exposure, while newer or less widely used methods such as faster payments (1%), cryptocurrency (1%), and mobile wallets (2%) were cited less often.

Differences in fraud exposure are seen when considering organizational revenue. Organizations with annual revenue of at least $1 billion experienced a higher incidence of fraud for all payments methods (except for virtual cards) than organizations with annual revenue less than $1 billion.

Fraud involving ACH debits (reported by 30% of organizations) and wire transfers (25%) declined year-over-year, Wire transfers continued to be disproportionately targeted at larger organizations, particularly those with more than 100 payment accounts. Lower value and emerging payment methods – such as corporate cards, virtual cards, mobile wallets, and cash – remained comparatively infrequent targets.

The 10-year trend shows an overall decline in check fraud activity. Over the past decade, payments fraud via checks has trended downward, albeit with some bumps along the way. The decline observed in recent years is likely due to a reduction in the number of checks issued, as organizations increasingly adopt digital payment methods. Still widespread, the use of checks continues to represent the primary area of fraud vulnerability for organizations; this year's survey results reveal that over 87% of organizations use checks. Even as fraudsters adopt new technologies, the continued use of paper checks sustains long-standing fraud schemes. Mail-theft-enabled check fraud is a large persistent problem.

Check Fraud Activity: Trends
(Percent of Organizations)



Source: 2026 AFP Payments and Fraud Control Survey Report

MARKET FACTORS: FRAUD & RISK MITIGATION

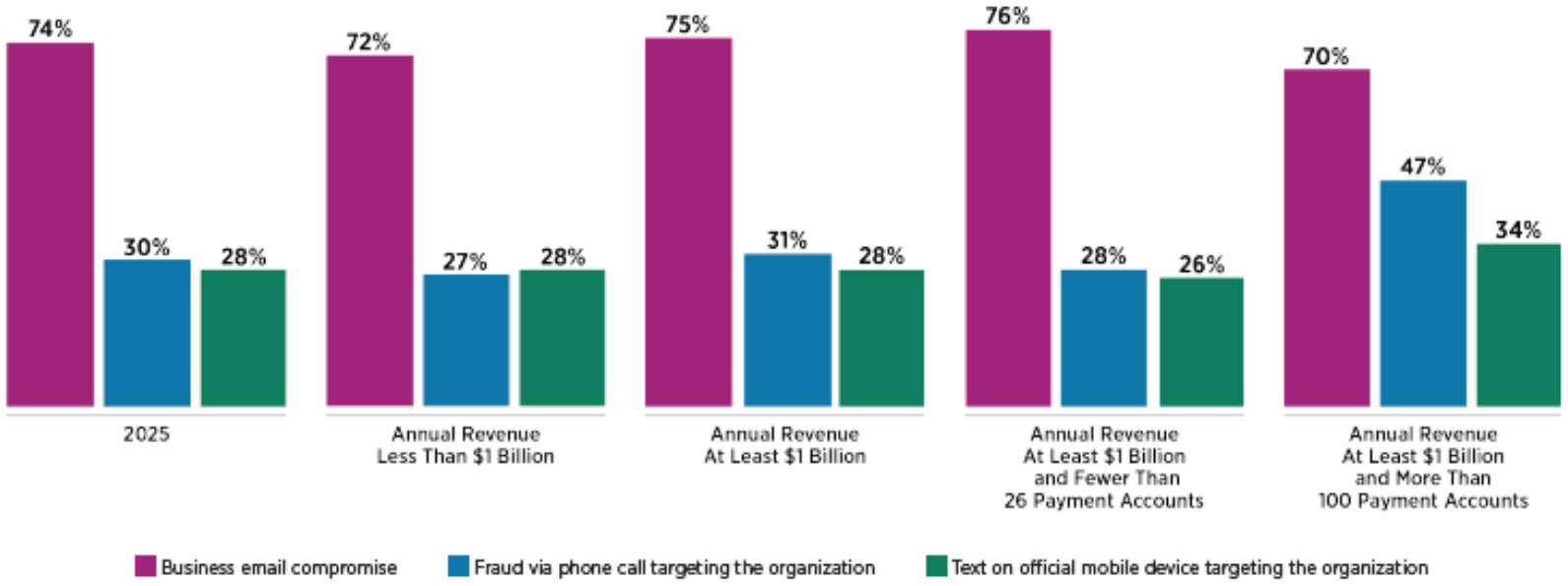
IMPACT OF TYPES OF IMPOSTER FRAUD

Business Email Compromise (BEC) Used Frequently by Imposters

Imposter fraud occurs when a criminal impersonates a trusted individual or entity – such as a company executive, vendor or government agency – to deceive employees and manipulate them into making unauthorized payments or sharing sensitive information. These schemes often use emails, phone calls or texts that appear legitimate in order to trick victims into complying with fraudulent requests. Recognizing and verifying communications before taking action is essential in preventing imposter fraud.

In 2025, nearly 75% of organizations experienced email or BEC fraud, 30% were targeted by fraudulent phone calls, and 28% received scam texts on company mobile devices. Organizations with at least $1 billion in annual revenue and more than 100 payment accounts report higher rates of phone and text fraud targeting their payment systems compared to others.

