AMTRAK: Insights on Fraud Risks as the Company Expands Its Mission

OIG-SP-2023-007 | May 15, 2023

AMTRAK
OFFICE of INSPECTOR GENERAL
NATIONAL RAILROAD PASSENGER CORPORATION


UNION STATION
TRAVEL by TRAIN
UNION STATION

The Amtrak Office of Inspector General remains committed to aggressively continuing our oversight mission, which includes actively investigating and prosecuting fraud cases, identifying opportunities to improve related internal controls, and proactively sharing our insights on fraud risks for company consideration.

Kevin H. Winters | *Inspector General*

FROM THE INSPECTOR GENERAL

One of the core requirements of each federal Office of Inspector General is to "prevent and detect fraud and abuse" in its respective agency's programs and operations. And as reflected in our semiannual reports to Congress, I am extremely proud of the impactful work conducted by our investigators and auditors—spanning years—on fraud-related matters affecting Amtrak (the company).

Given our staff's expertise and experience in these matters, we thought it would be helpful to share our perspective, for company consideration, as it continues its expansion into large-scale acquisitions and infrastructure programs. Accordingly, the purpose of this report is to help inform the company's efforts to combat the persistent threat of fraud by sharing insights we have developed through our work.[1]

Indeed, the fraud challenge facing the public and private sectors is not hypothetical—and the company shares that challenge. As you know, the Infrastructure Investment and Jobs Act (IIJA) provides $66 billion for passenger and freight rail improvements, the largest investment in rail in generations.[2] IIJA funding, in part, is intended to advance the company's long-term, large-scale infrastructure goals and will significantly expand its traditional passenger rail operations mission to now include a major capital delivery mission. In fiscal year 2023, the company anticipates that it will have at least $30 billion in active capital projects. The nation's investment in the company via IIJA not only provides the company with significant opportunities, but it also provides criminals with a lucrative target for fraud.

Industry research estimates that 10 percent of infrastructure investments could be lost to fraud,[3] and if history is any indicator, IIJA—like other large spending bills—will be targeted by criminals through a variety of unlawful fraudulent schemes. Pandemic relief fraud is a sobering example, where the Inspector General community estimates more than $76 billion in unemployment insurance benefits were likely stolen in 2021.[4] Risks related to protecting the capital expenditures associated with IIJA are also compounded by other persistent fraud risks facing the company such as health care fraud and cybercrime. For example, potential national (not company) losses from cybercrime surpassed $10 billion in 2022—a nearly 50 percent increase from 2021.[5]

To its credit, the company recently established an Integrated Risk and Compliance Program (IRCP), an enterprise-wide program to monitor fraud risks and establish new capabilities to proactively identify fraudulent activity, as well as other goals. As the company launches this program, the Amtrak Office of Inspector General (OIG) has already engaged with the IRCP, and we are optimistic that our insights will help make the company a harder target for financial crimes perpetrated through fraud.

Since 2017, our office has investigated 99 fraud-related cases impacting the company and helped recover $120 million in restitution, forfeitures, and other recoveries.[6] We have also issued 22 audit reports during this period identifying weak controls that would-be criminals could exploit (see Appendix A). Our analysis of this work revealed the following four high-risk fraud areas:

- Contracts and procurements
- Health care
- Employee wrongdoing
- Cybercrime

Throughout this report, we describe each fraud risk area, highlight cases to illustrate how the risks manifest (see Appendix B for the cases we cite), and share examples of how the company can mitigate them. We also provide additional information to help the company build its fraud risk management program, and otherwise increase the company's overall fraud awareness as it continues its unprecedented expansion in mission and federal funding.

SINCE 2017, OIG HAS INVESTIGATED 99 FRAUD-RELATED CASES IMPACTING THE COMPANY AND HELPED RECOVER $120 MILLION IN RESTITUTION, FORFEITURES, AND OTHER RECOVERIES.

