Internal Controls: Preventing Fraud Before It Happens

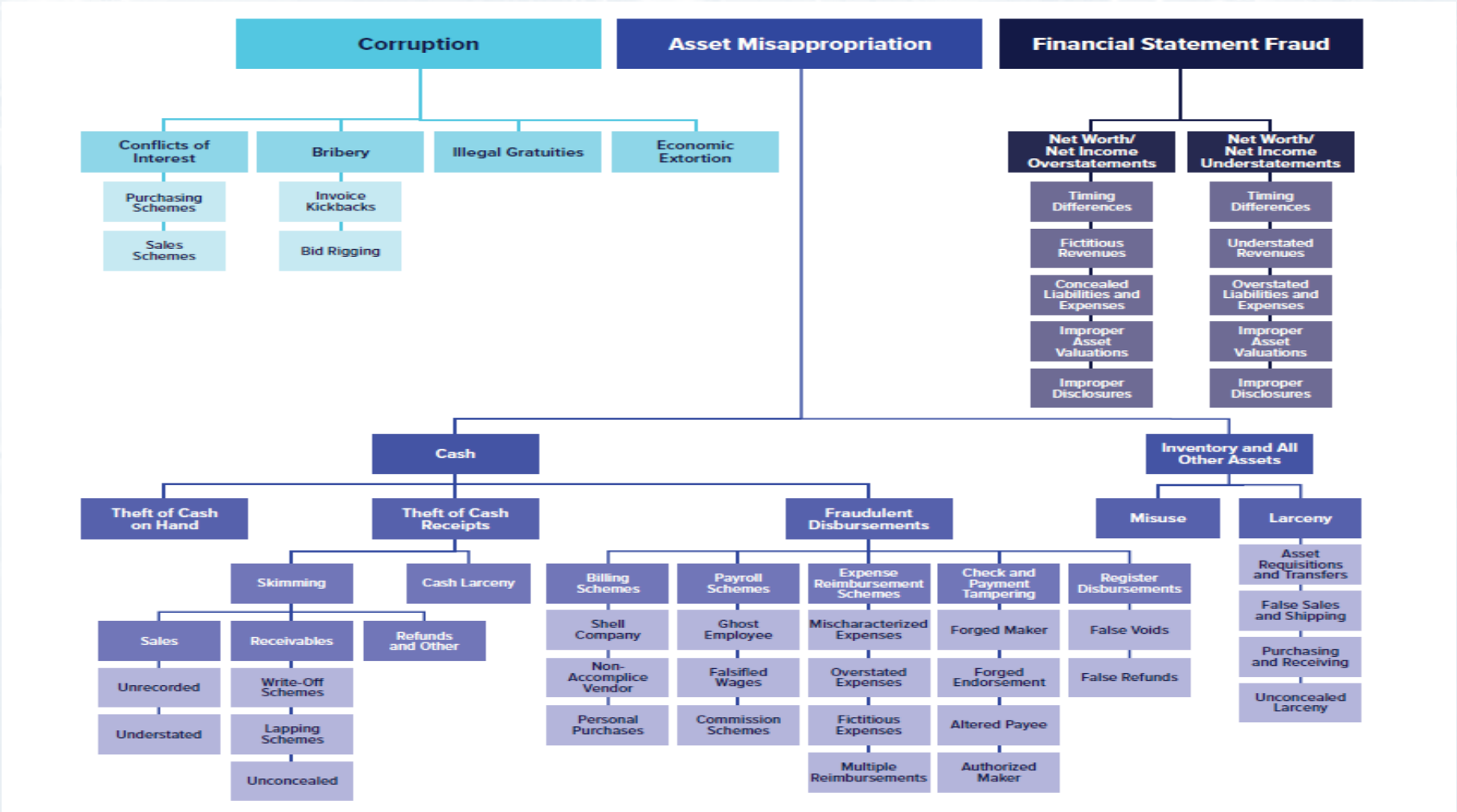
Prepared by: Sunni Zentner, Deputy Director, Statewide Payroll & Accounting
and Jennifer Efird, Internal Controls & Compliance Team Lead
Office of Accounts and Reports (OAR)
Department of Administration

KANSAS AGENCY BUSINESS SUMMIT

What's going on out there?