Types of Fraud Attacks Experienced by Organizations in 2025
(Percent of Organizations Experiencing Payments Fraud)



Source: 2026 AFP Payments and Fraud Control Survey Report

MARKET FACTORS: FRAUD & RISK MITIGATION

PAYMENT METHODS USED IN IMPOSTOR SCAMS

Business Email Compromise

Various payment methods continue to be vulnerable to BEC; 49% of fraud via email in 2025 were made using wire transfers, a decline from 63% in 2024, but higher than in 2023 and 2022. About one-third of organizations reports that the payment methods used by fraudsters were ACH debits (34%), checks (33%). The use of ACH credits for BEC, at 31%, is significantly lower than the 50% reported last year. For a third consecutive year, real-time payments were one of the payment methods impacted by BEC. Overall, 6% of respondents indicate real-time payments were targeted via BEC.

Telephone Calls

Fraudsters mainly used checks (40%) in phone scams, with wire transfers (35%) and ACH credits (33%) close behind.

Fraud Via Text (Mobile Devices)

Few organizations report payments were made through fraudulent texts, but checks, ACH credits and gift cards were the second most-common methods used in fraud in 2025.

Payment Methods Utilized in Fraud Attacks via Email, Telephone Calls and Text Messages
(Percentage Distribution of Organizations Experiencing Payments Fraud)

	BUSINESS EMAIL COMPROMISE		FRAUD VIA TELEPHONE CALL TARGETING ORGANIZATION	FRAUD VIA TEXT ON OFFICIAL MOBILE DEVICE
	2025	2024	2025	2025
Wire transfers	49%	63%	35%	20%
ACH debits	34%	26%	27%	20%
Checks	33%	26%	40%	30%
ACH credits	31%	50%	33%	30%
Corporate/commercial credit cards (e.g., purchasing, T&E, Fleet)	10%	11%	17%	35%
Third-party payouts (e.g., Venmo®, PayPal®, Zelle®, etc.)	7%	9%	17%	20%
Real-time payments (RTP®, FedNow®)	6%	3%	10%	10%
Gift cards	6%	6%	13%	30%
Cash	6%	8%	10%	15%
Cryptocurrency (Bitcoin, Ethereum®, etc.)	2%	3%	8%	15%
Virtual cards	2%	–	13%	35%

Source: 2026 AFP Payments and Fraud Control Survey Report

MARKET FACTORS: FRAUD & RISK MITIGATION

SOURCES OF FRAUD

Sources of Attempted/Actual Payments Fraud Attempts
(Percent of Organizations Experiencing Payments Fraud)

	2025	ANNUAL REVENUE LESS THAN $1 BILLION	ANNUAL REVENUE AT LEAST $1 BILLION	ANNUAL REVENUE AT LEAST $1 BILLION AND FEWER THAN 26 PAYMENT ACCOUNTS	ANNUAL REVENUE AT LEAST $1 BILLION AND MORE THAN 100 PAYMENT ACCOUNTS
Business email compromise (BEC)/Fraudulent email	70%	72%	75%	76%	70%
External individual using tactics other than email (e.g., forged checks, stolen cards, identity fraud)	51%	51%	52%	53%	47%
Manipulated ACH or wire transfer instructions	33%	33%	34%	35%	29%
Invoice fraud	26%	26%	26%	20%	40%
U.S. Postal Service office interference	20%	20%	20%	20%	16%
Imposter to a client posing as representative from your company	17%	12%	20%	21%	18%
Unknown or undetermined source	14%	14%	14%	16%	11%
Fraud via spoof/spam text on official mobile devices or fraudulent QR code	13%	15%	12%	10%	24%
Third-party or outsourcer (e.g., vendor, professional services provider, business trading partner)	13%	10%	14%	10%	33%
Fraudulent live phone calls on organization's phone/mobile lines.	8%	6%	10%	6%	13%
Account takeover via system breach or malware (e.g., spyware, social network-based attacks)	8%	7%	10%	9%	4%
Fraud via gateway credentials (fake messages are either emailed or texted impersonating a bank, to trick individuals to provide login credentials on a fake website)	8%	6%	10%	7%	18%
Deepfake attempt (e.g., voice and/or video swapping, "deep voice" technology, vishing)	7%	5%	8%	6%	13%
Organized crime ring (e.g., crime spree that targets other organizations in addition to your own, either in a single city or across the country)	5%	3%	6%	7%	4%
Ransomware	5%	7%	3%	2%	7%
Internal party (e.g., malicious insider)	3%	2%	4%	4%	4%
Other	8%	9%	7%	6%	9%

Other includes:
- Check-related fraud
- Credit card fraud
- Counterfeit currency

Source: 2026 AFP Payments and Fraud Control Survey Report

MITIGATING RISK

Internal Processes

- Separation of Duties
- AR & AP

Account Change & Payment Change

- Process around changing customer information and securely confirming request prior to change

Customer Information

- Housing Customer Information
- Clear Processes
- Payments, Account Changes, Transfers

Enterprise Visibility

- Reports, Cash Positioning, Card Holders
- User Access/Responsibility
- User add/change/delete