Several foundational activities constitute the core elements of an effective fraud prevention program. As such, they warrant special attention because they are universally relevant—enterprise-wide—to each discrete fraud risk area later discussed in this report.

These core elements include:

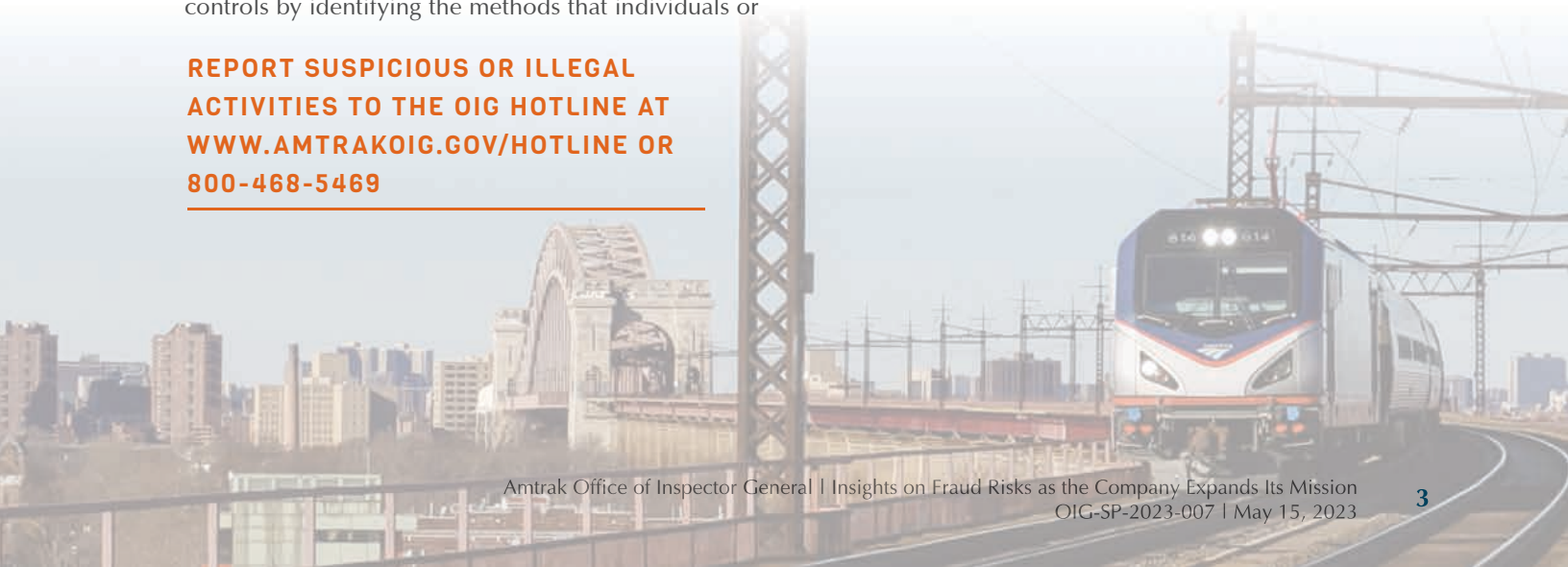
Building and maintaining a culture of integrity. An organization's culture plays a central and overarching role in preventing and detecting fraud. Executive leaders "setting the tone at the top" is the most important factor in establishing a culture of integrity. Management can set this tone and help build such a culture by proactively and frequently affirming ethical behavior as a top corporate priority—starting with personal example. Other top-driven actions include affirmatively requiring and encouraging the highest ethical conduct by all employees, vendors, and contractors; clearly communicating expectations for behavior; providing incentives to employees who uphold ethical standards; and transparently holding people accountable for fraudulent wrongdoing or ethical lapses.

