SMALL BUSINESS FRAUD CASE STUDIES:

Overview of Small Business Fraud Trends in Northeastern WI

CHALLENGES:

Northeast Wisconsin faces a complex and evolving landscape of small business fraud, characterized by unique regional economic factors, emerging technologies, and sophisticated criminal methodologies. These case studies examine the prevalent fraud trends, underlying causes, and potential mitigation strategies for small businesses in the region encompassing Brown, Outagamie, Winnebago, and surrounding counties.

REGIONAL ECONOMIC CONTEXT

Northeast Wisconsin, known for its diverse economic base including manufacturing, agriculture, and emerging technology sectors, presents a unique environment for fraudulent activities. The region's strong small business ecosystem, with approximately 96% of businesses classified as small businesses, creates both opportunities and vulnerabilities for fraudulent schemes.

American National Bank Fox Cities

FUEL OPPORTUNITY

KEY FRAUD TRENDS

1. Financial Statement Fraud

Prevalence: Highest reported fraud type in the region

Estimated impact: 5-7% of annual revenue for affected businesses

Common methods:

- Asset misappropriation
- Falsified expense reports
- Manipulated accounting records
- Unauthorized fund transfers

2. Cybercrime and Digital Fraud

Emerging threat vector with rapidly increasing sophistication

Primary attack methods/common methods:

- Phishing emails targeting small business owners
- Business email compromise (BEC) schemes
- Ransomware attacks
- Social engineering tactics

Regional Statistics:

- 42% increase in cybercrime incidents from 2021 to 2023
- Average financial loss per incident: $36,000 for small businesses
- 68% of affected businesses are located in urban areas like Green Bay and Appleton

3. Payroll and Accounting Fraud

Key characteristics:

- Internal perpetrators - typically long-term, trusted employees
- Most common in businesses with 10-50 employees

Typical schemes:

- Ghost employee fraud
- Timesheet manipulation
- Unauthorized compensation adjustments

4. Procurement and Vendor Fraud

Prevalent in Manufacturing and Supply chain Sectors

Common methods:

- Kickback schemes
- Fake vendor creation
- Invoice manipulation
- Collusive fraud between employees and external parties

DEMOGRAPHIC AND SECTOR INSIGHTS

VULNERABLE BUSINESS SECTORS

1. Manufacturing
2. Retail
3. Construction
4. Professional Services
5. Hospitality and Food Service

FRAUD RISK FACTORS

- Limited internal controls
- Family-owned business structures
- Lean accounting departments
- Trust-based management approaches
- Limited fraud awareness and training

ECONOMIC IMPACT

ESTIMATED ANNUAL LOSSES:

- Total small business fraud losses in Northeast Wisconsin: $42-55 million
- Average loss per business: $87,000
- 17% of affected businesses experience significant operational disruption

