



WIPFLI

Has Your Fraud IQ Kept Pace with Your Fraud Risk

Iowa Bankers Association

2026 Annual Convention

September 21, 2026

Table of contents

Introductions

Financial Institutions' risk perspectives **01**

Current risks — what we see **02**

Future risks **03**

Resources **04**

Ask questions

Presenter



Matt Storlie, CFE, CIDA

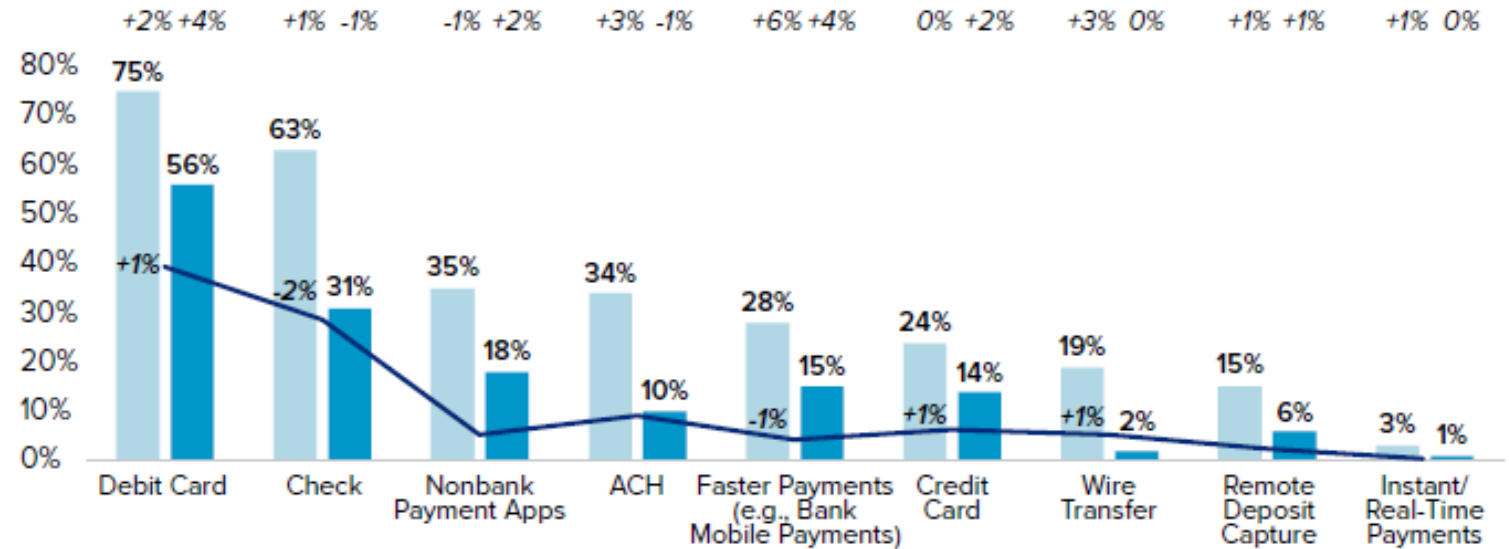
Senior Manager, Forensic & Litigation Services

01

Financial Institutions' risk perspectives

Financial Institutions' risk perspectives

Chart 1: Fraud Risk Summary by Payment Type



Percentages in italics at the top of the chart show year-over-year percent change in the portion of surveyed financial institutions reporting attempts and losses.

Percentages in italics on top of bars show YoY% change in total payment losses.

■ % Financial Institutions Experiencing Attempts

■ % Financial Institutions Experiencing Losses

■ % Total Payment Losses

Annual Federal Reserve Financial Services
(FRFS) Financial Institution Risk Officer Survey (2026)

Financial Institutions' risk perspectives

Illustrative challenges

“Balancing system limitations, mitigation tools and member experience. The more secure you make your systems, the more inconvenience it places on the account holders.” *Large Credit Union*

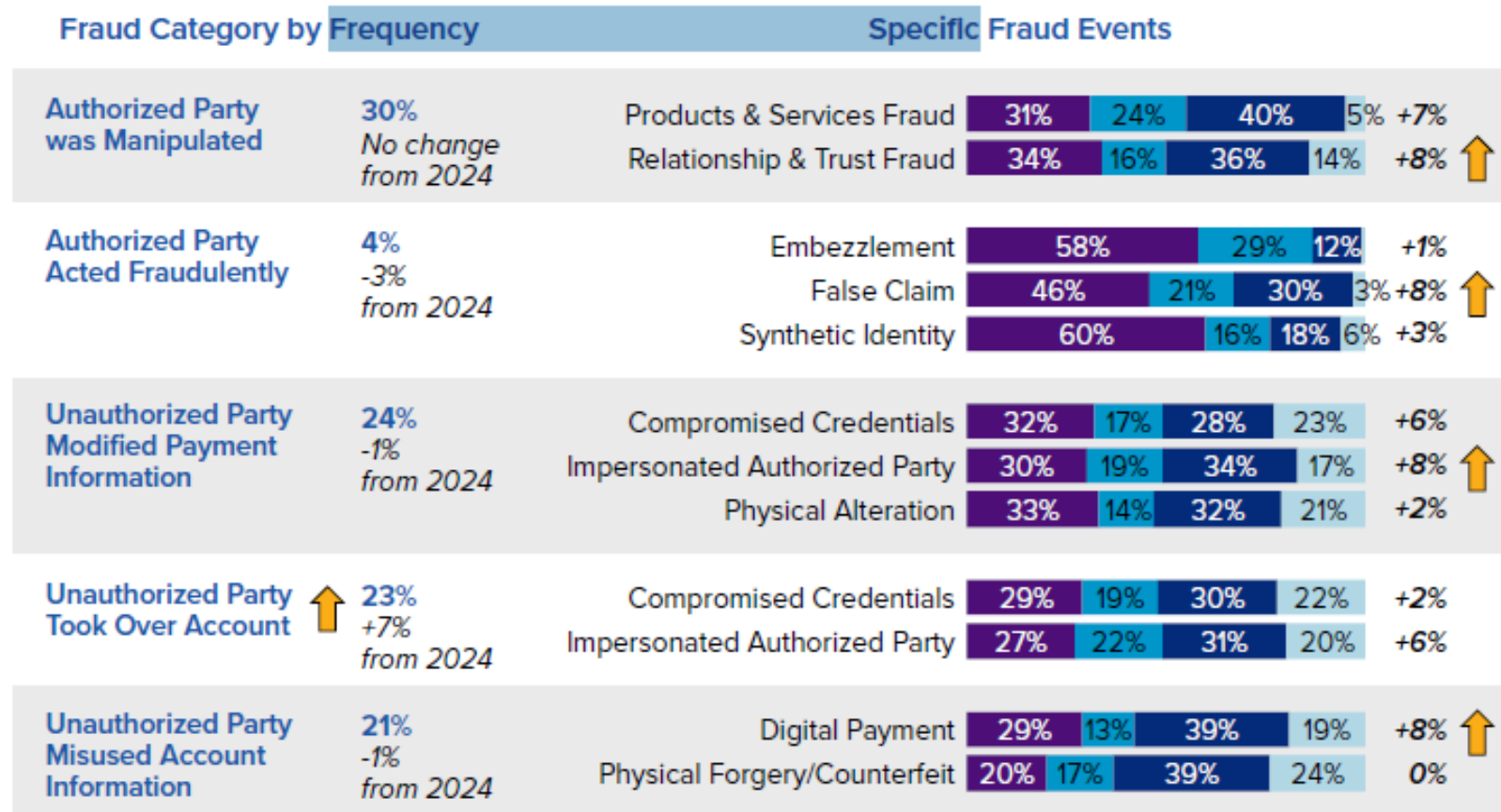
“Keeping our employees aware of current trends and red flags of fraud. As scams are always evolving and changing, training our staff what to watch for becomes more difficult.” *Regional Commercial Bank*