Instituting effective fraud controls. Implementing adequate safeguards and processes to protect the company's assets is an essential step in fraud prevention.[7] Such safeguards and processes are not static and should continue to evolve with real or anticipated risks, with a view toward effective fraud prevention or detection. Preventative controls include access restrictions or approval authorities, and detection controls include financial reconciliations and post-payment reviews. Management can build robust fraud controls by identifying the methods that individuals or employees use, or could use, to commit and hide their crimes and designing barriers to stop them. Moreover, continually monitoring these controls and related data for suspicious patterns or trends can help the company detect fraud faster and reduce its losses. Further, as the company expands its workforce, ensuring new employees know their responsibilities for implementing controls will help them better protect the company's interests.

Fostering fraud awareness and reporting. Employee tips are the most common method by which organizations identify fraud.[8] Educating employees about the fraud risks they may encounter in their daily work could help the company detect ongoing or potential fraud schemes. In the past, for example, the company has worked collaboratively with our office and the Department of Justice to train company procurement staff on indicators of contracting fraud schemes. Fraud awareness training such as this could help employees recognize potential wrongdoing and educate them on what to do if they suspect it. In fact, we have received employee tips in the immediate aftermath of OIG fraud awareness training sessions. Again, to the company's credit, all employees, contractors, and representatives have a responsibility, under company policy, to report any suspected violations related to fraud, waste, or abuse to our office.[9]

The following four sections present our insights on discrete areas of fraud risk to help the company reduce the likelihood of fraud and inform its efforts as it continues to build and refine its internal control capabilities.

REPORT SUSPICIOUS OR ILLEGAL ACTIVITIES TO THE OIG HOTLINE AT WWW.AMTRAKOIG.GOV/HOTLINE OR 800-468-5469



FRAUD RISK: CONTRACTS AND PROCUREMENTS

Contract and procurement fraud involves unlawfully taking advantage of the funding mechanisms associated with acquisitions, programs, and projects. These fraud schemes could come in several forms and at different times in the procurement process, from the bidding and award of contracts through project and contract delivery (see Contract and Procurement Fraud Schemes on the next page). Criminals can also use more than one scheme at a time to harm victim organizations, ultimately inflating costs and diverting funds from their intended purposes.

In fiscal year 2022, the company spent $2.8 billion on its acquisition of goods and services, ranging from new rail cars to consulting services, and IIJA will likely triple this amount in the years ahead. Capital projects such as those IIJA will fund can be highly susceptible to contract and procurement fraud. Industry research has found that the scale, complexity, and large number of stakeholders involved on capital projects complicate the tracking of project expenditures and make it easy to hide inflated costs.[10] In addition to the company's infrastructure investments, the procurement of professional services can be vulnerable to conflicts of interest, as well as bidding and billing schemes.

Contract and Procurement Fraud at Amtrak

Since 2017, our office has opened 41 investigations related to contract and procurement fraud, and our recent investigations indicate that the company remains vulnerable to these types of schemes, as shown in the following examples:

- A former company contracting official steered more than $7.6 million in contracts to a manufacturer in exchange for cash bribes and other items.
- A contractor on the Gateway program—a series of projects to improve rail infrastructure in and around New York City—charged overhead rates

that exceeded contractually allowed rates and had to pay the company back $3 million.

- Two architectural, engineering, and construction management firms overbilled the company on separate projects over six years and had to pay back about $600,000.
- A construction company used a defunct Disadvantaged Business Enterprise as a financial pass-through to win a contract by creating the appearance of meeting supplier diversity requirements.
- A former company manager discussed bidding strategies with a vendor and provided exclusive access to company facilities prior to bidding, giving the vendor an unfair competitive advantage.