- In the US, losses due to fraud in 2025 were estimated at $148.2 billion, as reported by Consumer Federation of America.
- This was up about 25% from the 2024 amount.
- Seniors are the largest targeted demographic with an average of $38,500 per reported incident.
- AI-enabled fraud is on the rise and includes technology where synthetic content is used to substantiate a scam. Examples include fake web sites, social media profiles, audio and even video conversations.
- There are places in the world where there are full office buildings of staff members who's sole job responsibility is to create and successfully scam individuals and business.

Which of these could happen in your agency?



KANSAS AGENCY BUSINESS SUMMIT

State of Kansas Internal Controls Framework

- Step 1: Identify significant fiscal processes
- Step 2: Conduct a risk assessment
- Step 3: Define and document controls
- Step 4: Test design and operating effectiveness
- Step 5: Address findings and deficiencies
- Step 6: Include non-fiscal controls
- Step 7: Evaluate third-party controls

Case Study on Controls

Agency accounting employee Lucy was contacted by her director as she was leaving for a meeting offsite. They need to pay the electrical contractor $200 today for emergency work being done in their office space. Tim with ABC Electrical Company needs to purchase supplies and cannot finish the electrical emergency project without payment.

Lucy enters a payment voucher of $200 as a single pay voucher to Tim; she decides a check for the supplies would get cut prior to end of the day and she could give it to him so he can get what he needs to finish.

Lucy processes the payment voucher and approves the payment in SMART; her director had already left but had verbally told her to get the payment made.

Lucy is also responsible for the reconciliation of the agencies monthly financial reports.

Lucy handed over the check at 4:30 pm to Tim and he left.

The next morning, Tim showed up to finish the work and when Lucy asked for a receipt, he claimed he lost it……. but also, Tim will need more supplies.

How many internal control violations can you identify in this situation?

Controls and Risk Identified

- Supplier Contract for Electrical supplies
- Gave money to ‘Tim’ for supplies
- No Prior Authorization for the purchase of the supplies
- No Record of the supplies purchased
- Payment Processing
- SMART Approvals
- Reconciliation
- Lack of independent review
- Excessive System access
- Separation of duties
- Documentation for the purchase

Is this a situation of fraud or internal control weakness within the agency?

Case Study on Data Monitoring

- Agency Accounting staff can approve transactions up to $5,000 or lower without additional review from OAR Audit staff.
- A supplier payment is entered for $4,950
- The transaction is a legitimate payment for services performed.
- The next monthly payment is $4,950.
- And another monthly payment of $4,950 is paid again.

Case Study - Analysis

Does anyone in your agency look for these types of transactions?

Does anyone question these types of transactions?

Are agency controls in place to detect payment patterns?

The payments are all legitimate payments.

Internal Controls is bigger than just checking the purchase or confirming processes were followed, as more fraud is occurring and new methods are transpiring, all agency staff need to look for

Patterns	Unusual transactions
Relationships	Rapid changes
Trends	Multiple Identities
Exceptions	Behavior changes
Repeated activity	Transactions just below approval thresholds

Which of the following have the biggest red flag for Fraud?

- Multiple payments just below approval thresholds
- Vendor bank account changed right before payment
- Employees approving their own payments in SMART
- Duplicate invoice numbers
- Same address for multiple suppliers
- Unusual payments outside the normal pattern
- Large increase in payments to one supplier
- Dormant supplier suddenly made active and receiving payments



Case Study on Ghost Invoice

It began on a dreary Monday morning. Rhonda, an administrative assistant, walked into her boss's office holding a printed invoice for a 'BAG - Tactical Carrier.' The item price was $226.33 which immediately raised a red flag since most gear labeled 'tactical' is at least $1,000.