“Limited system integration and data visibility create delays in detecting anomalies, while resource constraints and manual workarounds increase residual risk. Strengthening automation, cross-platform alerts and capacity alignment is essential to close these gaps.” *Regional Commercial Bank*

Annual Federal Reserve Financial Services
(FRFS) Financial Institution Risk Officer Survey (2026)

Financial Institutions' risk perspectives

Chart 3a and 3b: FraudClassifier Experience



Far right column: YoY% change in percent of institutions reporting this type of fraud is persistent or increasing. Arrows indicate largest YoY% increases.

Never/NA
 Declining
 Persistent
 Increasing

Annual Federal Reserve Financial Services
(FRFS) Financial Institution Risk Officer Survey (2026)

Financial Institutions' risk perspectives

1. Top increases in fraud by frequency: FIs identified authorized party was manipulated (scams) as their most common fraud, 30% of the time, with a significant increase (+6%) in account takeover as the next highest increase.

2. Top increasing fraud events: Fraud events physical forgery/counterfeit (86%) and physical alteration (75%) were experienced by more FIs than any other type and were also among the top three worsening events, with 27% and 19% of FIs describing them as increasing, respectively.

3. Top decreasing fraud event: On a positive note, the greatest area of improvement appears to be in products and services fraud, declining 16% from 2023.

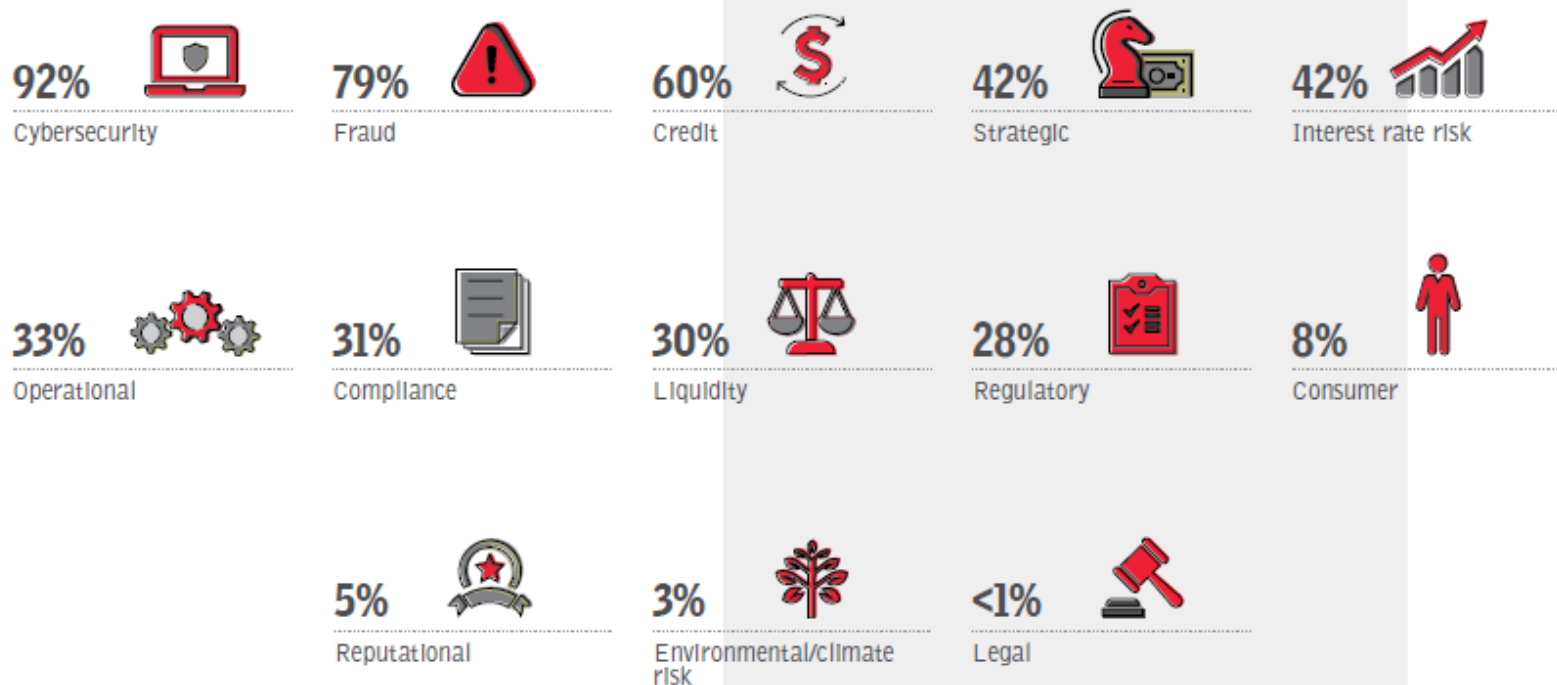
Annual Federal Reserve Financial Services
(FRFS) Financial Institution Risk Officer Survey (2024)

Financial Institutions' risk perspectives

STRATEGIC RISK

1. With respect to your bank, which five risk categories are you most concerned about for 2026?

Respondents were asked to select no more than five options.



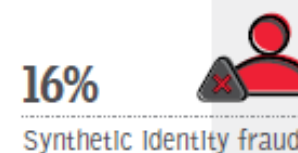
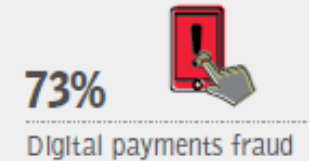
Bank Director's 2026 Risk Survey

Financial Institutions' risk perspectives

FRAUD & CYBERSECURITY

11. Have your bank or its customers been directly impacted by any of the following types of fraud over the past 18 months?

Question only asked of CEOs, CROs, CISOs, CIOs and CTOs. Respondents were asked to select all that apply.



Financial Institutions' risk perspectives

12. Did your bank take any of the following steps to address fraud concerns in 2025?

Question only asked of CEOs, CROs, CISOs, CIOs and CTOs. Respondents were asked to select all that apply.



