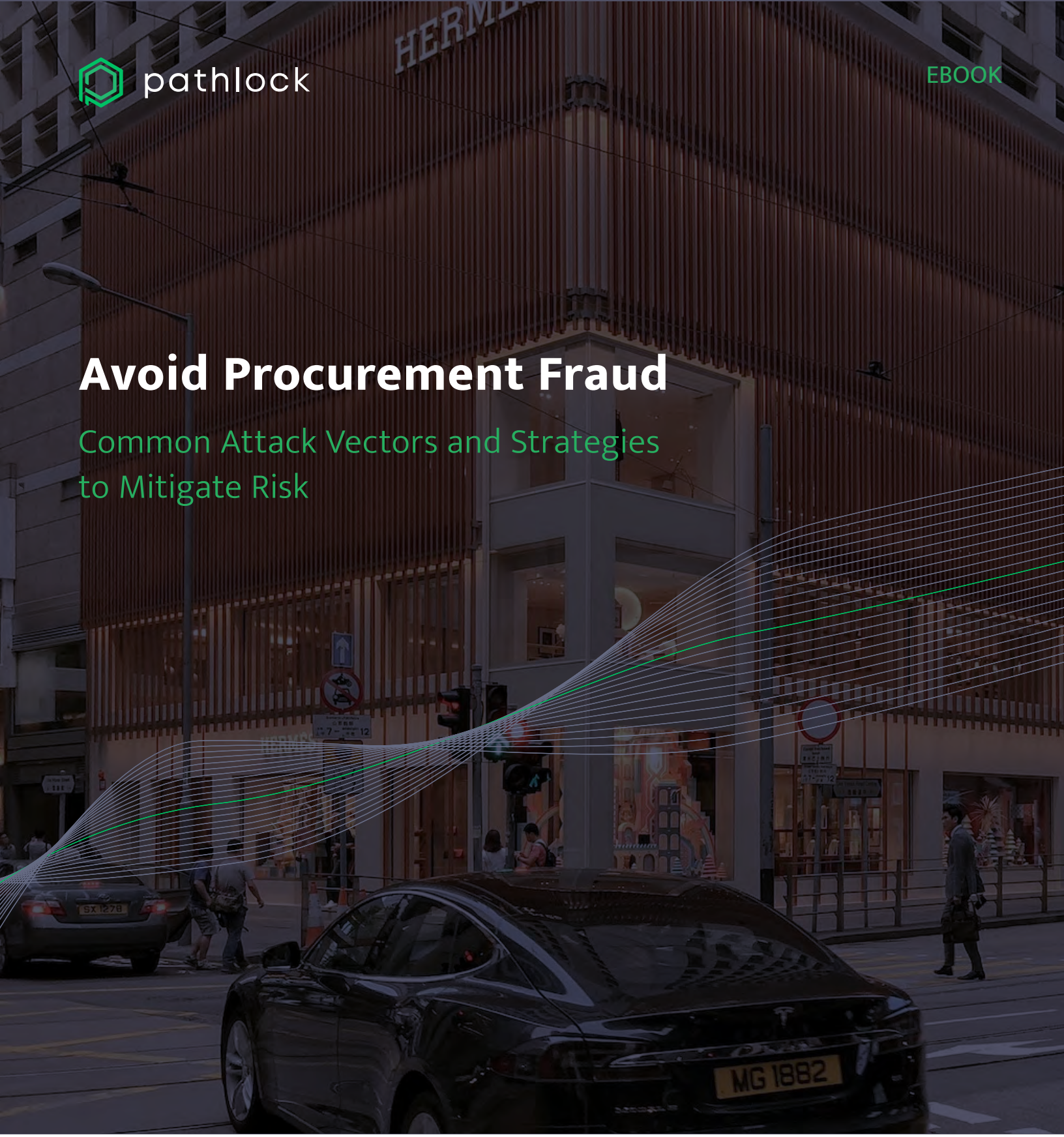
pathlock

EBOOK



Avoid Procurement Fraud

Common Attack Vectors and Strategies to Mitigate Risk

270 S. Main St., Flemington, NJ 08822
T +1-908-782-5700
info@pathlock.com

Insider Threats are on the Rise

Did you hear about the insider fraud that occurred at Amazon in 2020? One of the company's selling support associates in Arizona used his employee access to falsely and fraudulently issue 318 unauthorized refunds to himself and others, totaling over $95,000.[1] If you're familiar with the insider threat landscape, this isn't a surprising event, even for a company as tech-savvy as Amazon.