Rhonda asked her boss if he remembered requesting, approving or receiving the item, which he did not remember. After looking at the invoice, they noticed it had an old date and did not appear to be from any of their regular suppliers. They were unable to locate the supplier in the accounting system. Next, they searched online and found a legitimate website for the supplier, including addresses for headquarters and branch locations, but none of them matched the address on the invoice. After looking for the item on the supplier's website, they discovered no such item existed.

Further scrutiny of the invoice revealed that an agency employee's name was listed as the buyer. The individual on the invoice was a real employee at their agency but was not in their division, so should not have placed an order for their group. The date of the invoice matched his start date, which is typically when new staff get new equipment.

The agency has a centralized procurement office that procures the products, but each division is authorized to purchase small dollar items. The invoice was addressed to Rhonda, who is authorized to approve invoices not handled by procurement staff. Rhonda said that the invoice was routed to her from the procurement office since it had her name on it. Rhonda was going to process the invoice for payment but did not know which account code she should use, as it was not a normal purchase the division would make.

Case Study – Audience Analysis?

Why stop and look at the invoice?

Why didn't Rhonda just guess where to code the purchase and process the invoice?

Why didn't procurement look further at the invoice and compare to the accounting system?

Scope of the problem?

Case Study – Analysis continued



- External Fraudsters exploit public-sector systems to carry out all types of billing schemes
- Submitting invoices for goods or services never delivered (phantom billing)
- Inflating the costs of goods or services
- Duplicating invoices or manipulating supplier invoices
- Impersonating legitimate vendors
- Validation of invoices and/or New supplier
- Would your agency staff and process catch the above types of fraud?

Fraud & Risk: What to Look For

- Fraud Triangle
  - There are three factors, known as the fraud triangle, that make business fraud possible and probable: (1) pressure or a financial need, (2) an opportunity to exploit gaps in systems or controls, and (3) a way to rationalize the behavior.
- Understanding the fraud triangle elements can help managers place the right checks and balances in place to reduce risk.

- With the fraud triangle in mind, look for:
  - Internal control weaknesses
  - Operational gaps
  - Areas that need process improvement

Current Fraud Trends

STATE of KANSAS and CURRENT TRENDS
Check Tampering and Alteration / Washing
Expense Fraud
Emails impersonating employees, suppliers, or other state agency staff requesting assistance
Internal Fraud – Employee expenses reports, employees and suppliers working together, employees creating fake invoices
Payroll fraud
Technology-Enabled Fraud or AI
Agency Policy and Processes not followed
Procurement Fraud

Match the Fraud Term

Do you know your fraud terms?

Match each fraud term (1-12) with the correct definition (A-L).

Fraud Terms	Definitions
1 Artificial Intelligence (AI)	A A scam delivered through text message, often containing a malicious link or urgent request.
2 Generative AI	B A new type of computing that could solve certain complex problems much faster than today's computers and may eventually impact current encryption methods.
3 Phising	C A fraudulent email or electronic message that attempts to trick someone into clicking a link, opening an attachment, or providing sensitive information.
4 Data Analytics	D An identity created using a combination of real and fake personal information for fraudulent purposes.
5 Social Engineering	E Technology that can perform tasks like recognizing patterns, analyzing information , and making predictions. It can also be misused to support fraud schemes.
6 Smishing	F Manipulating people into providing information, transferring money, or taking another action that benefits a fraudster.
7 Synthetic Identity	G Technology that creates new content, including text, images, audio, and video, which can be used to create convincing fraudulent communications.
8 Vishing	H A fraudster impersonates a trusted person or organization, usually through email, to trick you into sending money or changing payment information.
9 Payment Diversion Fraud	I Examining large amounts of data to identify patterns, trends, or unusual activity that may indicate fraud.
10 Quantum Computing	J A fraudulent phone call or voice message used to obtain sensitive information.
11 Deepfake	K A fraudster tricks an organization into redirecting a legitimate payment to a fraudulent account.
12 Business Email Compromise (BEC)	L Mechanism that includes a video, photo, or audio recording that seems real but has been manipulated with artificial intelligence technologies.