Bank Director's 2026 Risk Survey

Financial Institutions' risk perspectives

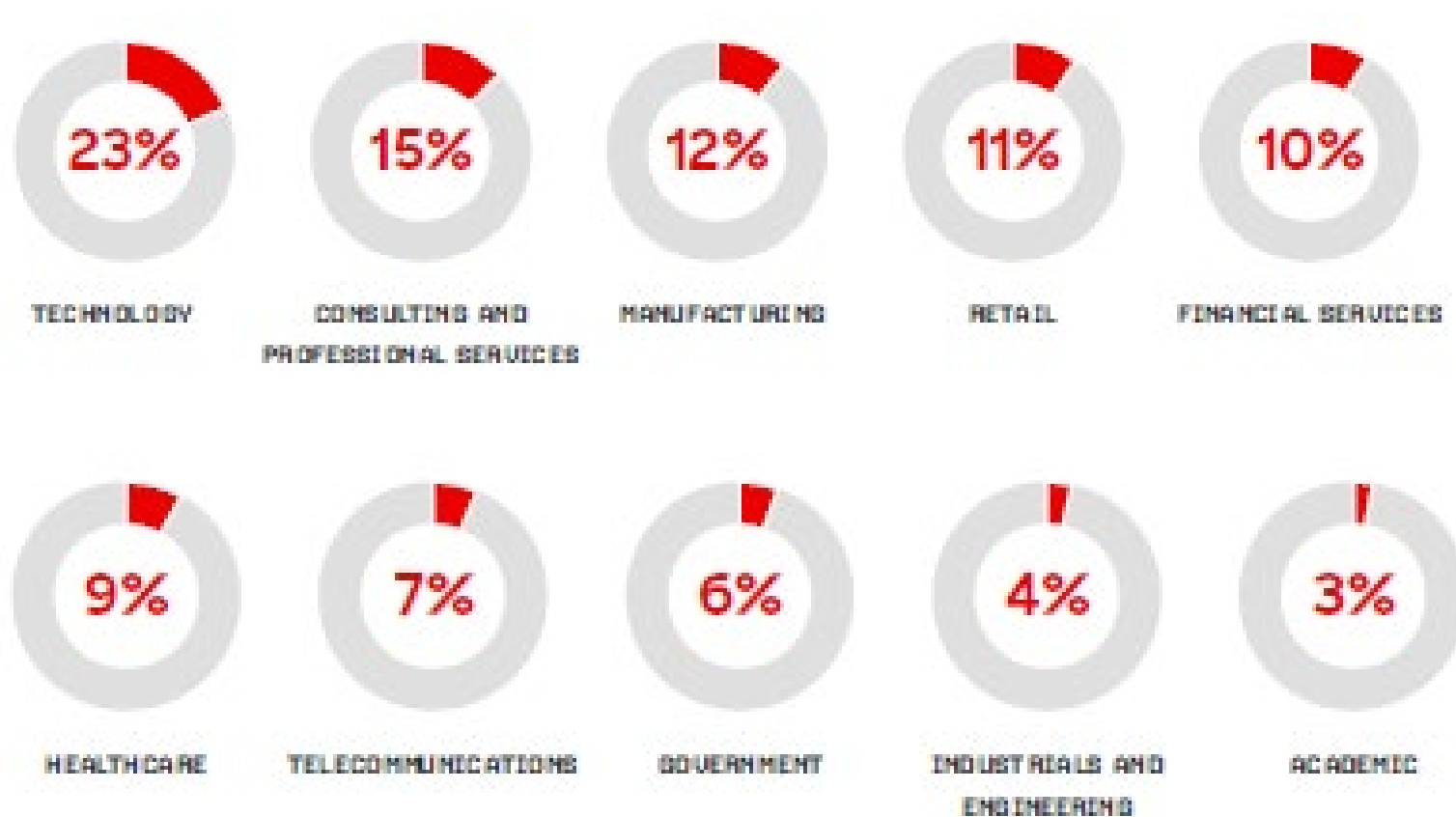


Average total cost of a data breach by industry in USD millions

IBM Cost of a Data Breach Report 2026

Financial Institutions' risk perspectives

Top 10 Industries Targeted by Interactive Intrusions



CrowdStrike 2026 Global Threat Report

Financial Institutions' risk perspectives

How much money has your organization incurred in direct fraud losses in the last twelve months?

\$0 - \$500K



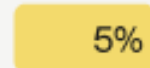
\$500,001 - \$1M



\$1,000,001 - \$5M



\$5,000,001 - \$10M



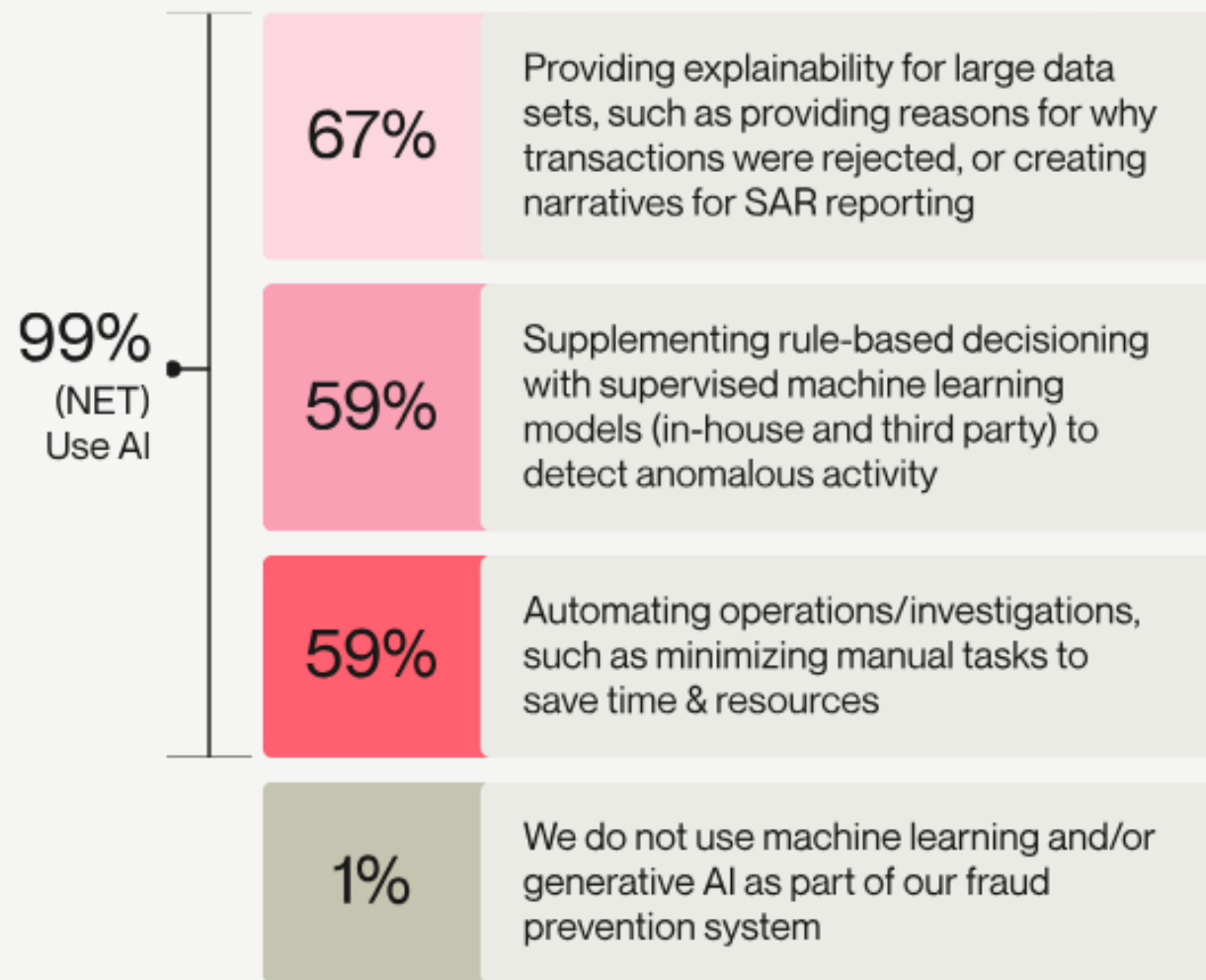
Over \$10M



Alloy's 2025 State of Fraud Benchmark Report

Financial Institutions' risk perspectives

How are you using machine learning and/or AI as part of your fraud prevention system?



