



Fraud Mitigation

KIM HARLESS

DECEMBER 5, 2025



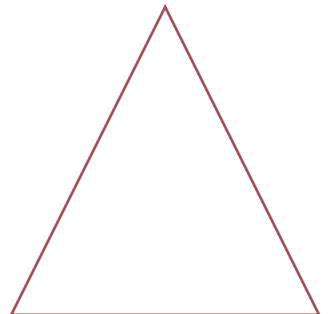
Kim Harless

▶ VP, Treasury Management Officer at Dart Bank



- Dedicated banking professional with nearly four decades of experience serving commercial clients.
- Passionate about building strong relationships with businesses and the community, providing tailored financial solutions, and supporting local initiatives.


kharless@dartbank.com | 517.699.3388





Overview


- Understand how fraud impacts K-12 organizations
- Review current fraud and identity theft trends
- Learn common fraud schemes
- Explore banking best practices, protective measures, and internal controls
- Discover strategies for secure digital and cashless payments
- Understand the value of proactive bank partnerships and annual account reviews
- Build a culture of fraud awareness across your district



Fraud poses a significant threat to businesses, affecting their finances, reputation, and customer trust.



Why Fraud Prevention Matters in Schools

- School districts manage predictable, high-volume funds, like payroll, vendor payments, and grants, making them attractive targets for fraud.
 - Misused or lost funds impact students, staff, and taxpayer confidence.
 - Fraud can disrupt daily operations, delay payments, and require significant recovery effort.
 - Even minor incidents can damage a district's credibility and community relationships.
- 

The Fraud Landscape in 2025



Over **3 million** consumer reports filed with the FTC, including fraud, identity theft, and more



\$7.1 billion in losses



Top Fraud Categories:

Imposter Scams:

\$1.6 Billion Lost

Online Shopping & Negative Review Scams:
\$224.8 Million Lost

Internet Service Scams:
\$98.5 Million Lost



748,555 identity theft reports



Credit Card Fraud:
42.5% of cases



Other Identity Theft:
33.4% of cases



Loan/Lease Fraud:
15.3% of cases

State of Michigan Fraud Insights

67,561

Total Consumer Reports

\$125.1 Million

Total Losses

16,315

Identity Theft Reports

Top Report Categories

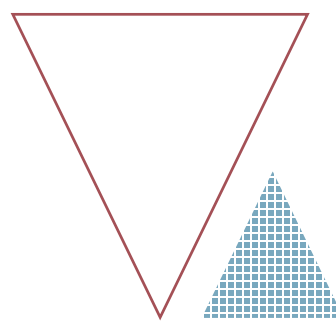
Identity Theft- **16,315** reports
Imposter Scams- **9,991** reports
Debt Collection- **7,129** reports
Online Shopping & Negative Reviews- **4,134** reports
Internet Services- **3,882** reports

Top Fraud Subcategories

Business Imposters- **4,602** reports
Government Imposters- **4,187** reports
Online Payment Services- **2,733** reports
Job Scams & Employment Agencies- **1,196** reports

Top Identity Theft Categories

Credit Card Fraud- **6,790** reports
Other Identity Theft- **5,418** reports
Loan/Lease Fraud- **2,636** reports
Bank Fraud- **1,618** reports



K-12 Cyber Threat Statistics

- **82%** of K-12 organizations experience cyber incidents
- Nearly **14,000** security events observed
- Over **9,300** confirmed incidents
- Cyber threat actors target human behavior **45% more often** than technical vulnerabilities
- More than **5,000** K-12 organizations show that cyber threat actors appear to target schools during critical periods
- Top Malware Infection Vectors
 - 63% Malvertisement
 - 27% Multiple
 - 7% Dropped
 - 3% Malspam

Source: CIS MS-ISAC K-12 State of Cybersecurity Report: Where Education Meets Community Resilience





Common Fraud Schemes in K-12 Organizations



Payroll Redirection

Fraudsters impersonate employees or HR staff to request payroll changes, diverting direct-deposit paychecks into fraudulent accounts. These scams often begin with phishing or compromised credentials.

Business Email Compromise (BEC)

Cybercriminals spoof or hack district email accounts to pose as vendors, staff, or administrators, convincing staff to make unauthorized payments or share sensitive data.