Just a few years ago, a fraud incident like this one qualified as big news. In 2018, when a director of alliances at Microsoft was indicted for creating fake invoices totaling $1.4 million and then changing bank account information to route payments to his personal accounts, it made headlines around the world. Now, for fraud trackers, it's just another day at the office.

> ***In 2020, actors within purchasing departments accounted for 5% of all reported fraud cases, with a median loss of $200,000 per case.***

Revelations of procurement fraud have become commonplace. Uncertain economic conditions in the pandemic year of 2020 created an environment ripe for fraud as workers became concerned about their next paycheck. At the same time, supply chain disruptions and the dramatic increase in remote work exposed vulnerabilities in the internal controls and security postures of many organizations.

Under these conditions, the number of insider threat incidents increased globally by 47% between 2018 and 2020.[2] In the U.S. alone, businesses encountered approximately 2,500 internal security breaches daily, and more than 34% of businesses worldwide were affected by insider threats annually.[3] In 2020, actors within purchasing departments accounted for 5% of all reported fraud cases, with a median loss of $200,000 per case.[4]

Today, every company is a potential target of procurement-related insider threats. The question is: How will you minimize your exposure?

In this eBook you'll learn:

- Which types internal control weaknesses lead to procurement fraud
- Why legacy security solutions aren't sufficient to protect your procurement processes
- How you can prevent procurement fraud and mitigate exposure with integrated security controls

SOX is designed to prevent procurement fraud. So why isn't it working?

The primary goal of Sarbanes Oxley (SOX) is to enforce transparency into business processes and financial transactions to ensure that public enterprises are employing accepted accounting principles. Non-public companies are also encouraged to follow SOX as a framework for accounting best practices.

Internal Controls for Financial Reporting (ICFR), which allow for the monitoring of financial processes and verification of transactions, are essential mechanisms of SOX compliance. Internal controls govern and audit access to business-critical IT systems, such as procurement software and specific transactions executed within that software.

Segregation of Duties (SOD) is fundamental to sustainable risk management and internal controls. The principle of SOD disperses critical functions of business processes to more than one person or department. In the case of procurement, for example, one person shouldn't be able to a) create a new vendor and b) authorize payment for that vendor. Too much concentrated power is a violation of SOD and an invitation for procurement fraud.

Financial transactions cross many applications in a modern enterprise

As organizations grow larger and more distributed, they leverage an increasingly diverse set of technologies to conduct business. Financial transactions take place across a wide range of systems. Enterprises may have multiple ERP systems, such as SAP, Oracle, and Netsuite. They may have procurement applications related to their ERP, such as SAP Ariba, and tools that aren't integrated completely with the rest of the financial or security IT suite.

Architecting and enforcing appropriate ICFRs such as SOD across multiple teams, geographies, and applications is more difficult than ever before. Even with the best of intentions, organizations often fail to establish the oversight, change management, and audit processes needed to defend against procurement fraud.

Yesterday's Enterprise	Today's Enterprise
• 1-3 relevant systems and applications • On-premises infrastructure • Dedicated workstations • Static user base	• 10+ enterprise systems with business-critical info • 1m+ transactions/processes involving multiple systems • On-premises - Public / Private Cloud - Hybrid - SaaS • Virtualized - Microservices • Diverse security models/roles/permissions management • BYOD - Remote workforces - Contractors