Mitigations

As the company prepares for an increase in acquisitions, programs, and projects, industry research and our prior audit work suggest a series of mitigation activities could help reduce its fraud risk.[11] Potential mitigation actions include the following:

Implementing approvals and segregations of duties. Having strong approval processes—with different people responsible for duties such as billing, payments, and disbursements to suppliers and subcontractors—helps mitigate risk. We previously reported on a situation where Amtrak used contractors to review invoices that their own company submitted—an inherent conflict that increased fraud risk.[12]

Practicing strong contract oversight. Strong oversight is crucial for major acquisitions and large-scale construction projects. For example, conducting regular and random inspections of job sites can help oversight personnel ensure that invoices align with the work performed or the materials and equipment supplied. And for major acquisitions, particularly those involving manufacturing and construction, contracting officers and their technical representatives play a key role in verifying that vendors uphold contract terms

CONTRACT AND PROCUREMENT FRAUD SCHEMES

Bid Suppression
Competitors agree to refrain from bidding or withdraw a submitted bid so that the designated competitor is likely to win.

Complementary Bids
Competitors collude to submit high bids or bids with terms unacceptable to the buyer to give the appearance of competition while favoring selection of one vendor.

Bid Rotation
A group of competitors predetermines the strongest bidder to take turns winning across multiple procurements.

Market Allocation
Competitors divide customers or geographic locations and either refrain from bidding or submit a complementary bid to reduce competition.

Subcontracting
Competitors agree not to bid or submit losing bids in exchange for subcontracts from the successful low bidder.

Price Fixing
Competitors collude to set prices for services, which restricts competition and results in inflated prices.

Bribery/Kickbacks
Competitors make payments to gain an advantage or avoid a disadvantage in a procurement or during contract execution.

Conflicts of Interest
Employees conduct business with related parties or those with whom they have a financial interest.

Billing/Payroll Schemes
Vendors knowingly charge unallowable costs; falsify labor, material, or equipment charges; or submit duplicate invoices for goods and services.

Substandard Materials/Work
Contractors boost profits by using substandard materials or work, or substituting products and services that do not meet contract specifications.

Disadvantaged/Minority Owned Business Enterprise (D/MBE) Fraud
Contractors use D/MBE as a pass-through or create bogus firms to create the appearance of meeting D/MBE participation requirements on projects.

throughout the life of a project. We previously reported that without strong oversight employees committed the company to paying vendors for work that was not in the contract, which also increased the risk that contractors could submit fraudulent invoices.[13]

Resourcing oversight roles. Fraud is most commonly uncovered by employees.[14] Our prior audits found, however, that the company was understaffing oversight roles in programs with $100 million or more in spending.[15] In 2021, the company established the Capital Delivery department to improve the oversight and management of its large projects and programs. To that end, staff assigned to such programs need to have (1) the necessary knowledge and skills to oversee them and (2) the capacity to exercise oversight without competing or detracting responsibilities. Knowing the fraud indicators (see right column) can also help those in such roles spot potential fraud. Such staffing can also help controls that depend on people to operate effectively, like invoice reviews.

Conducting due diligence on vendors. Establishing and maintaining processes to ensure that the company is conducting business with law-abiding vendors—and incentivizing them to remain so through aggressive internal controls—is another action that can mitigate fraud risks. Conducting checks on vendors and subcontractors and ensuring that the company does business only with responsible vendors can reduce the risk of harm to the company. Requiring all vendors, particularly those who are new, to attest in contracts to their commitment and compliance with applicable procurement and ethics-related laws, regulations, and company ethics policies could provide an additional safeguard.

Leveraging technology. Implementing effective electronic internal controls can help minimize opportunities for fraud. For example, we previously reported that the company's electronic procurement system allowed contractors to see the funds the company had set aside for cost increases.[16] Without controls to restrict their access, contractors could take advantage of this information.

CONTRACT AND PROCUREMENT FRAUD INDICATORS

Bidding

Unusual bid patterns.

Competitors refraining from or withdrawing bids.

Fewer bidders than normal.

Bids with terms unacceptable to the buyer to give the appearance of competition.

Identical errors or line-item amounts in bids.

Persistently high prices from all bidders.

Numerous sole-source contracts awarded to the same bidder.

