Huntington Bank

IN CPA Society NFP Conference

Presented By: Penelope (Penny) Lewis

Date: July 23, 2026

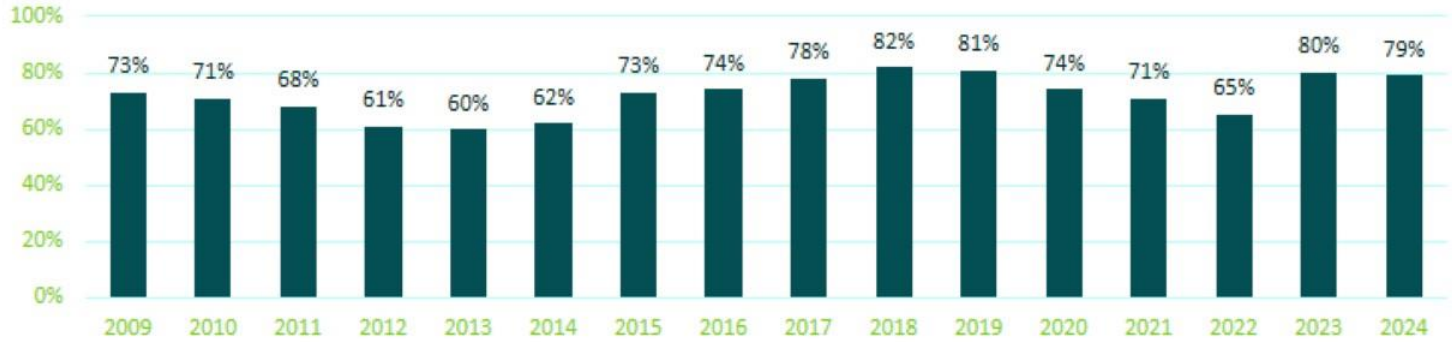
Huntington Bank

FRAUD PROTECTION

Fraud Mitigation

Fraud mitigation should be viewed as an integral part of an overall business continuity strategy

Percentage of Organizations that were Victims of Actual/Attempted Fraud 2009-2024*



WHO IS AT RISK?

No organization is immune.

According to the latest Association for Financial Professional's Payments Fraud and Control survey Report, 79% of organizations cited having been targets of payments fraud activity.

WHY DOES IT MATTER?

The potential financial loss from payment fraud can create a serious hardship. Fraud can expose confidential information — impacting an organization's reputation and putting employees at risk.

Companies cannot be complacent in their efforts to manage and mitigate payment fraud.

The most important step is to create a plan.

* Association for Financial Professionals. AFP Payments Fraud and Control Survey Report.

Protecting Against Business Email Compromise (BEC)

Monitor Payment Methods & Changes

- **Businesses don't change their banks often; Be mindful of any requests to change payment institution, payment account, or payment type**
- Avoid using paper checks by using ACH or other electronic payment methods when possible

Follow Established Protocols

- **Verify contact information by phone if you receive a change notification**
- Use dual authentication/approvers
- Never call phone numbers or reply to email addresses sent in suspicious emails or texts
- Confirm any notifications of new payment information with a known contact at the recipient

Treat Emails With Caution

- **Use a secure email solution, monitor message change notifications**
- Avoid clicking suspicious links and report them promptly

Act Quickly

- **Trust your instincts; If something feels off, it probably is**
- In the event of an incident, move fast to promptly report it to the appropriate team or organization

Huntington Bank

Preventing Business Email Compromise (BEC) Scams

Business email compromise (BEC) is a sophisticated phishing attack that targets individuals, businesses, and organizations.

Fraudsters use a variety of techniques to convince an email recipient that a message is coming from a legitimate and trusted source.

These messages often mimic previous emails sent from a known party and exploit existing trusted relationships, making them difficult to identify – and resulting in over $2.7 billion in losses last year. *

How are you staying vigilant against BEC?

*FBI Internet Crime Complaint Center (IC3). 2024. « Federal Bureau of Investigation Internet Crime Report 2024. Accessed July 28, 2025. https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

How to Help Protect Against Data Breaches

Avoiding a security incident or breach altogether is ideal. However, current trends indicate that it is likely not a matter of if, but when. It is nearly impossible to try to prevent every type of attack, so focusing on risk management is key to success.

Companies should use risk management to align focus on strengthening and hardening their security hardware, software, standards, and policies, and developing an Incident Response plan.