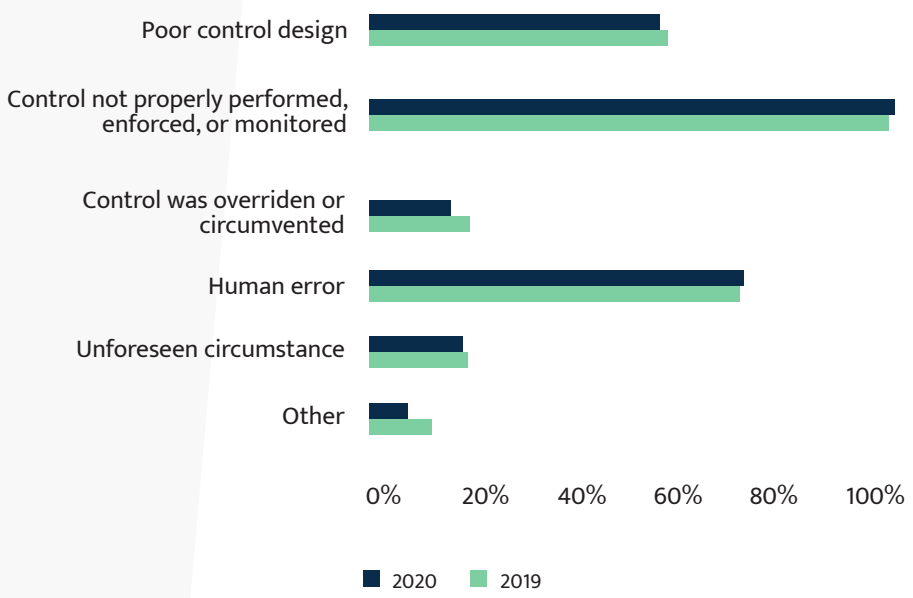
Legacy, manual approaches drive internal control failures

Control issues rose 4% in the past year, according to the 2020 *State of the SOX/Internal Controls Market Survey.* Respondents reported more control issues compared to the year prior, and the most cited cause was "control not properly performed, enforced, or monitored." "Human error" and "poor control design" were also commonly cited causes of failures.[5]

To anyone experienced in helping organizations meet SOX obligations, these findings aren't surprising. Traditionally, the development, management, and enforcement of ICFRs has been conducted in a largely manual fashion. As a result, the effort required to design, operate, audit, and document an organization's ICFR protocols is incredibly burdensome, and the resulting programs are highly prone to human error.

> ***"At this crucial point, financial executives will have to be more mindful about incorporating great amounts of flexibility and resiliency to support a future that seems less forgiving to manual processes and in-person collaboration."***
>
> –Andrej Suskavcevic,
> President and CEO of Financial Executives International and Financial Education & Research Foundation

What were some of the causes for control failures?



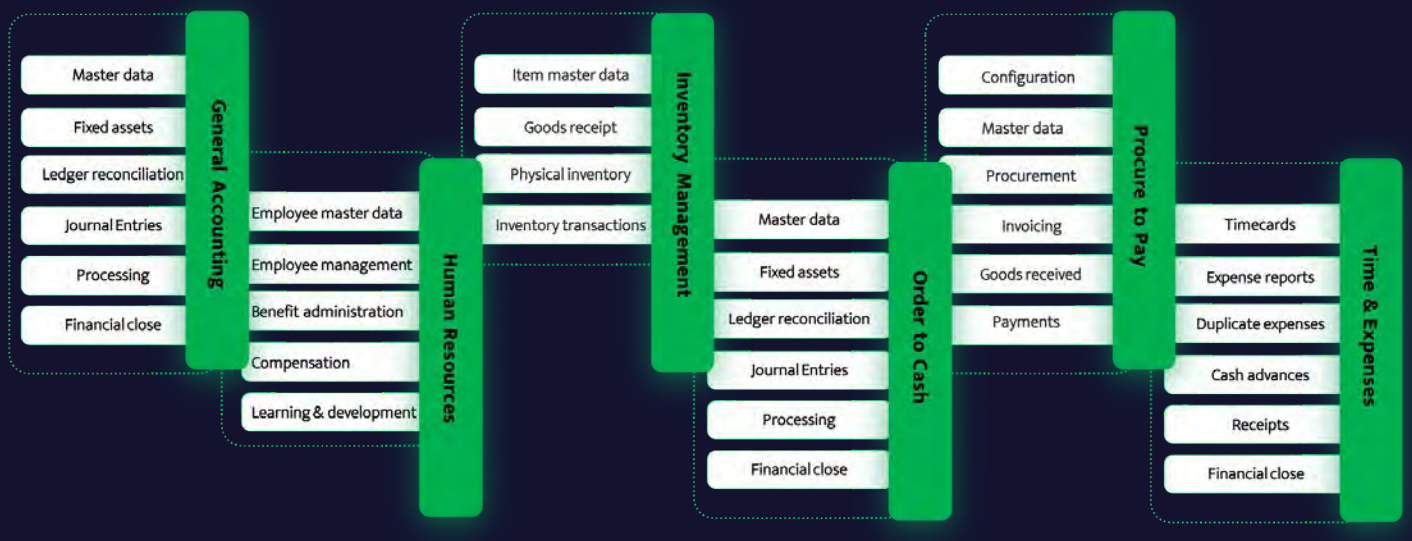
Measuring hypothetical risk isn't sufficient to understand business impact