Approval Levels

- Clear process around approvals
- ACH Fraud Monitoring Attestation
- Acknowledgement of Certain Requirements for ACH Origination Services

MITIGATING RISK

Positive Pay

- Is a fraud-prevention service that helps protect organizations from unauthorized or altered checks before the item is paid.
  - Matches presented checks to issued-check records
  - Flags discrepancies for review
  - Allows the organization to approve or return exceptions
  - Helps prevent unauthorized check payments

ACH Filters

- Is a fraud-prevention service that helps protect organizations from unauthorized ACH transactions
  - Screens incoming ACH payments (debits) against approved criteria
  - Flags unauthorized or suspicious transactions
  - Provides control over which payments are processed
  - Helps reduce ACH fraud risk

ACH Block

- Is a fraud-prevention service that protects organizations accounts by stopping unauthorized ACH payments (debits) before funds leave the account
  - Prevents unauthorized ACH payments (debits) from posting
  - Adds an extra layer of account protection
  - Helps reduce exposure to ACH fraud

Dual Control

- Adds an extra layer of protection and reduces the risk of internal and external fraud by requiring two-person authorization
  - Requires two people to initiate and approve transactions
  - Separate key responsibilities to reduce errors and fraud
  - Provides greater oversight of high-risk activity

MITIGATING RISK

Multi-Factor Authentication (2FA)

- An additional layer of security designed to keep information safe. 2FA takes away the fraudsters ability to guess answers to security questions and helps to ensure only established online banking users are getting access by confirming the user's identity using a second step (such as a code or prompt) when signing in.

Passkey

- Is a password free sign in using secure, device stored credentials for stronger security and a smoother login experience

FIDO

- Allows you to securely sign in using a security key or biometric method, such as fingerprint, PIN, or facial recognition

Alert Notifications

- Delivers critical, real-time visibility to help detect potential fraud the moment it happens
  - Receive immediate alerts for suspicious activity
  - Identify unauthorized activity quickly
  - Take action before fraudulent activity results in losses

FRAUD MITIGATION BEST PRACTICES

First Commonwealth Bank is committed to helping clients reduce the risks associated with fraud that can contribute to financial loss. There are common best practices that can help reduce risk exposure. We strongly recommend that you review and implement the following policies and controls.

GENERAL BANKING

- Review your bank accounts daily to identify any unusual or unknown transactions.
- Use positive pay on all accounts with check writing and issuance privileges.
- Use ACH blocks and filters to monitor transactions and block or restrict debit activity.
- Eliminate paper and access bank account information and statements online.
- Separate bank account reconciliation and reporting functions from payment initiation and management.
- Ensure corporate resolutions, authorized signatures, and other banking agreements are current.

GENERAL WORKPLACE

- Keep all IDs, passwords, security codes and cards safe and secure, and do not allow employees to share them.
- Store financial information in a secure area with restricted access and dispose of unused and outdated documents properly.
- Establish a company security policy for all areas including computers and physical building security.
- Implement a third party or independent review and audit system.
- Know your customers, vendors and business partners, and have contracts and controls in place.
- Know your employees; perform background checks; and always verify employee access to information.

INTERNET SECURITY BEST PRACTICES

First Commonwealth Bank recommends the follow strategies to best safeguard your accounts from online fraud.

- Perform or initiate all online banking activities from a stand-alone, completely locked down computer system from which email is not accessed and web browsing is restricted to online banking activities.
- Use dual control to initiate and approve wire transfers and ACH transactions.
- Change passwords frequently.
- Use complex passwords (minimum eight characters, containing upper and lowercase letters, numbers, and special characters).
- Do not use the same password for all applications.
- Do not open unsolicited emails.
- Do not open attachments or click on links in unsolicited emails.
- Do not open or execute files from untrusted sources.
- Educate your employees on your corporate security policy.
- Be continuously vigilant for social engineering attempts at fraud.
- Make sure your desktop anti-virus/malware software is current and is configured to receive signature updates frequently and automatically.
- Configure your desktop anti-virus/malware software to continuously scan automatically in the background (real-time scanning).
- Configure your desktop anti-virus/malware software to run frequent full scans on all disk drives.
- In case of infection, see your anti-virus vendor for instructions.
- Install application and operating system patches regularly.
- Practice security in layers by using:
  - Anti-virus/malware/spam software at the desktop.
  - Anti-virus/malware software at the server.
  - Anti-virus/malware/spam software for email.
  - Anti-virus/malware/web filtering software for

First Commonwealth Bank
Time to be first.

APPENDIX

CONTACT INFORMATION

First Commonwealth works with you to know your business and proactively provide unique opportunities to help you improve your business' success.

KATE NELSON *Treasury Management Consultant*

740-657-7468 740-564-9487 KNelson@fcbanking.com

BRETT CUNNINGHAM *Treasury Management Consultant*

216.299.5082 Bcunningham@FCBanking.com

First Commonwealth Bank®

Time to be first.™

fcbanking.com

MEMBER FDIC

OUR MISSION:

To improve the financial lives of our neighbors and their businesses.