02

**Current
risks—
what we see**

Current risks – what we see

- ❑ However, you quantify it – Your fraud risk is greater/higher now than it was just a few years ago
- ❑ Employees will steal
- ❑ Fraud occurs in every organization
- ❑ You won't keep perpetrators out
 - Most perpetrators have never been charged or convicted
 - Most perpetrators have never been punished or terminated
- ❑ Greatest risk is from
 - Longer tenured
 - More experienced
 - Better educated
 - More trusted

Current risks – what we see

- ❑ Estimated that organizations lose 5% of revenue to fraud
 - Median loss \$104,000
 - Average loss \$1,457,000
- ❑ Financial Statement Fraud – 6%, median loss \$1,000,000
 - Fictitious revenues, inflating assets, concealing or underreporting expenses or liabilities
- ❑ Corruption – 45%; median loss \$150,000
 - Conflict of interest, bribery, extortion
- ❑ Asset misappropriation – 90%; median loss \$100,000
 - Embezzlement, theft (cash and/or other), false expense reports, forgery, equipment

Current risks – what we see

Some factors are within your control... Some aren't



Current risks – what we see

Items largely “outside” your control

☐ Pressure

- Family stress - too much family time
- Illness, long covid,
- Income loss
- Home schooling

☐ Rationalization

- Fewer staff doing the work
- Same staff doing more work
- I’m at risk from required contact with participants, staff, public
- No work social time
- Inflation
- “I just need a loan to get through this rough patch”

Current risks – what we see

Items “slightly” within your control

☐ Employee Pressure

- May be mitigated through EAP or similar programs
- Connection with peers and leadership
- Impacted by relationship/connection
 - Peers
 - Leadership

☐ Employee Rationalization

- May be mitigated through messaging and information to staff
- Also impacted by relationship/connection
 - Organization
 - Peers
 - Leadership

Current risks – what we see

Items “mostly” within your control

- ❑ Opportunity
- ❑ Internal control environment
 - Actual Controls
 - Perceived internal
 - Changes to business processes
 - Changes in your services
 - Work from home/hybrid
 - Reduced staffing
 - Changes to your partners, service providers, clients
 - Changes at your partners, subgrantees, service providers

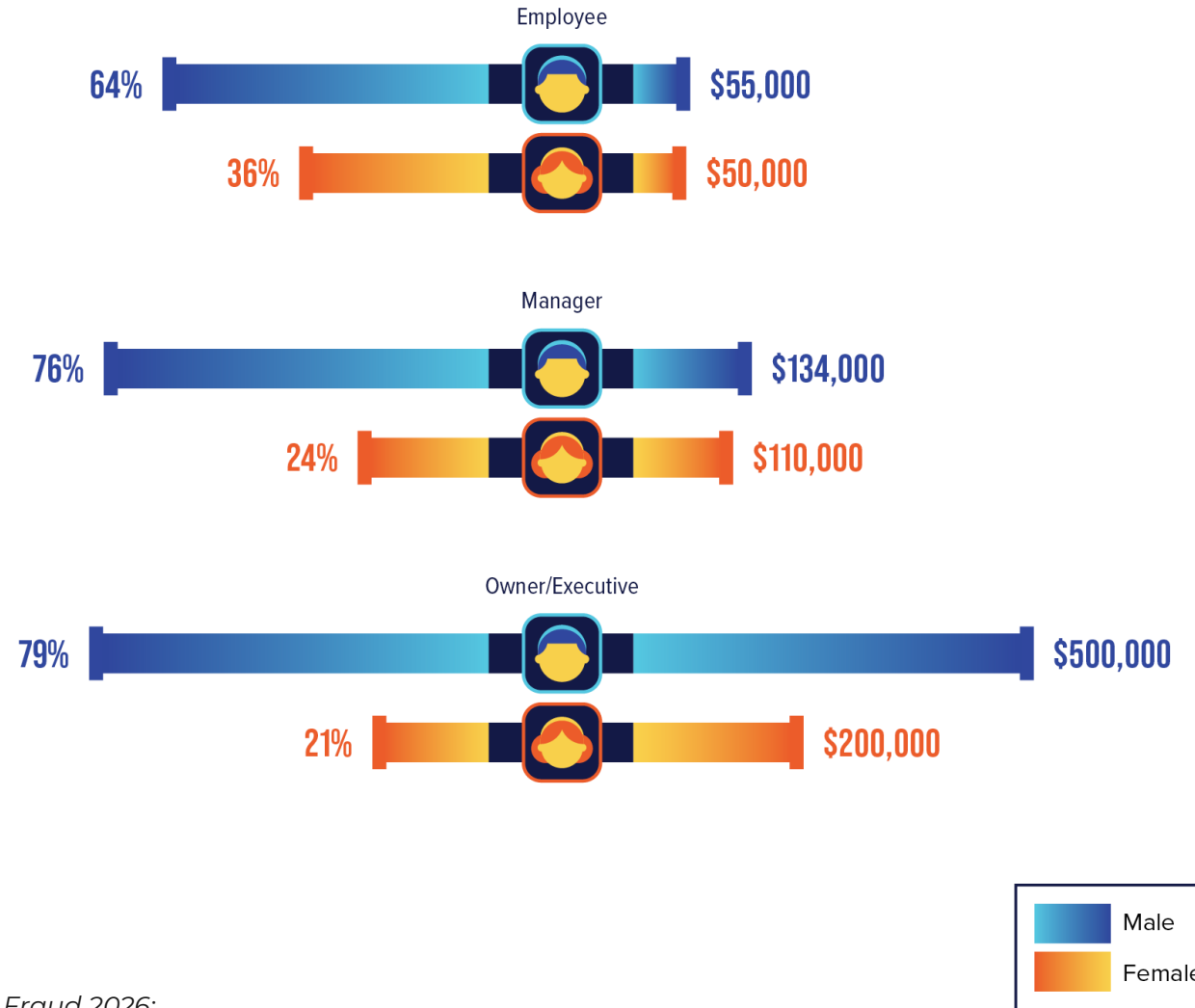
Current risks – what we see

FIG. 25 How does occupational fraud affect organizations in different industries?



Occupational Fraud 2026: A Report to the Nations. © 2026 by the Association of Certified Fraud Examiners, Inc.