How did you do?

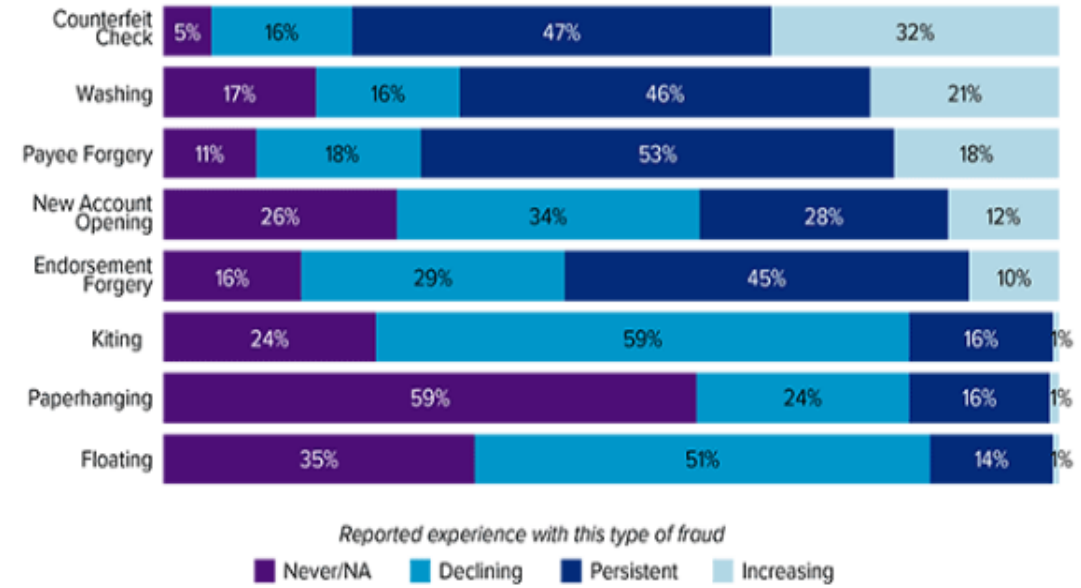
10-12 correct	7-9 correct	4-6 correct	0-3 correct
Fraud Fighther	Fraud Detective	Fraud Spotter	Keep learning!