If faced with a data breach, how confident are you that your current risk management strategy positions your organization to recover financially, operationally, and reputationally?

How to Build an IT Resiliency Plan for Your Business

The National Institute of Standards and Technology developed a framework for protecting critical infrastructure against natural and cybersecurity risks, including the following pillars*:

IDENTIFY

Consider data and assets at your company that could be at risk.

PROTECT

Train employees on safety issues, backing up data, and email security best practices.

DETECT

Set up systems to detect an intrusion into your system and integrate checks and balances into all processes.

RESPOND

Be prepared to assess your response once the crisis has been resolved and to refine your plan for future disasters or interruptions to operations.

RECOVER

Once you've created a plan and are confident it covers every contingency, the final step is to bring in an outside expert to conduct an audit of your plan.

*Framework for Improving Critical Information Cybersecurity. National Institute of Standards and Technology, United States Department of Commerce. More details available at https://www.huntington.com/Commercial/insights/cybersecurity/business-resiliency

Password Security Best Practices to Help Defend Your Data

Passwords are your first line of defense against cybercriminals and data breaches. Strong password management practices can help keep your organization safe.

1. Create a strong culture of security by implementing routine cybersecurity awareness training for all employees, regardless of their role's access to company systems.
2. Consider using a passkey that leverages more secure and convenient methods of authentication and allows users to bypass usernames and passwords entirely.
3. Remain vigilant against phishing attacks and train employees on how to recognize suspicious emails attempting to get them to reveal sensitive information.
4. Review account activity where possible and report any suspicious activity. For example, if you receive a prompt to complete a multi-factor authentication (MFA) activity you did not initiate, change your password immediately.
5. Stay on top of software and device vulnerabilities. Running older versions of software and operating systems opens you up to vulnerabilities that could compromise sensitive data – like your passwords.

Developing a comprehensive expense policy is crucial to establishing a strong foundation for preventing credit card misuse.

Commercial credit card data is typically stolen through merchant compromise. Once stolen, data is sold to create counterfeit cards or make online purchases. For companies, this can be particularly devastating, as commercial cards often have high limits.

Huntington Bank

How to Help Prevent Company Credit Card Misuse

Help manage spending and reduce misuse with these commercial card control measures:

Transaction limits: Assign individual or cardholder group spending limits based on job roles and responsibilities. These can include amount of a single purchase, amount spent each day or month, and transactions allowed each day or month.

Merchant category limits: Limit the type of merchant groups, ranges, and codes where the corporate credit card can be used. For example, you can limit transactions to travel merchants for plane tickets, car rentals, or hotels.

Receipt requirements: Require employees to submit receipts, including a scanned image or copy of the receipt, for expenses made with their corporate credit card to ensure transparency and accountability. You could require receipts for all expenses or only those over a set dollar amount.

More details available at https://www.huntington.com/Commercial/insights/cybersecurity/prevent-commercial-card-fraud

Business Security Checklist

Strong security doesn't happen alone. It's something we build together. This practical checklist can help your business stay ahead of fraud, strengthen your defenses, and enhance payment security.

CHECKS, ACH & WIRE

- ❑ Regularly review your list of authorized personnel accessing your bank accounts, especially those with check issuance, ACH initiation, wire initiation and approval access
- ❑ For consistency and increased transparency to errors and/or fraud, implement and utilize:
  - ❑ Check Positive Pay fraud protection services with teller line protection and payee positive pay
  - ❑ ACH Positive Pay
  - ❑ Wire-transfer templates or block wire debits
  - ❑ Use dual authentication and approvers
- ❑ Always verify changes to payment instruction:
  - ❑ Businesses don't change their banks often; Be mindful of any emails requesting to change payment account or institution
  - ❑ Never call or click on details presented in a change request
  - ❑ Confirm updates with a known contact at the recipient
- ❑ Introduce stale-date and maximum dollar threshold protocols for check items to help ensure only intended payments are processed
- ❑ Establish transfer limits for all wire transactions
- ❑ Diligently monitor the account for all non-standard check, ACH, and wire transaction activity
- ❑ Reconcile your account regularly to ensure correct transactions are posting

CARD ACCEPTANCES

- ❑ Implement tokenization and encryption security for terminal or web-based transactions
- ❑ Adopt and utilize EMV card capabilities
- ❑ Establish a Payment Card Industry Data Security Standard (PCI DSS) compliance and annually complete PCI DSS Self-Assessments to identify gaps