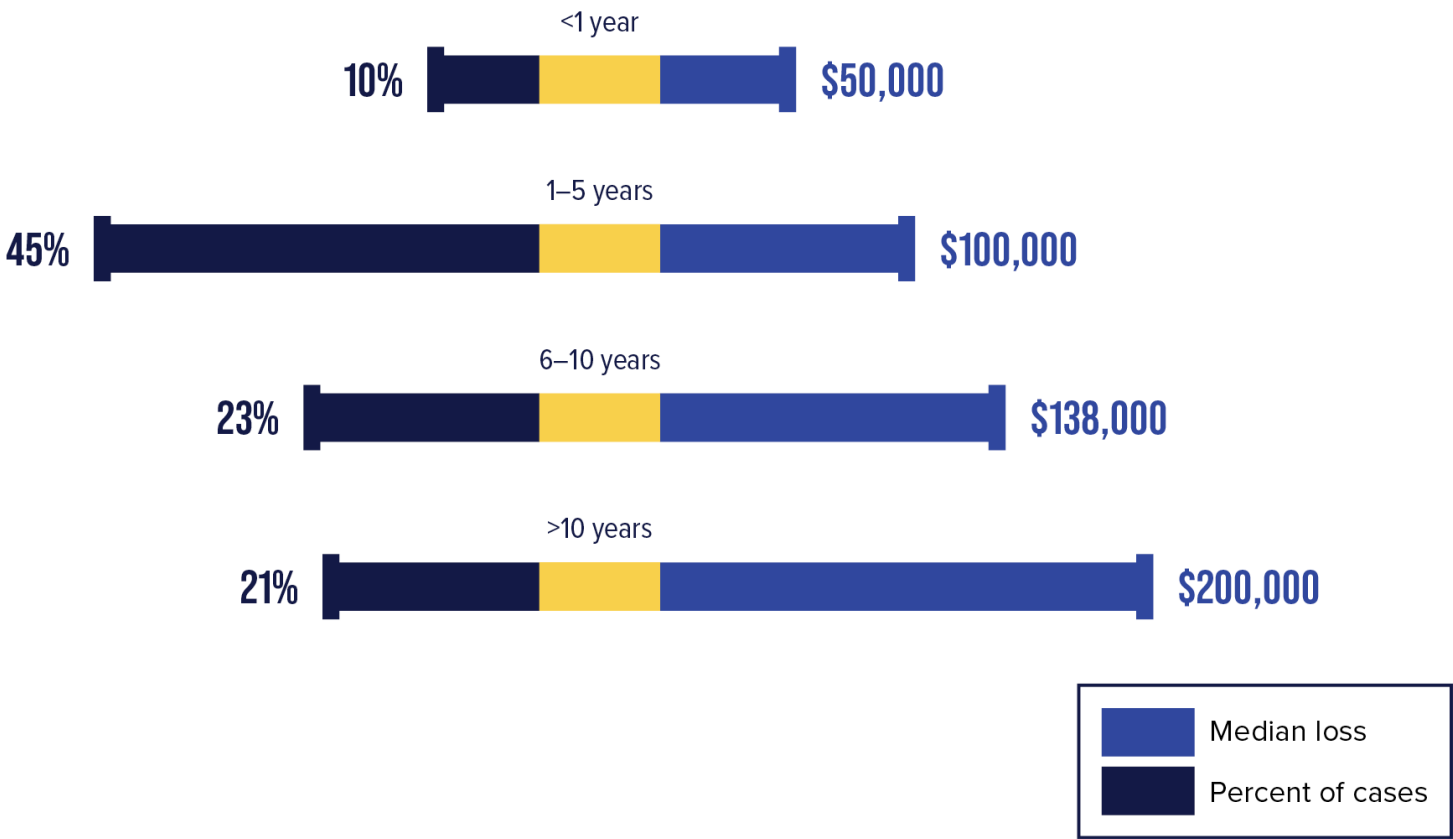
FIG. 47 How do gender distribution and median loss vary based on the perpetrator's level of authority?



*Occupational Fraud 2026:
A Report to the Nations. ©
2026 by the Association of
Certified Fraud Examiners,
Inc.*

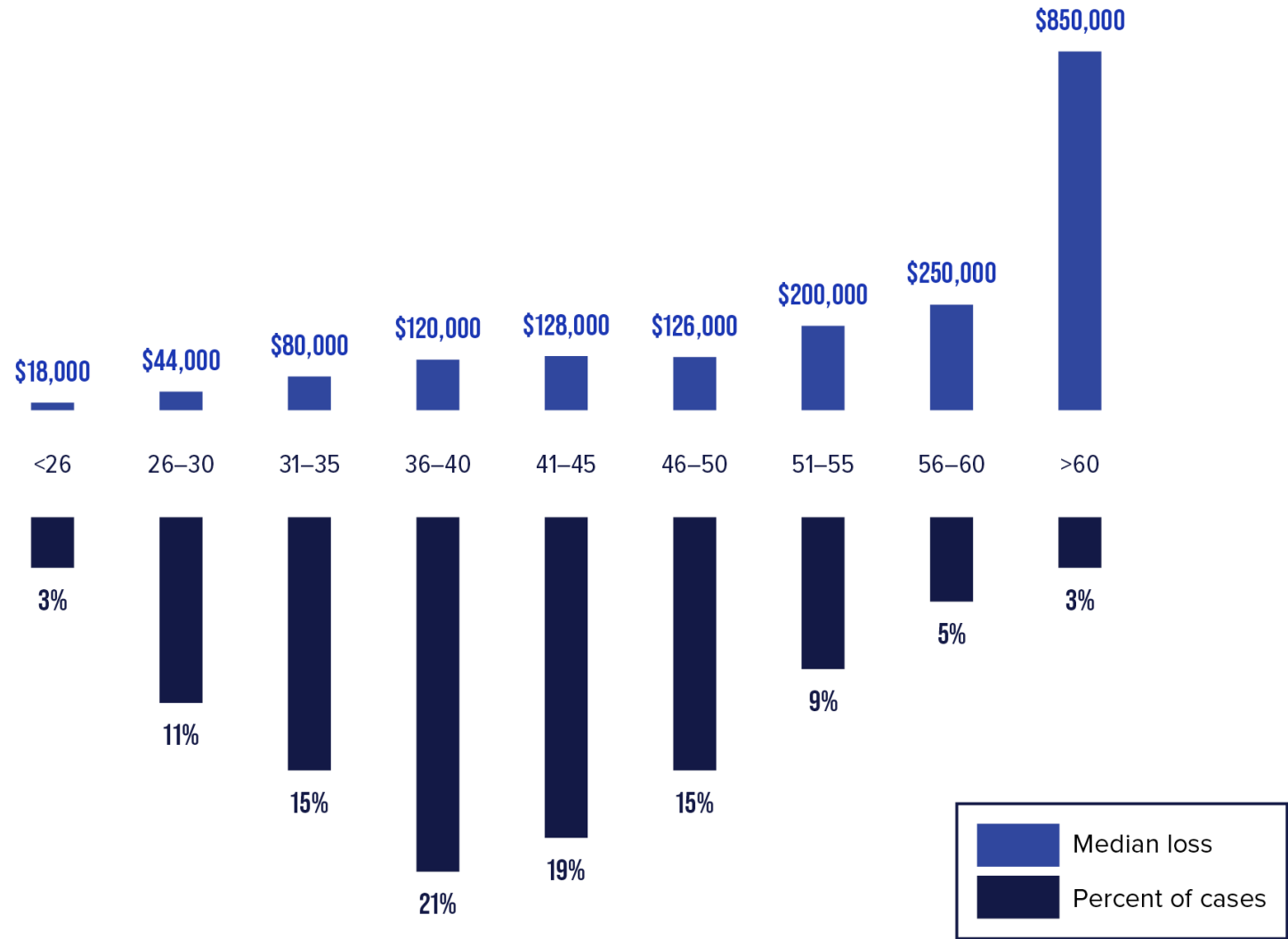
Current risks – what we see

FIG. 42 How does the perpetrator's tenure relate to occupational fraud?