One of the greatest weaknesses of the legacy approach to ICFR management has been its focus on potential user activity and hypothetical risk, rather than actual user activity and measurable risk. In the legacy model, point-in-time analysis estimates risk based upon theoretical user activity. The approach asks: "What damage could someone do given the access they have? What would be the impact if that activity happened?"

The hypothetical approach may have been adequate in the past, when most organizations used a limited number of systems to facilitate financial transactions, accessible by a small number of individuals. But within modern organizations, financial transactions are now facilitated through 10-13 different technical systems and services, each with their own access controls and security models, and often involve geographically distributed individuals.

To accurately measure risk of activity, you need to know actual SOD violations, not hypothetical ones.

You need full oversight of financial, operational, and process controls



Four Recent Examples of Legacy ICFR Failure Leading to Procurement Fraud

Procurement fraud can arise in a variety of ways, including creation of phantom vendors, kickbacks, invoice falsification, and more. The following examples of recent fraud cases demonstrate how inadequate financial controls fail to prevent fraudulent transactions from occurring.

Example 1: Fraudulent Transfers

A financial manager at an Indiana trucking company stole over $380,000 in 2020 by creating approximately 400 unauthorized transfers.[6]

SoD Violation

- A single individual was permitted to authorize and issue checks.

How Did it Happen?

- The manager entered the company's payment system and authorized a series of check numbers to make them available for use by truck drivers.
- She obtained the authorization codes for the checks, made them payable to herself, and filled in the dollar amount or obtained a cash advance.
- To cover the scheme, she altered years of bank statements to hide the true balances.

Example 2: Fraudulent Invoices

A laboratory chemist embezzled $9.2 million dollars from Lubrizol Corporation over 19 years by submitting fraudulent invoices for laboratory services from two companies he owned.[7]

SoD Violation

- A single individual was permitted to submit and approve invoices.

How Did it Happen?

- The chemist created fraudulent invoices for services not rendered by the chemist's sub-contracting lab.
- The same individual entered charges into Lubrizol's accounting system.
- Money was electronically transferred to the sub-contracting firm's accounts.

Example 3: Fraudulent Checks

A finance manager at Target Financial was sentenced to prison for stealing over $700,000 in 2020 after being found guilty for writing hundreds of fraudulent checks for personal benefit.[8]

SoD Violation

- A single individual was allowed to issue checks and manipulate accounting records. She could approve reimbursement requests from employees, issue reimbursement checks, pay vendors, and report to the owner regarding the financial condition of the company.

How Did it Happen?

- The manager wrote hundreds of checks to a family member for records management services that were never provided.
- Additionally, she wrote herself checks for nonexistent expense reimbursement, totaling over $600,000.

Example 4: Fraudulent Purchases

A public library employee in Austin, Texas made $1.5 million in fraudulent purchases for personal gain.[9]

SoD Violation

- A single individual was responsible for making and approving purchases, cash receipts, billing, and other accounting transactions.

How Did it Happen?

- The employee purchased $1.5 million in printer toner using library funds.
- She attempted to sell toner cartridges online for personal gain.

ICFR Requirements to Prevent Procurement Fraud

Effective ICFR management requires more than single-application SOD and static, hypothetical risk analysis. To defend against procurement-related threats, modern organizations must adopt an ICFR management program that is resilient and agile enough to protect the highly distributed, multi-application, dynamic nature of today's procurement processes.