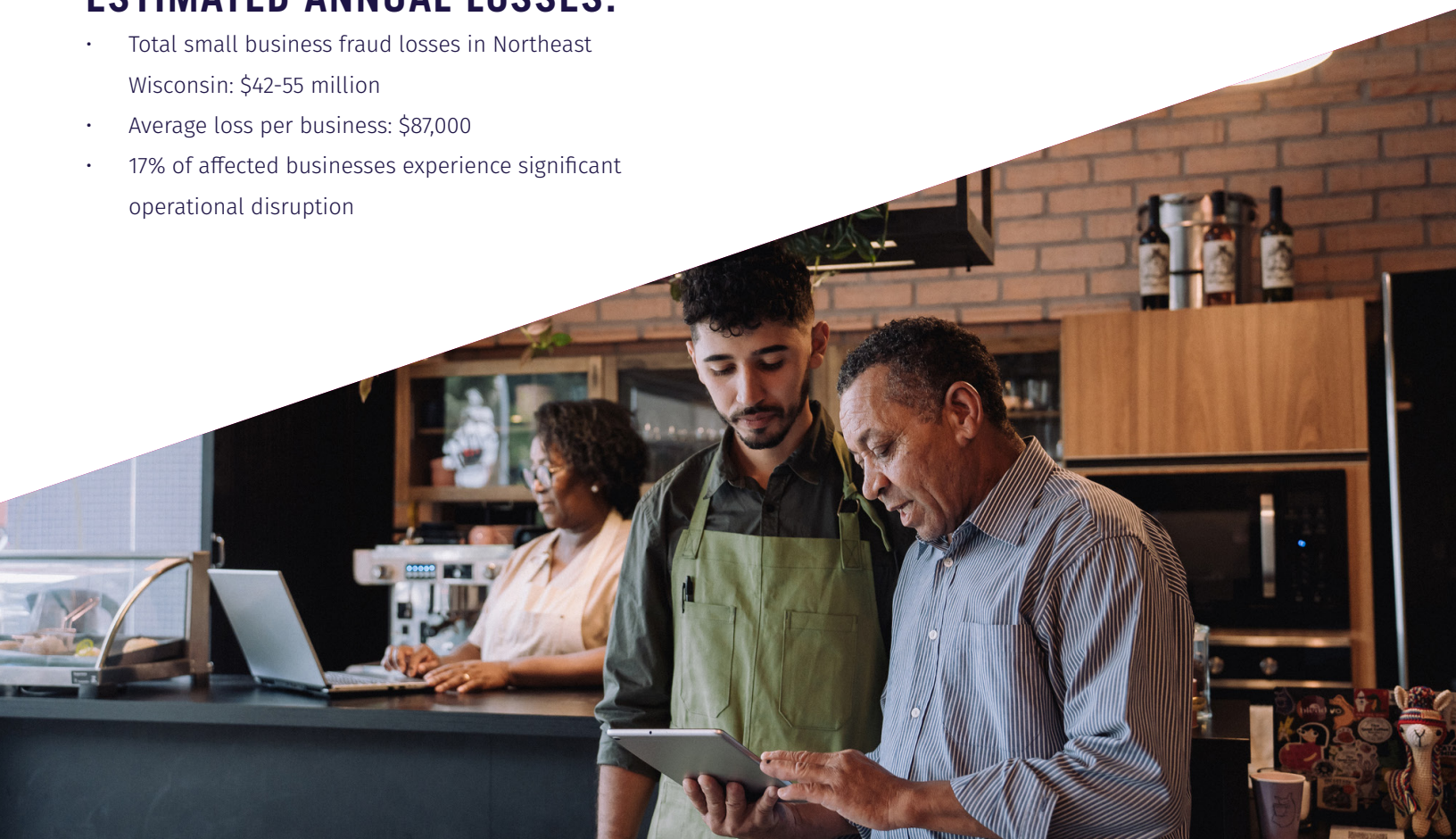
EMERGING FRAUD PREVENTION STRATEGIES

TECHNOLOGICAL APPROACHES:

- Advanced accounting software
- Multi-factor authentication
- Regular cybersecurity audits
- Employee monitoring systems

EDUCATIONAL AND CULTURAL APPROACHES

- Regular fraud awareness workshops
- Implementing whistleblower programs
- Creating transparent reporting mechanisms
- Developing robust internal control systems



CONCLUSION

The fraud landscape in Northeast Wisconsin demands a proactive, multi-faceted approach. Small businesses must invest in prevention, leverage technological solutions, and create a culture of transparency and accountability to protect themselves against sophisticated fraudsters.

RECOMMENDATIONS FOR SMALL BUSINESS OWNERS

1. Conduct regular internal audits
2. Implement robust internal control systems
3. Provide ongoing employee fraud awareness training
4. Invest in cybersecurity infrastructure
5. Maintain open communication channels
6. Develop clear reporting and investigation protocols

Methodology Note:
This case study background is based on AI data from local law enforcement data, small business survey responses, forensic accounting reports & economic development center insights.

FRAUD CASE STUDIES: WHEN CRIMINALS STRIKE

The Stolen Business Check

A NIGHTMARE OF CHECK FRAUD

The Incident: In March 2024, this small business experienced a devastating check fraud scheme that put the company in a dangerous predicament.

THE VICTIM:

Family-owned business of 20 employees with an established reputation

LOCATION:

Appleton, WI

BUSINESS:

Small food and beverage

ANNUAL REVENUE:

$5 million

American National Bank Fox Cities

FUEL OPPORTUNITY

HOW IT HAPPENED:

1. An invoice was paid and the check of $8,750 was mailed to a long-standing supplier

2. The check was stolen directly from the sender's business mailbox, likely overnight when no one was there

3. Criminals used a chemical washing technique to remove the original ink:

- Acetone or similar chemical solution used to erase original details
- Original payee name completely removed
- Amount potentially altered
- New payee name added: "John Stevens"

4. The fraudster used mobile deposit at a large national bank

5. Deposited the manipulated check through a mobile banking app

6. ***Total amount stolen: $8,750***

DISCOVERY AND IMPACT:

- "Long-standing supplier" contacted "small food company" when they never received payment

- "Large national bank" suspected fraud on the account that the check had been deposited to, and attempted to reach the client to notify them.