Current risks – what we see

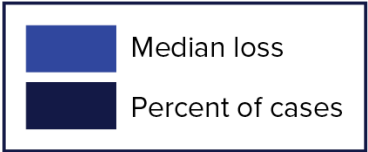
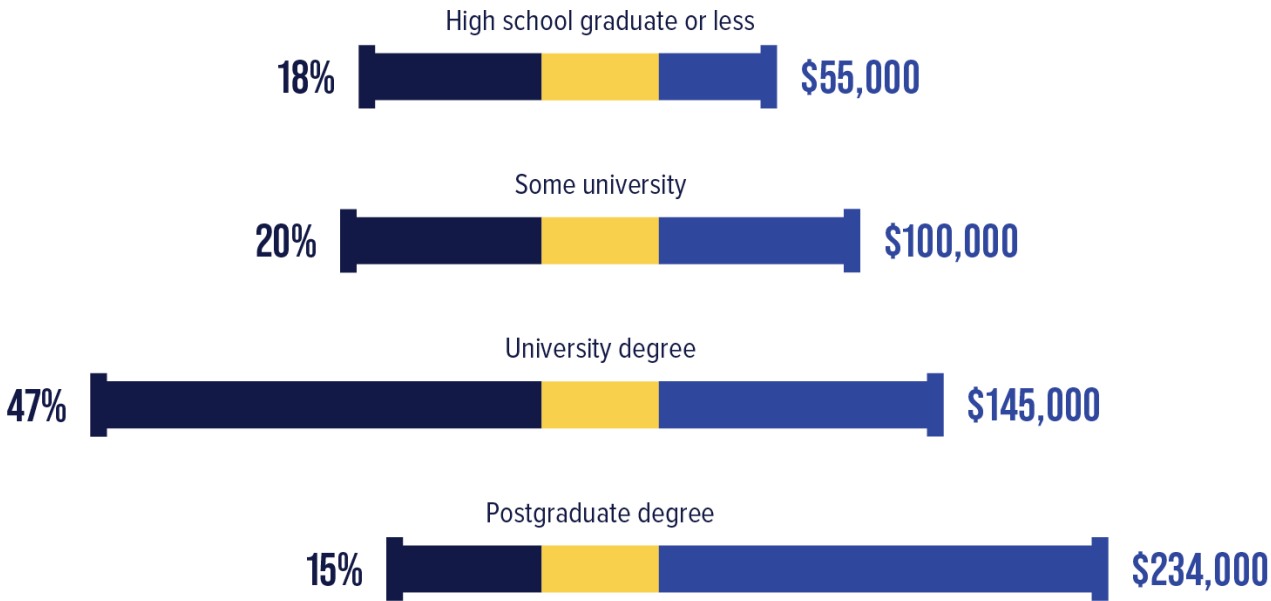
FIG. 48 How does the perpetrator's age relate to occupational fraud?



Occupational Fraud 2026: A Report to the Nations. © 2026 by the Association of Certified Fraud Examiners, Inc.

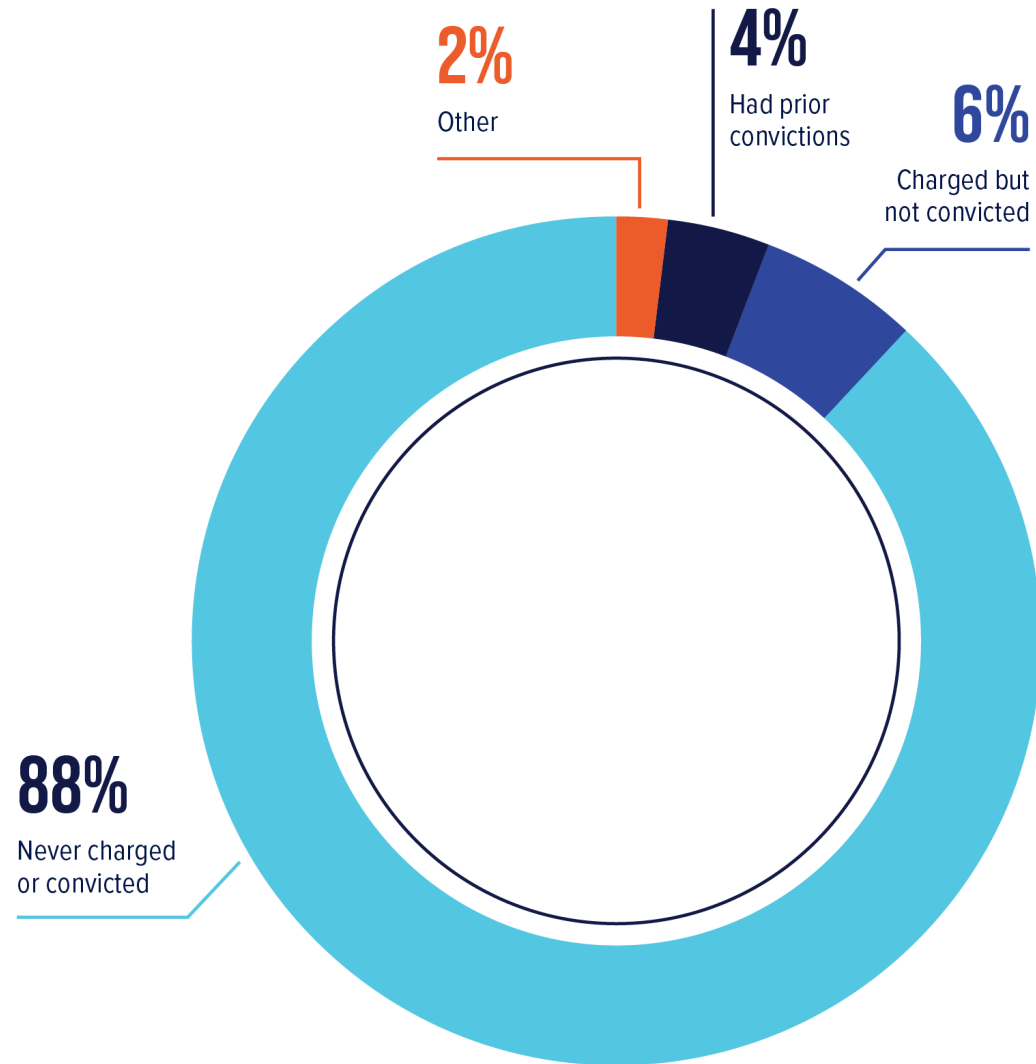
Current risks – what we see

FIG. 49 How does the perpetrator’s education level relate to occupational fraud?