Unusually close relationship between bidder and employee.

Contract Execution

Frequent, questionable, or undocumented change orders.

Change orders or invoices valued just below approval thresholds.

Employees shuttling between prime and subcontractor payrolls.

Prime contractors who always use the same subcontractors.

Irregularities in signatures, dates, or quantities on delivery documents.

Spotlight on Fraud: Bid Rigging

The president of a company that performs electrical work and three construction firms agreed to pay back $466,500 to the United States in connection with a scheme to rig bids and submit inflated invoices as part of work performed to improve the accessibility of Amtrak stations. A construction firm employee shared a bid for the electrical work on a Texas station with the electrical company president in exchange for cash. The firms also submitted false invoices for work at other Amtrak locations. Strong contract oversight helps mitigate the risk of this type of fraud.

FRAUD RISK: HEALTH CARE

Health care fraud involves medical providers and others seeking unlawful or unwarranted benefits or payments from a health care plan (see Health Care Fraud Schemes). In fiscal year 2022, the company spent about $340 million on medical, prescription, and dental claims for its workforce. Although it contracts with administrators who manage claims on its behalf, the company self-insures its medical and prescription plans; therefore, it bears a significant risk of improper payments. Consequently, health care fraud increases costs for the company and its employees.

Industry research estimates that three to ten percent of all health care expenditures are fraudulent,[17] the median loss for a health care fraud offense is about $1 million,[18] and the value of health care losses to fraud, waste, and abuse nationwide may total $100 billion annually.[19]