ACH Fraud

Attackers use stolen login credentials or malware to initiate unauthorized ACH transfers, moving district funds to fraudulent accounts before detection.

Phishing Emails

Fake emails appear to come from trusted sources (bank, IT, superintendent, or vendor) and trick recipients into revealing passwords, clicking malicious links, or downloading malware.

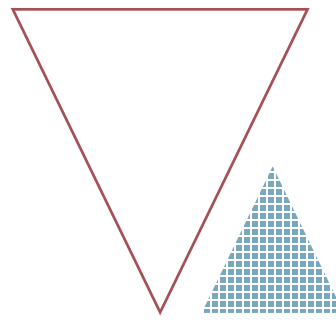
Outdated Software & Systems

Running outdated operating systems or unpatched software leaves vulnerabilities open to exploitation, allowing hackers to gain unauthorized access or install ransomware.

Check Fraud

Even in a digital world, checks remain a major vulnerability for schools. Fraudsters steal checks from mailboxes, drop boxes, or outgoing mail.

Fraud Typologies and Red Flags to Watch For



Payroll Redirection

- Urgent requests for payroll updates
- Unfamiliar email addresses
- Requests made outside standard HR procedures

ACH/Vendor Payment Fraud

- New vendor setup requests
- Pressure to process payments quickly
- Mismatched contact information between invoices and prior records

Check Fraud

- Suspicious or altered check details
- Payment anomalies
- Verification issues

Business Email Compromise

- Slight variations in email addresses
- Urgent or secretive payment requests
- Changes to established payment instructions

Outdated Software or Weak Controls

- Frequent system errors
- Skipped updates
- Lack of audit trail for financial transactions

Phishing & Social Engineering

- Unusual sender addresses
- Requests for login verification
- Misspellings and unexpected attachments



The Rise of Business Bank Fraud

1

Alarming Statistics

Business bank transaction fraud has surged in recent years, with attempts tripling in some cases. Fraudsters are constantly devising new scams to target.

2

Diverse Fraud Tactics

Fraudsters utilize a wide range of techniques, from phishing emails to sophisticated hacking attempts, to gain unauthorized access to business accounts and initiate fraud transactions.

3

Shared Responsibility

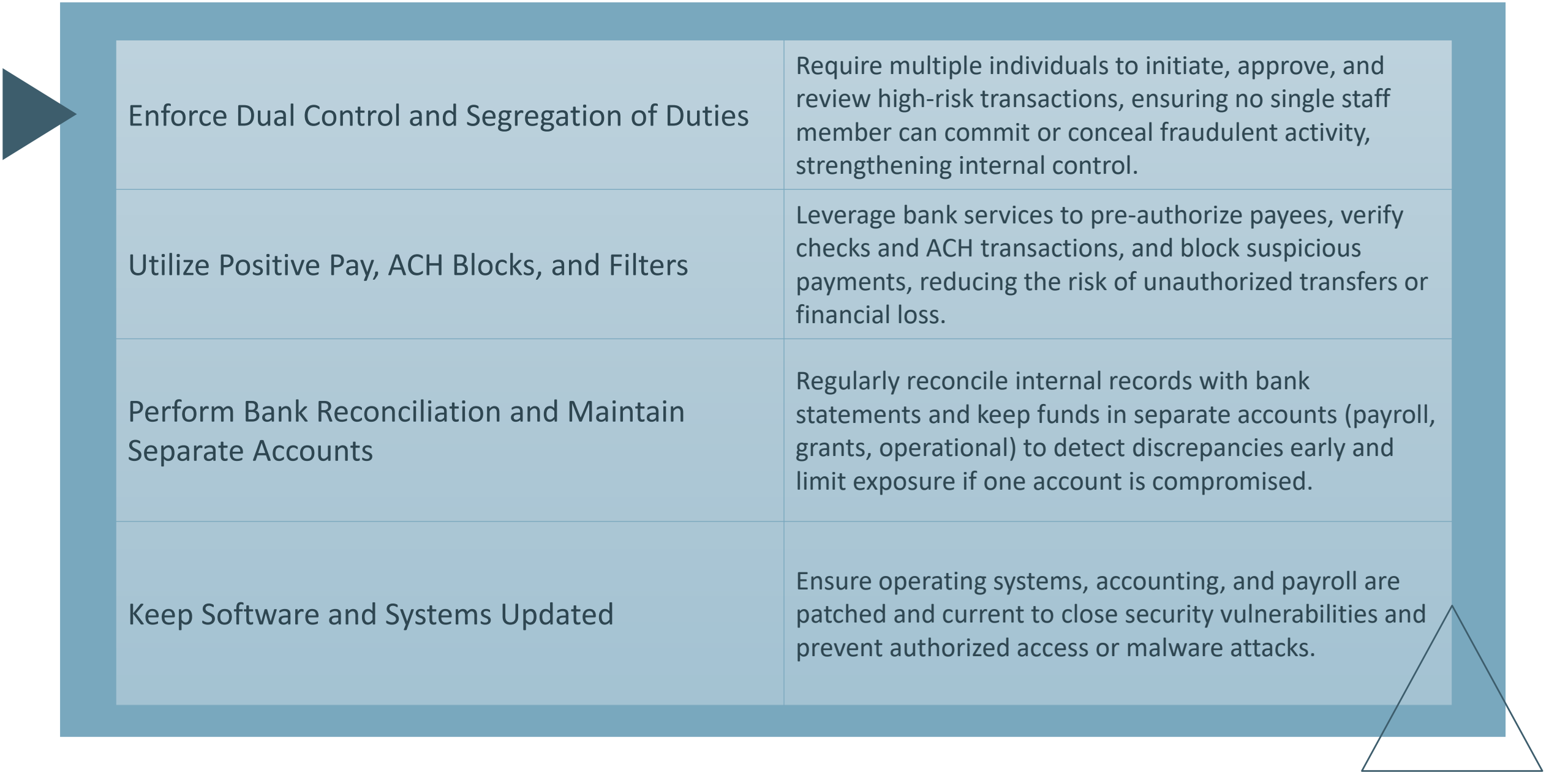
Both banks and businesses share the responsibility for preventing fraud. With banks' security measures, businesses must also be vigilant and implement robust internal policies to protect themselves.