- The business confirmed the fraudulent check, and that it had been cashed two weeks after the initial mailing; however, they did not notice the payee's name had been changed until the national bank contacted them

- Upon notification from the client, American National Bank Fox Cities immediately reached out to the national bank to assist with recovering the funds.

- American National Bank Fox Cities assisted the client with the affidavit of alteration and worked with the national bank to have the funds returned.

- The small business had limited fraud awareness and training

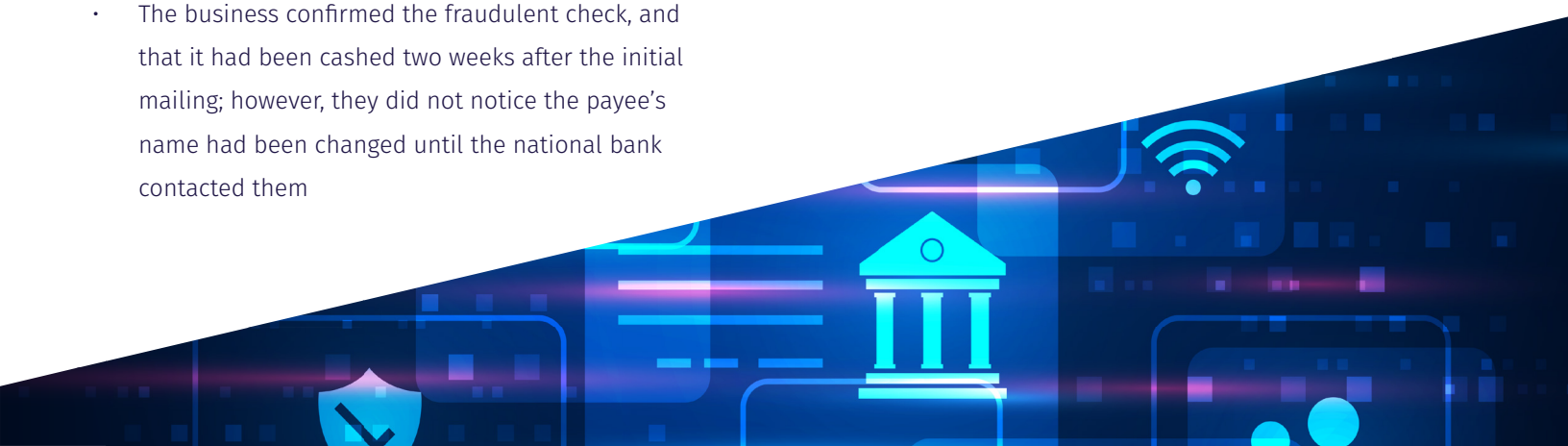
CONSEQUENCES:

- Cash flow disruption
- Reputation risk with supplier relationship
- Potential legal and banking dispute
- Cost of replacing the funds
- Potential credit impact

LESSONS LEARNED

- Install secure, locked mailboxes
- Use trackable mailing methods
- Implement Positive Pay services with bank that include Payee Name Mismatch
- Consider electronic payment methods such as ACH
- Conduct frequent bank statement reconciliations that include viewing the front and back of checks that have been cashed

Disclaimer: Specific business identities have been anonymized to protect privacy and confidentiality.



FRAUD CASE STUDIES: WHEN CRIMINALS STRIKE

THE EMAIL COMPROMISE TRAP

WHEN INTERNAL COMMUNICATION GOES WRONG

The Incident: In July 2024, the small B2B company fell victim to a sophisticated email compromise scheme that exposed their financial vulnerabilities in a dangerous predicament.