Current risks – what we see

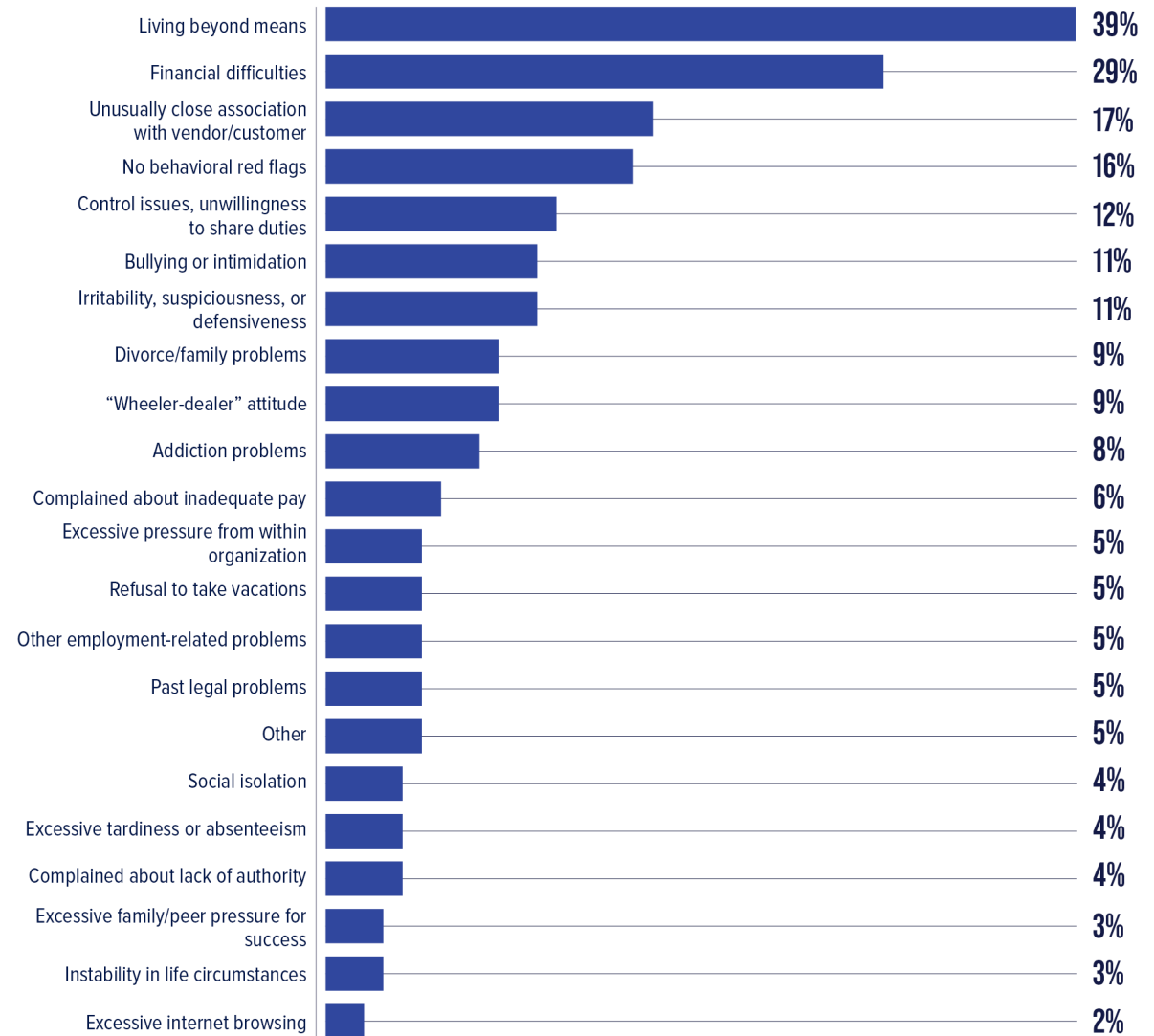
FIG. 52 Do perpetrators tend to have prior fraud convictions?



*Occupational Fraud 2026: A Report to the Nations.
© 2026 by the Association of Certified Fraud
Examiners, Inc.*

Current risks – what we see

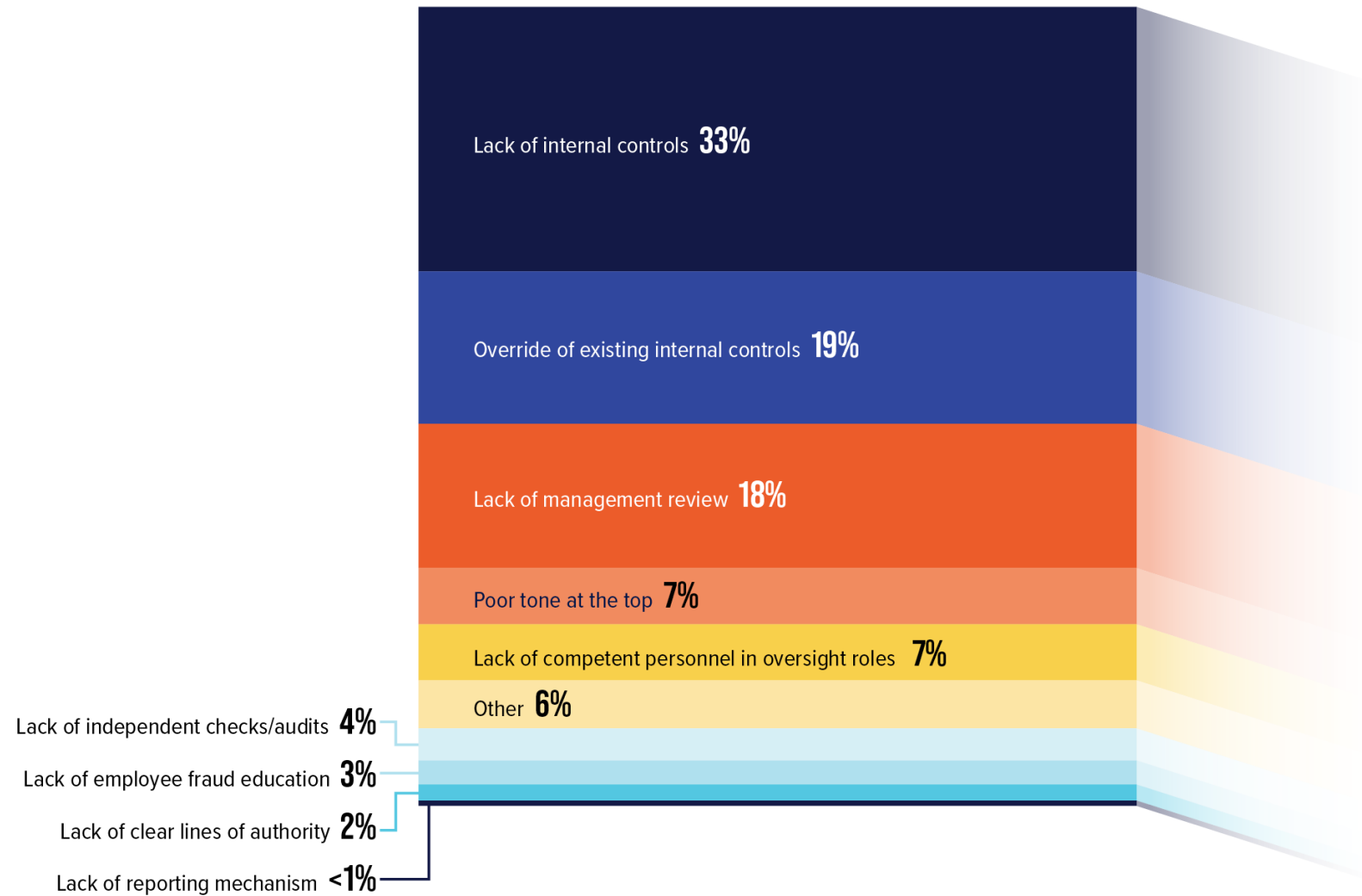
FIG. 55 How often did perpetrators exhibit behavioral red flags?