Business Security Checklist

CONDUCTING ONLINE BUSINESS

Strengthen your cybersecurity defenses by:

- ❑ Prioritizing incident response planning that includes data recovery
- ❑ Managing vulnerabilities by keeping all systems and applications updated; ensure antivirus, malware protection and email security software are active
- ❑ Reduce or eliminate vulnerable connection methods into your network
- ❑ Employ identity and access management (IAM) policies
- ❑ Protect your network by using a secure firewall; Monitor VPN connectivity and maintain anti-virus and anti-spyware solutions

Develop or deepen a strong security culture by:

- ❑ Implementing cybersecurity training program for employees, and communicate to employees about common threats and best practices for protecting against them
- ❑ Evaluating a cyber liability insurance policy to provide first and third-party coverage for damages when private, personal, and financial information is compromised due to a data breach or network intrusion

MALWARE, RANSOMWARE, OR MALICIOUS SOFTWARE

- ❑ Be diligent in protecting login information
- ❑ Use computers and networks that are secured by firewalls and anti-virus software
- ❑ Be wary of clicking on suspicious emails, attachments, and links to websites
- ❑ Hover on a link before clicking to see if the website address is as expected
- ❑ Ensure that virus scans and network security methods are updated
- ❑ Do not respond to unsolicited requests for information and use caution before giving out information either online or over the phone

Business Security Suite

Our payment and fraud mitigation tools are designed to make it easier for you to monitor your payments so you can stay a step ahead of threats to your business's finances.

FEATURE	BENEFIT
ACH Positive Pay	Protection by placing filters and/or blocks on ACH transactions. Only electronic payments that meet personalized criteria will be processed.
Check Positive Pay	Early detection of fraudulent, altered, or counterfeit checks by verifying items presented against a check issue file. Exception or non-matching items are referred to the client for review and decisioning via Business Online.
Reverse Positive Pay	Review daily exceptions on one screen and decide to pay, return, or pay but correct. This allows the monitoring of checks posting to the account without uploading a file.
Check Block	Protects against fraudulent checks posting to the account by transforming into an electronic only account. All paper-based debits will be blocked.
Wire Block	The ability to manage wire transfer activity by blocking all incoming and/or outgoing wires on an account depending on business needs.

Your Dedicated Huntington Relationship Team is comprised of multiple experienced professionals working together to assist you in accomplishing all your personal and professional financial goals.

Penelope Lewis

Regional Banking Relationship Manager

Penny.Lewis@huntington.com

(317) 201-3419

Jessica Walker

Treasury Management Advisor

Jessica.Walker1@huntington.com

(317) 269-4687

Huntington Bank

THANK YOU

Disclosures

These materials have been prepared by The Huntington National Bank (HNB) and are provided for informational or illustration purposes only. Nothing herein shall be construed as an advertisement or offer to buy or sell any Huntington product, nor shall the information be considered advice or a recommendation to enter into or refrain from any transaction. Any statements, including opinions and recent quotations on rates and products, are subject to change without notice. The content presented within this material is based upon information that HNB believes is reliable, but HNB does not warrant its completeness or accuracy, and it should not be relied upon as such. Additional information to what is presented in this material can be made available upon request. HNB does not provide accounting, legal, or tax advice; you should consult with your accounting, legal, or tax advisor(s) on such matters. HNB is a wholly-owned subsidiary of Huntington Bancshares Incorporated.

HNB and its affiliated companies, and their respective directors, officers, and employees, expressly decline and are not responsible for any liability for loss or damage whatsoever caused by or related to the use of information contained in these materials.

Lending and leasing products and services, as well as certain other banking products and services, may require credit approval.

Huntington Capital Markets® is a federally registered service mark and a trade name under which investment banking, securities underwriting, securities sales and trading, foreign exchange and derivatives services of Huntington Bancshares Incorporated and its subsidiaries, Huntington Securities, Inc. and The Huntington National Bank, are marketed. Securities products and services are offered by licensed securities representatives of Huntington Securities, Inc., registered broker-dealer and member, FINRA and SIPC. Banking products and services are offered by The Huntington National Bank, Member FDIC.

Capstone Partners is a trade name under which financial advisory and certain investment banking services of Huntington Bancshares Incorporated are marketed. Securities products and services are offered by licensed securities representatives of Capstone Capital Markets LLC, registered broker-dealer and member, FINRA and SIPC.