KANSAS AGENCY BUSINESS SUMMIT

2026 Fraud Risk Report
(The Federal Reserve, May 2026)

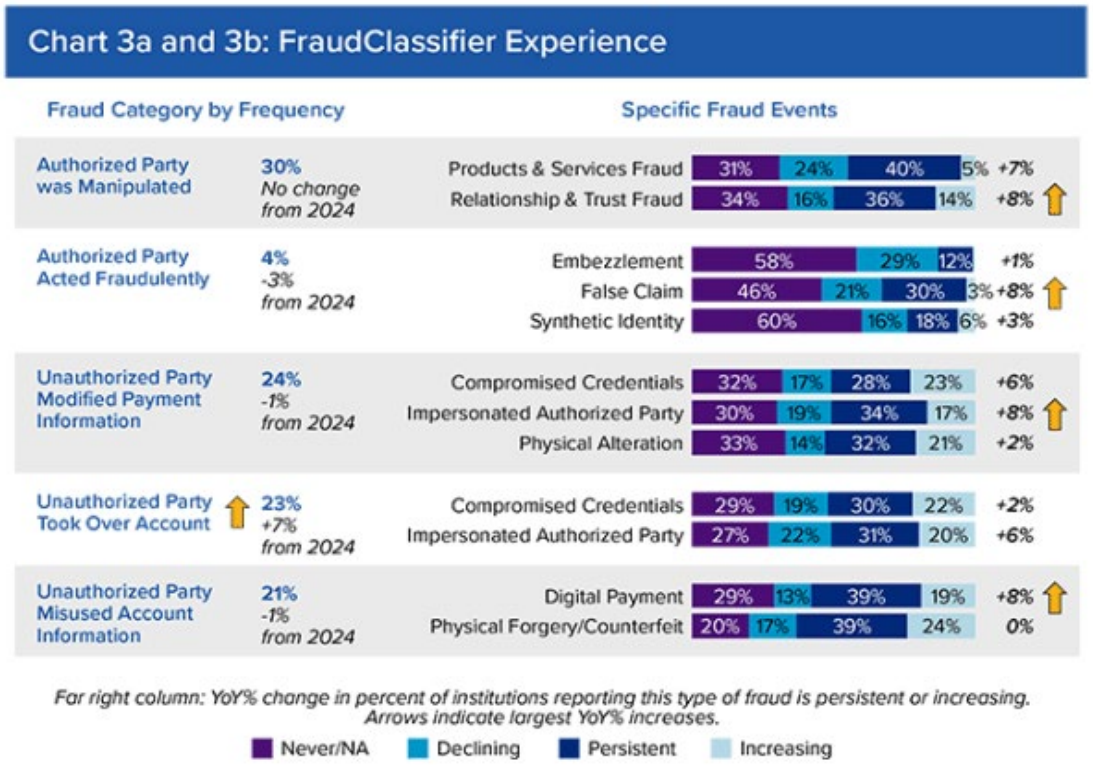
- Sixty-three percent of financial institutions reported check fraud attempts in the prior 12 months. Further, 32% of respondents noted an increase in counterfeit checks, while others saw jumps in check washing (21%) and payee forgery (18%).

Chart 2a: Specific Check Fraud Events



- Account takeover fraud is emerging as a trend, with 23% of surveyed financial institutions affected — a 7% increase year over year.

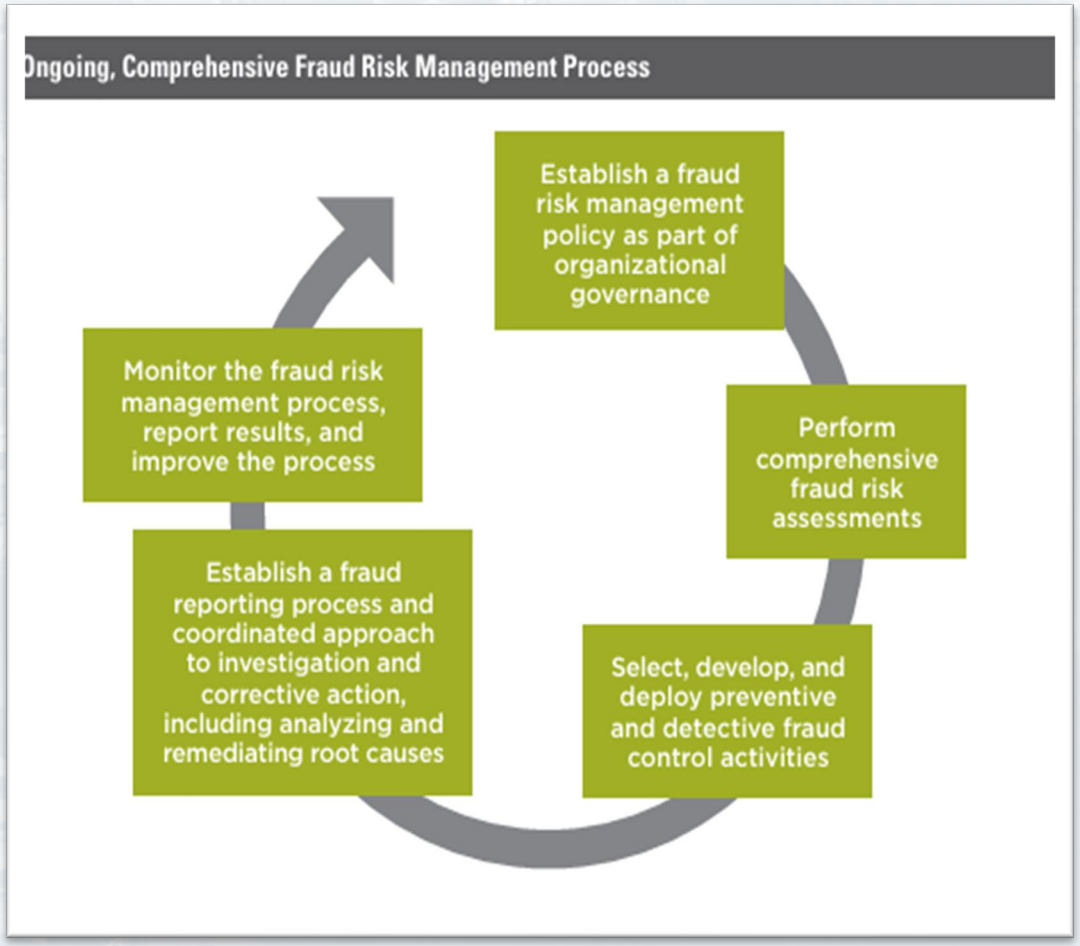
Chart 3a and 3b: FraudClassifier Experience