Occupational Fraud 2026: A Report to the Nations. © 2026 by the Association of Certified Fraud Examiners, Inc.

Current risks – what we see

FIG. 37 What are the primary internal control weaknesses that contribute to occupational fraud?



Current risks – what we see

Insider risks

- ❑ Misappropriation
 - Fictitious Vendor
 - Duplicate invoices
 - Credit Card/P Card
- ❑ Fixed Assets
- ❑ Fiduciary accounts
- ❑ Payroll

Current risks – what we see

External risks

❑ Breaches

- Ransomware
- Exfiltration

❑ Attempted account takeovers

- Associated with “bursts.”
 - “Have we been breached?”
 - We believe they are associated with other breaches.

❑ Payment / information misdirection

- Business email compromise
 - Bank system, 3rd-party system

Current risks – what we see

Address the three components of the “Fraud Triangle”

- ❑ Pressure
 - Work environment
 - Total rewards
 - EAP
- ❑ Rationalization
 - Work environment
 - Communication from leadership
 - EAP
- ❑ Opportunity
 - Actual Internal Control environment
 - Perceived Internal Control environment

Current risks – what we see

Frequently employed internal control measures

- ☐ Policies and procedures
- ☐ Segregation of duties:
 - Job rotation or cross- functional “splitting”
- ☐ Management review – Must be meaningful
- ☐ Surprise audits/internal audit
- ☐ Employee support/assistance programs
- ☐ Hotline
- ☐ Data analysis
- ☐ External audit

Current risks – what we see

Lessons from an \$8 million fraud at ING in Twin Cities

JOURNAL OF
ACCOUNTANCY



Nathan
Mueller

- Life insurance company ReliaStar bought out by ING
- An expert on the ERP system as part of changeover team
- Found out he had authority to approve checks up to \$250k
- Realized he could login as someone else, request a check, then login as himself to approve his own check request
- Started small and paid off \$88K of credit card debt
- Check returned to him from AP without any questions
- Set up phony business and stole \$8M from 2004-2007

03

Future risks

Future risks

AI poses the biggest risk

- ❑ The confluence of AI trends will increase the risk.
- ❑ Deepfake technology
 - Audio cloning
 - Video cloning
 - Document forgery
- ❑ Generative AI

Future risks

Deepfake technology

- ❑ Improvements in deepfake technology will make it more difficult to combat fraudsters armed with more complete information.
- ❑ Customers will have a more difficult time preventing:
 - Payment misdirection.
 - Unauthorized payments.
- ❑ FIs will need to adapt security measures to account for deepfake technology.

Future risks

Deepfake technology is improving

- ❑ Currently, you only need six to 60 seconds to create a deepfake.
- ❑ Audio (voice cloning)
 - As few as three words needed to make a passable deepfake.
- ❑ Video
 - Under one minute for face swaps.
- ❑ Full synthetic video generation
 - Nothing needed.

Future risks

Generative AI

- ❑ If we (legitimate business users) can point AI tools at large data, why can't/wouldn't fraudsters?
 - Customers/individuals are poor at security hygiene.
 - There are more frequent breaches with exfiltration.
 - AI will lead to more complete dossiers for use by fraudsters.

Future risks

Deepfake + Gen AI

- ❑ Marrying generative AI and deepfake technology will pose significant problems.
- ❑ Businesses and individuals need to adjust internal controls to account for this.
 - Your customers
 - Your employees

Future risks

Deepfake + Gen AI

- In 2019, fraudsters cloned the German executive's voice with AI.
 - The CEO of a U.K. energy company was certain he'd talked to the head of his firm's parent company in Germany. He recognized his boss's German accent and lilt over the phone, so when the boss urgently instructed him to transfer 220,000 euros (\$243,000) to the company's supplier in Hungary, the CEO didn't hesitate. But what the CEO thought was a request to pay a vendor became the earliest known deepfake attack against a company.

Future risks

Deepfake + Gen AI

- 2024 deepfake attack against multinational engineering firm, Arup.
 - In this scheme, criminals choreographed an elaborate multi-person video conference call featuring synchronized deepfakes of the company's chief financial officer and senior staff. The video conference was so convincing that the only real employee invited to the meeting authorized transfers totaling \$25.6 million.

04

Resources

Resources

Resources	Websites
The Federal Reserve	frbservices.org
American Bankers Association	aba.com
Bank Director	bankdirector.com
Nacha	nacha.org
Insurance Accounting & Systems Association (IASA)	iasa.org
Alloy	alloy.com
CrowdStrike	crowdstrike.com

Resources

Resources	Websites
SANS (SysAdmin, Audit, Network, Security) Institute	sans.org
Computer Emergency Response Team at Carnegie Mellon University's Software Engineering Institute	cert.org
International Organization of Standardization (ISO)	iso.org
National Institute of Standards and Technology (NIST)	nist.gov/cyberframework
Federal Financial Institutions Examination Council (FFIEC)	ffiec.org

Resources

Resources	Websites
Association of Certified Fraud Examiners	acfe.com
Transparency International (Corruption Perception Index)	transparency.org
The Institute of Internal Auditors	theiia.org
Open Compliance and Ethics Group	oceg.org
International Association of Financial Crimes Investigators	iafci.org
Society of Corporate Compliance and Ethics	corporatecompliance.org
American Institute of Certified Public Accountants – Forensic and Valuation Services	fvs.aicpa.org

Resources

Resources	Websites
The Committee of Sponsoring Organizations of the Treadway Commission (COSO)	coso.org
Chartered Institute of Management Accountants	cimaglobal.com
ASIS International	asisonline.org
The Serious Fraud Office (UK)	sfo.gov.uk
Information Systems Audit and Control Association	isaca.org
U. S. Department of Justice	usdoj.gov
U.S. Securities and Exchange Commission	sec.gov

Questions?

Matt Storlie

Senior Manager

matt.storlie@wipfli.com

651 556 2236

wipfli.com

"Wipfli" is the brand name under which Wipfli LLP and Wipfli Advisory LLC and its respective subsidiary entities provide professional services. Wipfli LLP and Wipfli Advisory LLC (and its respective subsidiary entities) practice in an alternative practice structure in accordance with the AICPA Code of Professional Conduct and applicable law, regulations, and professional standards. Wipfli LLP is a licensed independent CPA firm that provides attest services to its clients, and Wipfli Advisory LLC provides tax and business consulting services to its clients. Wipfli Advisory LLC and its subsidiary entities are not licensed CPA firms.

WIPFLI