THE VICTIM:

Family-owned business with 100 employees

LOCATION:

Green Bay, WI

BUSINESS:

Contractor

ANNUAL REVENUE:

$3 million

American National Bank Fox Cities

FUEL OPPORTUNITY

HOW IT HAPPENED:

1. Criminals gained access to the company's email system

2. Carefully studied internal communication patterns

3. Sent a fraudulent email from a seemingly legitimate internal account

- Spoofed email address of the finance director
- Requested urgent change to direct deposit information
- Targeted the payroll specialist

4. ***Total amount stolen: $5,000 in employee salary***

TECHNICAL DETAILS:

- Email appeared to come from an internal employee
- Actual source: external criminal email
- Requested immediate update to direct deposit for the employee
- Provided bank details for a criminal-controlled account

EXECUTION:

- Payroll specialist, believing the email was legitimate, processed the change without verifying the information with the employee

Routing and account number for the current payroll cycle was changed and their payroll was redirected to the fraudulent account.

DISCOVERY AND IMPACT:

- Discovered when employee reported missing paycheck
- Forensic investigation revealed email spoofing
- Significant reputation damage
- Potential legal and regulatory complications

CONSEQUENCES:

- Cash flow disruption
- Potential legal and banking dispute
- Cost of replacing the funds
- Potential credit impact

LESSONS LEARNED

- Implement multi-factor authentication
- Create verbal verification protocols for financial changes
- Use dedicated communication channels for sensitive requests
- Regular cybersecurity training
- Email authentication technologies (DMARC, SPF, DKIM)

Disclaimer: Specific business identities have been anonymized to protect privacy and confidentiality.

FRAUD CASE STUDIES: WHEN CRIMINALS STRIKE

THE SOCIAL MEDIA ADVERTISING INVOICE

EXPLOITING LEGITIMATE BUSINESS PRACTICES

The Incident: In September 2024, the business fell victim to a sophisticated email fraud targeting their advertising expenditures.

THE VICTIM:

Small B2B company with 15 employees

LOCATION:

Appleton, WI

BUSINESS:

Marketing business with an active social media marketing presence

ANNUAL REVENUE:

1.8 million

American National Bank Fox Cities

FUEL OPPORTUNITY

HOW IT HAPPENED:

1. The business regularly runs social media advertisements

2. Received an official-looking email mimicking a major social media platform's billing department

3. Email appeared to be a legitimate invoice for advertising services

- Detailed breakdown of ad spend
- Professional formatting
- Urgent payment request
- Included logos and seemingly authentic contact information

4. ***Total fraudulent invoice: $50,000***

EXECUTION:

- Accounting staff member processed the payment
- Payment sent to a fraudulent bank account
- No actual additional advertising services rendered

Disclaimer: Specific business identities have been anonymized to protect privacy and confidentiality.

DISCOVERY AND IMPACT:

- Discovered when the owner received the email confirmation of the approved ACH payment, owner immediately notified American National Bank Fox Cities to assist and attempt to stop the ACH

- Actual social media platform confirmed the invoice was fake

- Due to the timing of catching the error, American National Bank Fox Cities was able to assist with reversing the file and recovering the funds

- Required extensive internal investigation

- Additional dual controls set up for the client and the American National Bank Fox Cities

LESSONS LEARNED

- Implement multi-step verification for large payments
- Cross-reference invoices with actual advertising accounts
- Create a mandatory, in-person approval process for unexpected invoices
- Verify payment requests through official channels like a trusted phone number, do not reply to an email request

CONCLUSION

These case studies demonstrate the evolving and sophisticated nature of modern financial fraud. Businesses must remain vigilant, implement robust security measures, and foster a culture of skepticism and verification. No business is immune, and vigilance is the key to protection. The good news is that American National Bank Fox Cities took immediate action to protect its business clients. We need to work together as a team to stop the fraud before it happens.

Here are the practical steps you can take right now:

- Sign up for Positive Pay service - it's like having a security guard verifying every check and electronic debit that comes through your account
- Enable multi-factor authentication on all your business email accounts
- Work with your employees to create a system for verifying (in person or with a trusted phone number) any requests involving money or banking information
- Make sure your employees know your expectations regarding changing information for vendor or employee accounts or requesting wires to be sent out
- Keep your business contact information up to date with the bank so they can reach you quickly if they spot something suspicious

The most important takeaway is this: don't wait until after fraud happens to protect your business. The small amount of time it takes to set up these security measures is nothing compared to the weeks or months it can take to recover stolen funds. American National Bank Fox Cities has a dedicated team ready to help you put these protections in place - please contact us to review your security measures.

Tiffany Binish

AVP | Treasury Management

direct: 920-560-5950

tbinish@anbfc.bank