Huntington Insurance, Inc.
Insurance products are offered by Huntington Insurance, Inc., a licensed agency and a wholly-owned subsidiary of Huntington Bancshares Incorporated and underwritten by third party insurance carriers not affiliated with Huntington Insurance, Inc.

HBI Title Services, Inc.
Title Insurance products are offered by HBI Title Services, Inc., a subsidiary of Huntington Bancshares Incorporated and a licensed title agency authorized to sell title insurance in the following states – CO, FL, IL, IN, KY, MI, MN, OH, PA, SD, TN, WI and WV.

Huntington Private Bank®
Huntington Private Bank® is a team of professionals dedicated to delivering a full range of wealth and financial services. The team is comprised of Private Bankers, who offer premium banking solutions, Wealth and Investment Management professionals, who provide, among other services, trust and estate administration and portfolio management from The Huntington National Bank, and licensed investment representatives of The Huntington Investment Company, which offers securities and investment advisory services. Huntington Private Bank® is a federally registered service mark of Huntington Bancshares Incorporated.

Trust and investment management services are provided by The Huntington National Bank, a national bank with fiduciary powers.

Huntington Financial Advisors®
Huntington Financial Advisors® is a federally registered service mark and a trade name under which The Huntington Investment Company offers securities and insurance products and services. The Huntington Investment Company is a registered broker-dealer, member FINRA and SIPC, and registered investment adviser with the U.S. Securities and Exchange Commission (SEC). The Huntington Investment Company is a wholly-owned subsidiary of Huntington Bancshares Incorporated.

Investment, Insurance and Non-Deposit Trust products are: NOT A DEPOSIT • NOT FDIC INSURED • NOT GUARANTEED BY THE BANK • NOT INSURED BY ANY FEDERAL GOVERNMENT AGENCY • MAY LOSE VALUE

Fraud Protection & Mitigation (Accounting Perspective)

July 23, 2026

Indiana CPA Society Not-for-Profit Conference

Cherry Bekaert

Your Guide Forward

Agenda

- Fraud in Accounting
- Fraud Triangle
- Why Internal Controls Matter
- Segregation of Duties
- Approval and Authorization Controls
- Reconciliation and Monitoring Controls
- Access Controls and Technology Safeguards
- Fraud Awareness and Ethical Culture
- Summary

Fraud in Accounting

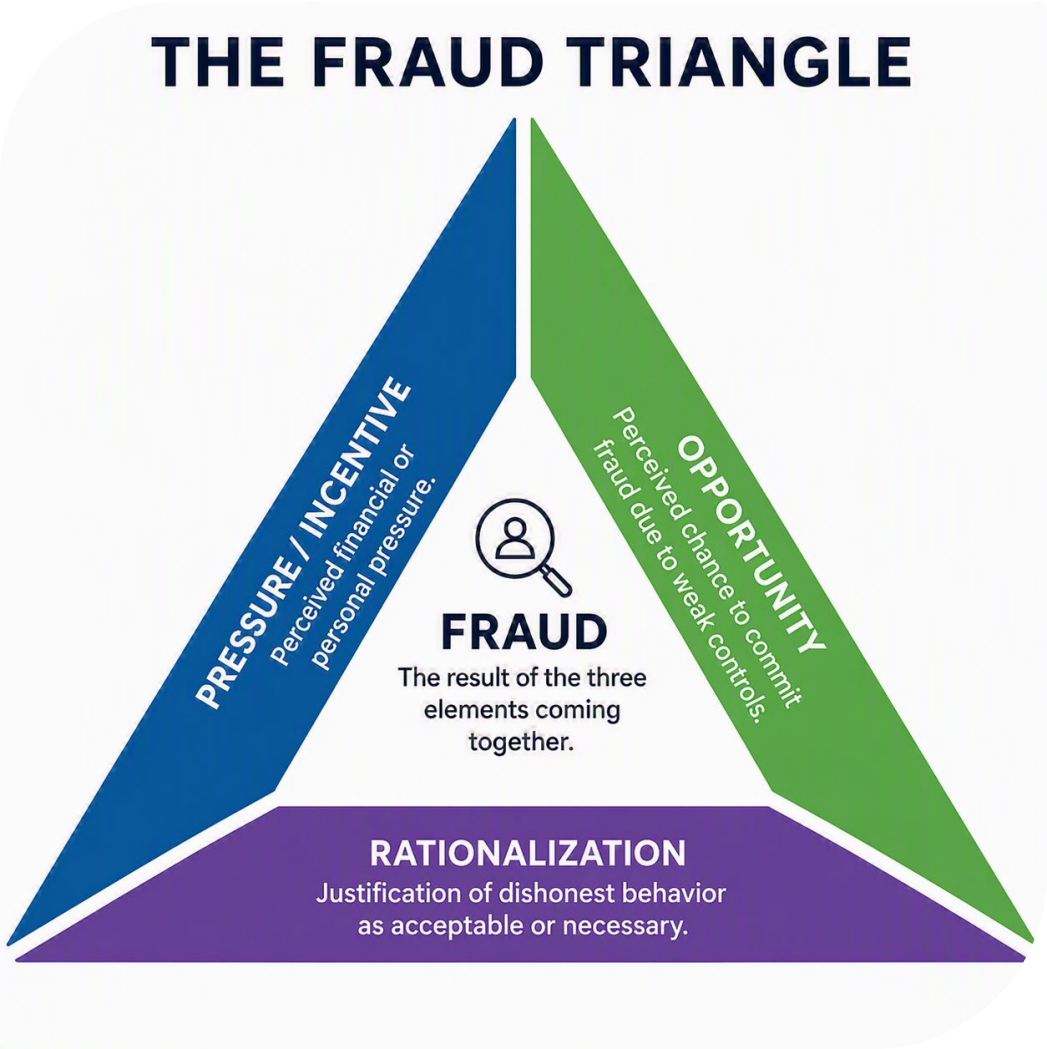
- Misappropriation of assets: Theft of company resources for personal benefit.
- Examples:
  - Theft of cash through a fictitious vendor scheme.
  - Creation of ghost employees and collection of their paychecks.
  - Theft of cash receipts before they are deposited.
  - Charging personal expenses to organization credit cards.