KANSAS AGENCY BUSINESS SUMMIT

Fraud Risk Management

Strong Agency Policy and Procedures	Standardize supplier invoice submission and document requirements	Setup shared email boxes
Enhance Supplier verification and authentication	Implement and enforce robust internal controls	Review, Audit, and Test processes
Employee Training and awareness	Create an Organizational Culture to Combat Fraud at all levels of the agency	Whistleblower protections and reporting channels
Utilize the GAO Greenbook as a guide to provide additional structure	Identify and Assess Agency Program's fraud risk profile	Plan and Conduct fraud risk assessments to programs and operating environment



Reporting & Response

Internal Controls Website

- Developing a Financial Risk and Prevention Resource page (DoA website)
- Fraud Risk Assessment
- Internal Controls Team Email - OARControls_Compliance@ks.gov

SMART/SHARP Tile for Fraud Events

- Centralized Fraud or Suspicious Reporting – Fraud Checklist
- Process of tracking fraud and recovery of funds

Office of Inspector General division of Kansas Attorney General's Office

- Reporting Fraud, Waste, or Abuse | Kansas cash, food, and health assistance programs

Annual Internal Controls Agency Self-Assessments – Kick-off Monday, October 19th

- Agency staff evaluate the effectiveness of risk and controls with self audit

Fraud Prevention - Resources

- FBI Internet Crime Complaint Center - Home Page - Internet Crime Complaint Center (IC3)
- Department of Treasury Financial Crimes Enforcement Network - United States Department of the Treasury Financial Crimes Enforcement Network - Home | FinCEN.gov
- U.S. Government Accountability Office Reports
- GAO-26-109100, Combating Fraud: Managing Risks in Federally Funded, State-Administered Programs [Reissued with revisions on Aug. 7, 2026]
- GAO Antifraud Resource
- A Framework for Managing Fraud Risks in Federal Programs | U.S. GAO
- Association of Certified Fraud Examiners (ACFE) - Association of Certified Fraud Examiners
- State Financial Officers Foundation (SFOF) - State Financial Officers Foundation (SFOF) - Look to the States
- The Federal Reserve – Home | FedPayments Improvement

Lines of Defense

Controls are the responsibility of all Agency staff, even the small things

Monitor, Analyze Red flags, Question Processes, Document everything

Independent Reviews, Central reporting and oversight, speak up when things don't seem right



Questions?

KANSAS AGENCY BUSINESS SUMMIT