Successful fraud prevention requires an automated approach to ICFR that continuously evaluates procurement-related activity in real-time across all relevant systems and applications, quantifies risk across both operational and financial dimensions, and enforces SOD policies in a comprehensive manner across the entire enterprise.

From the time access is provisioned to when it's deprovisioned, every activity within and across every application must be controlled and monitored in real time. Cross-application SOD controls must proactively prevent procurement fraud by managing access at a granular, transaction level.

This approach allows you to identify actual user activity and quantify risk, automatically evaluating the financial and operational consequences of every transaction as it progresses through various systems and services.

To mitigate risk, security and compliance teams must have access to a unified console to monitor and administer controlled process activity, manage user access and privilege, and respond to potential policy breaches with automated remediation protocols. Anomalous behaviors that could indicate procurement fraud in progress should trigger alerts and give you the option to automatically terminate a risky transaction before it can execute.

When deployed successfully, this approach can help you secure your financial operations without impacting the productivity and agility of your team to do their jobs.

Protect Against Procurement Fraud with Access Orchestration and Continuous Controls

The **Pathlock Access Orchestration Platform** empowers you to manage SOD across every one of your applications, and enable preventive, detective, continuous controls to prevent insider financial fraud and data theft.

With over 140 out-of-the-box integrations, Pathlock securely communicates with all of your enterprise applications and cyber security technologies, and serves as the unified platform to ensure proactive ICFR management and comprehensive protection against insider threats.

Pathlock Access Orchestration and Continuous Controls Platform

- ✓ 100% activity/process analysis vs. sampling
- ✓ Automated vs. manual
- ✓ Continuous vs. point-in-time
- ✓ Proactive instead of reactive

Segregation of Duty Management

- Cross-application view of SODs and risks
- Real-time SOD risk analysis and quantification
- SOD simulated risk assessment and provisioning
- Inline, rule-based transaction enforcement

User Access Management

- Unified UAR dashboard and automated reporting
- Emergency access management and monitoring
- Risk-based user control prioritization
- Adaptive authentication
- Attribute-level, conditional, and location-based access provisioning
- Usage-based role and access recommendations
- Least privilege enforcement

Reporting and Intelligence

- Out-of-box regulatory policy mapping
- Transaction-level UEBA
- SIEM and helpdesk workflow integration

Learn more about Pathlock and see how access orchestration can help you reduce the risk of procurement fraud.

Innovative
SOLUTION

Comprehensive

Granular access controls cover 100% of transactions, all users, all applications.

Proven

No company has had ITGC-related weakness since working with Pathlock.

Strongest
ROI

Savings

Automated processes replace time-consuming manual work.

Seamless

Fits into your workflow and toolset to extend your investments.

Future
PROOF

Scale

Consistent controls adapt as business and compliance requirements change.

Agility

Modern UX, SaaS solution is easy to adopt and pain-free to manage.

About Pathlock

Pathlock protects digital enterprises from the inside out. Our access orchestration solution supports companies on their journey to Zero Trust by surfacing violations and taking action to prevent loss. Enterprises can manage all aspects of access governance in a single platform, including user provisioning and temporary elevation, ongoing User Access Reviews, control testing, transaction monitoring, and audit preparation.

References

1. https://www.foxbusiness.com/money/former-amazon-employee-arrested-for-allegedly-issuing-more-than-96000-in-refunds
2. https://www.pandasecurity.com/en/mediacenter/security/cost-insider-threat-report/
3. https://techjury.net/blog/insider-threat-statistics/
4. https://www.schgroup.com/resource/blog-post/procurement-fraud-and-high-risk-events/
5. https://www.workiva.com/sites/workiva/files/pdfs/thought-leadership/sox-state-of-market-report-2020.pdf
6. https://www.justice.gov/usao-ndin/pr/hammond-woman-ordered-pay-381759-restitution
7. https://www.justice.gov/usao-sdtx/pr/chemist-sent-prison-embezzling-millions
8. https://www.justice.gov/usao-sdca/pr/san-diego-finance-manager-sentenced-prison-stealing-over-725000-employe
9. https://www.wgowam.com/news/a-former-austin-library-employee-is-accused-of-stealing-1-3m-in-printer-toner/