Fraud in Accounting

- Intentional misstatement of financial statements: Manipulating the accounting records or financial statements.
- Examples:
  - Intentional overstatement of revenue to meet budget targets.
  - Recording revenue before it is earned.
  - Understating expenses by not recording accrued liabilities or expenses.
  - Understating allowance for uncollectible receivables.

Fraud Triangle

- Three factors that commonly contribute to fraud:
  - **Pressure/Incentive:** Financial or personal pressure that motivates an individual to commit fraud.
  - **Opportunity:** Weak internal controls or lack of oversight that create a chance to commit fraud without detection.
  - **Rationalization:** Individual's ability to justify the fraudulent behavior.



Why Internal Controls Matter

- Fraud can occur in organizations of any size.
- Fraud schemes often exploit weaknesses in processes.
- Strong internal controls help to protect assets and maintain financial reporting integrity.
- Internal controls should be designed to:
  - Prevent fraud
  - Detect fraud timely to mitigate losses

Segregation of Duties

No single individual should control an entire transaction from beginning to end.

If one individual has the ability to control multiple components of a transaction, there is an opportunity for fraud.

Segregation of Duties

Authorization: Approving transactions

- Examples: Approving purchases, vendors, journal entries, payroll changes

Custody: Having physical or electronic access to assets

- Examples: Handling cash/investments, managing bank accounts, possessing check stock, controlling inventory

Recordkeeping: Recording transactions in the accounting records.

- Examples: Entering invoices, posting journal entries, maintaining the general ledger

Reconciliation/Review: Independently reviewing and verifying transactions.

- Examples: Review of bank reconciliations, journal entries, internal financial reports, budget-to-actual reports

Segregation of Duties

Example of appropriate segregation of duties for accounts payable

- Employee 1 enters vendor invoice
- Employee 2 approves invoice
- Employee 3 releases payment
- Employee 4 reconciles the bank account

Fraud risks addressed

- Fictitious vendors
- Unauthorized payments
- Misappropriation of cash

Approval and Authorization Controls

Approval Considerations

- Appropriate level of management
- Adequate knowledge of transaction
- Consider risk – every transaction or type of transaction may not require the same level of scrutiny.

Examples

- Purchase approvals based on spending thresholds
- Journal entries reviewed by someone independent of the preparer
- Changes to vendor master files approved and documented
- Changes to payroll records approved and documented

Reconciliation and Monitoring Controls

- Establish and document an internal process for consistent reconciliations including frequency for each key account area.
- Establish timelines for completion of monthly reconciliations and reviews.
- Independent review helps identify errors and irregularities.
- Recommend asking at least one question as part of the review process.