Essential Fraud Safeguarding Strategies



Implement Robust Security Measures	Utilize multi-factor authentication, encryption, and secure payment processing to protect against unauthorized access and data breaches.
Enhance Monitoring and Detection	Closely monitor financial transactions, account activity, and suspicious behavior to identify and respond to fraud in a timely manner.
Empower Employees with Training	Provide ongoing education and training to help employees recognize and report fraudulent activities, enhancing the organization's overall fraud resilience.
Collaborate and Report Incidents	Engage with law enforcement agencies, industry associations, and other stakeholders to share information, support broader anti-fraud efforts, and ensure accountability.
Conduct Regular Audits	Perform periodic internal or external reviews of financial transactions and internal processes to identify irregularities, ensure compliance with policies, and strengthen overall fraud resilience.

Essential Fraud Safeguarding Strategies Cont.



Enforce Dual Control and Segregation of Duties	Require multiple individuals to initiate, approve, and review high-risk transactions, ensuring no single staff member can commit or conceal fraudulent activity, strengthening internal control.
Utilize Positive Pay, ACH Blocks, and Filters	Leverage bank services to pre-authorize payees, verify checks and ACH transactions, and block suspicious payments, reducing the risk of unauthorized transfers or financial loss.
Perform Bank Reconciliation and Maintain Separate Accounts	Regularly reconcile internal records with bank statements and keep funds in separate accounts (payroll, grants, operational) to detect discrepancies early and limit exposure if one account is compromised.
Keep Software and Systems Updated	Ensure operating systems, accounting, and payroll are patched and current to close security vulnerabilities and prevent unauthorized access or malware attacks.



Embracing Secure Digital & Cashless Payments

Streamline Transactions

Digital and cashless payment methods improve efficiency, reduce manual errors, and support accountability across district departments and activities.

Enhanced Security

Use verified payment platforms with multi-factor authentication and encryption to safeguard transactions from unauthorized access or fraud.

Policy and Oversight

Implement clear district policies for approving, tracking, and reconciling digital payments to prevent misuse or unapproved transactions.

Parental and Community Payments

Ensure tools used for lunch accounts, athletics, or donations are verified and secure, protecting families from scams.



Proactive Fraud Monitoring & Reporting

1

Monitor Transactions

Closely monitor your business's bank transactions and account activity for any suspicious or unauthorized activity. Promptly report any concerns to your financial institution.