Reconciliation and Monitoring Controls

Examples

- Monthly bank reconciliations
- Review of unusual journal entries
- Comparison of budget vs. actual results
- Review of accounts receivable and accounts payable aging

Red Flags

- Reconciling items that never clear
- Unexplained adjustments
- Excessive manual journal entries
- Unexpected fluctuations in budget vs. actual results
- Unexplained increase in accounts receivable

Access Controls and Technology Safeguards

Limit access to systems, data and financial processes

- Role-based system access
- Multi-factor authentication
- Periodic user access reviews
- Automated approval workflows

Fraud Awareness and Ethical Culture

Controls are strongest when supported by an ethical culture.

- Tone at the top
- Code of conduct
- Whistleblower hotline
- Fraud awareness training
- Management accountability

Summary

Effective fraud prevention is not one control. It is a system of preventive, detective and monitoring controls working together.

Segregate responsibilities

Review and reconcile regularly

Build a culture that promotes ethical behavior and accountability

Contact

Rebekah Payne

Partner

rebekah.payne@cbh.com

317.224.1278

cbh.com

Cherry Bekaert

Your Guide Forward

Fraud Protection & Mitigation (Technology Perspective)

July 23, 2026

Indiana CPA Society Not-for-Profit Conference

Cherry Bekaert

Your Guide Forward

What We Will Cover

- Where the accounting perspective leaves off, closing the “Opportunity” gap in the Fraud Triangle
- Why not-for-profit organizations face elevated fraud risk
- How banking controls, accounting safeguards and IT capabilities work together
- Common vulnerability points in financial operations
- Practical steps to reduce exposure and strengthen controls

Why Not-for-Profit Organizations Are Prime Targets for Fraud

- Lean finance teams make segregation of duties difficult
- A high-trust culture exists among staff, volunteers and board members
- Manual processes and shared logins remain common in some organizations
- Multiple funding sources, grant disbursements and cash-handling points add exposure
- Budget for dedicated IT security oversight is often limited

Common Vulnerability Points

Financial Process Gaps

- Shared or undocumented approval authority
- Infrequent bank and account reconciliations
- Manual, paper-based disbursement processes

Technology Gaps

- Shared logins and stale user access
- Unmonitored networks and endpoints
- Email systems without safeguards against impersonation

Three Connected Layers of Protection

Banking Controls

- Positive pay and payment verification
- Dual approval on disbursements
- Regular account reconciliation

Accounting Safeguards

- Segregation of duties
- Documented approval workflows
- Regular internal and external review

IT Capabilities

- Access controls and identity management
- Network security and monitoring
- Systems that enforce policy consistently

Why Secure IT Is the Connective Tissue

- Banking controls depend on systems that can verify who is initiating a transaction
- Accounting safeguards depend on reliable, tamper-resistant records and audit trails
- IT capability determines whether those controls are enforced day to day, not just on paper
- A secure IT environment is what turns policy into practice across banking and accounting
- Together, these three layers close the “Opportunity” leg of the Fraud Triangle

Access Controls and Identity Management

What This Looks Like

- Access provisioned by role, not by request
- Multi-factor authentication required for every login that touches cash or donor data
- Access recertified on a set schedule, not left to institutional memory

How It Reinforces Accounting Safeguards

- Enforces the segregation of duties pillars from the accounting session in the system, not only on paper
- Removes access automatically when roles change
- Creates a clear audit trail of who approved what

Network Security and Monitoring

What This Looks Like

- Continuous monitoring for unusual account or system activity
- Endpoint protection across every device that touches financial data
- A defined incident response plan and escalation path

How It Reinforces Banking Controls

- Flags suspicious login or payment activity before funds move
- Supports faster detection of compromised email or vendor accounts
- Provides a record for banks and auditors when questions arise

Bringing the Layers Together

- One weak link, such as a shared password, a stale user account or an unreconciled account, can undo controls built everywhere else.
- Fraud prevention works best as a system, not a checklist. When banking controls, accounting safeguards and IT capabilities are designed to reinforce each other, a gap in one area is more likely to be caught by another.

Practical Next Steps for Finance and Board Leaders

- Review who has access to banking and accounting systems, and how often that access is reviewed
- Confirm dual approval is required for payments and account changes
- Ask whether your network and endpoints are actively monitored
- Request an IT risk assessment that maps directly to your accounting controls
- Build fraud response steps into your existing risk and audit calendar

Let’s Connect

Jim Kramer,

Partner
jim.kramer@cb.digital

502.882.4348

cbh.com

Cherry Bekaert
Your Guide Forward