2

Implement Alerts

Set up transaction alerts and notifications to be notified of any unusual or high-risk activities, allowing you to take swift action to mitigate potential fraud.

3

Maintain Detailed Records

Keep meticulous records of all your business's financial transactions, including any fraud-related incidents, to aid in investigations and potential legal proceedings.



Embrace a Culture of Fraud Awareness



Collaboration

Foster a culture of collaboration and open communication within your organization, encouraging employees to share any concerns or suspicions about potential fraud.



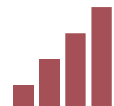
Continuous Learning

Provide ongoing training and education for your employees, keeping them informed about the latest fraud trends and best practices for prevention and detection.



Proactive Vigilance

Instill a mindset of proactive vigilance, where everyone in your organization is empowered and encouraged to be on the lookout for any suspicious activities or red flags.



Data Driven Insights

Leverage data analytics and monitoring tools to gain deeper insights into your business's financial transactions and identify potential fraud patterns or anomalies.



Strengthen Your Banking Partnerships

Annual Review Meetings

Meet annually with your bank to discuss new fraud trends, cash management tools, and digital banking tools.

Stay Current on Banking Technology

Review updates to ACH filters, payment controls, and fraud detection tools that help keep your district efficient and protected. Leverage Positive Pay for both checks and ACH to automatically flag or block unauthorized transactions.

Optimize District Accounts

Evaluate account structures, reconciliations, and authorization limits to ensure alignment with best practices.

Collaborative Approach

A strong bank partnership helps districts proactively adapt to evolving financial risks and regulations.

FDIC Insurance

- Understanding the Scope of FDIC Protection
- Transactions Covered by FDIC Insurance
- Limits and Exclusions

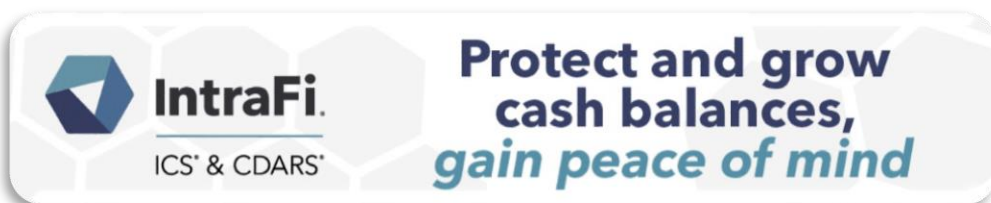
FEDERAL DEPOSIT
INSURANCE CORPORATION



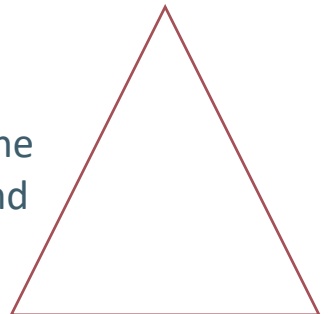
550 17TH STREET

The Importance of FDIC Insurance & Coverage Limits

Individual Accounts	Joint Accounts	Business Accounts
For individual accounts, the FDIC insures up to \$250,000 per depositor, per insured bank. This means that if you have \$250,000 or less in a single account, your money is fully protected.	For joint accounts, the FDIC insures up to \$250,000 per co-owner. So, if you and your business partner have a joint account with \$500,000, the entire balance is covered.	FDIC insurance also applies to business accounts, such as checking, savings, and money market accounts. The coverage limit is \$250,000 per business, per insured bank.



With the ICS and CDARS services, you can enjoy the safety and simplicity that comes with access to multi-million-dollar FDIC insurance through a single bank relationship. You can choose the service or combination of services that can offer the returns and access to funds you see.



Key Takeaways

- Established layered fraud defenses
- Train and empower staff to spot red flags
- Use secure, cashless, payment systems
- Meet with your bank annually to stay ahead of evolving risks





Questions?



Testimonial

“Since our district transitioned to Dart Bank, we’ve seen a significant increase in our earned interest and reduction in banking fees. Dart Bank consistently provides excellent customer service and truly feels like a friendly neighborhood bank!”

Alexis Regnier, MBA, CFO Certified
Director of Finance
Holt Public Schools



Thank You!

Email

kharless@dartbank.com

Phone

517.699.3388