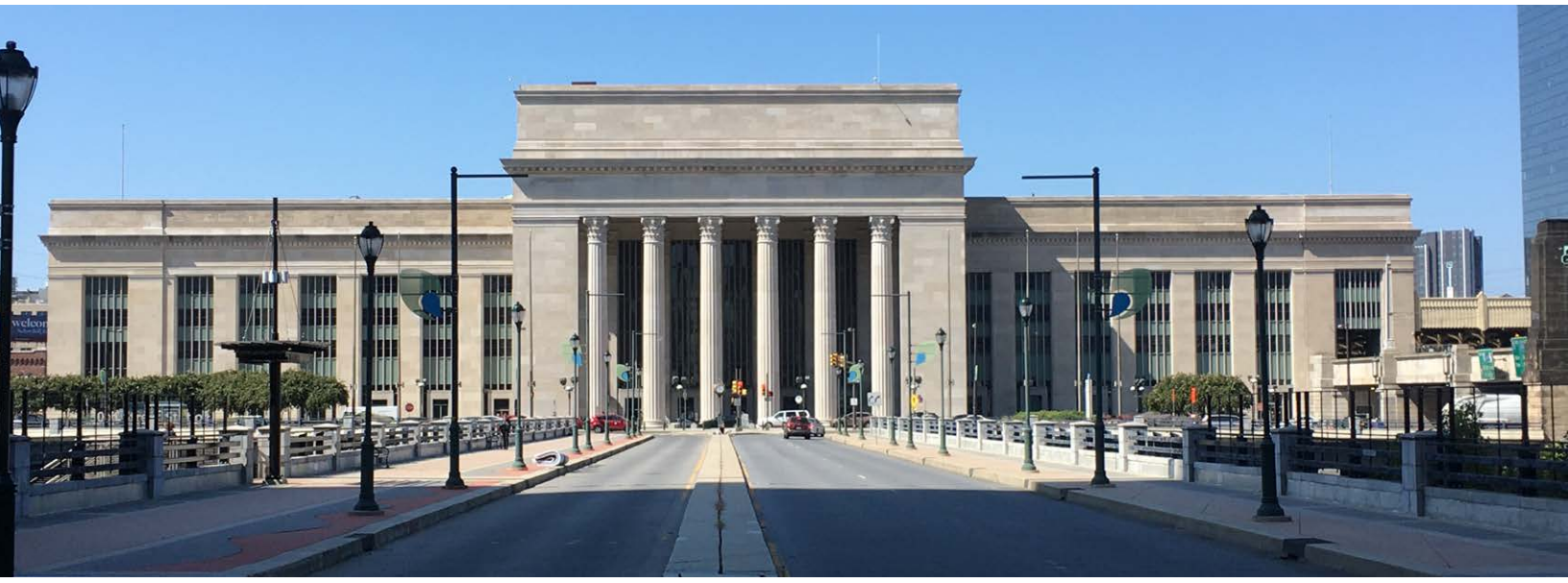
Health Care Fraud at Amtrak

Left unchecked, health care fraud can lower the quality of services provided to employees and their dependents. In 2019, we identified nearly $57 million in claims against the company's health care plan that were at risk for fraud. Our more recent investigations show that the company continues to be exposed to this risk, as shown in the following examples:

- A total of 27 defendants pleaded or were found guilty at trial to a kickback scheme involving billing insurance companies for drug and alcohol treatments the defendants did not provide. The company's plan paid about $2.5 million to these providers.
- A doctor fraudulently billed the company's health care plan more than $1.6 million for services that were not provided or were not medically necessary, and recruited employees to participate in the scheme by paying kickbacks, including opioid prescriptions.
- A doctor was sentenced to 20 years in prison for fraudulently billing expensive, duplicative, and medically unnecessary tests and treatments for patients seeking care for drug and alcohol addiction across multiple health plans. As part of this scheme, the provider improperly billed the company's health care plan nearly $2.2 million, of which the company paid the provider more than $535,000.

Mitigations

Through our prior audits of medical claim data and our reviews of industry research, we identified several



actions to detect and prevent health care fraud.[20] Taking the following actions will likely reduce the company's risk associated with these schemes and help it prevent such criminals from exploiting its health care plan:

Educating employees participating in company plans. We previously reported that employees serve as the first line of defense against health care fraud, and organizations commonly educate plan members to better recognize and report indicators of potential fraud (see Health Care Fraud Indicators).[21] Educating plan members to protect their personal information, review explanations of benefits, beware of free offers, and report suspicious activity can mitigate this risk. Plan members must also be aware of attempts by medical providers to recruit them—either wittingly or unwittingly—to participate in health care fraud schemes, as we have identified multiple times.

Reviewing emerging schemes. Gathering information on emerging schemes helps organizations better target fraud monitoring efforts. As we have reported, for example, regularly meeting with its plan administrators' investigative units and our investigators could help the company identify emerging risks.[22] Contracts could also require administrators to tailor their anti-fraud controls to the company's plans and dictate the frequency with which administrators must notify the company of potential fraud.

Monitoring claims for fraud. In addition to the administrator's fraud prevention efforts, proactively analyzing medical claims data for trends, patterns, and fraud indicators could help the company identify abnormal billing patterns early enough to stop fraudulent payments.[23] Such a capability could include monthly monitoring of paid claims to identify unusual spikes in provider billings.

HEALTH CARE FRAUD SCHEMES

Upcoding
Billing for more expensive services or procedures than were actually provided.

Medically Unnecessary Services
Delivering unnecessary services to generate insurance payments.

Services Not Rendered
Billing for visits, procedures, or supplies that the patient never received.

Unbundling
Billing separately for procedures when less expensive bundled billing is available.

Kickbacks
Paying patients to allow providers to bill falsely on their behalf.

Waiving Co-Pays or Deductibles
Waiving patient co-pays or deductibles for unnecessary services and, in turn, over-billing the benefit plan.

Medical Identity Theft
Using stolen identities to falsely bill for non-patients.

HEALTH CARE FRAUD INDICATORS

Provider's price far exceeds the average.

Provider has high number of patients from the same company.

Provider sees high number of patients from the same company and their dependents in one day.

Provider has high number of procedures administered per patient.

Provider has high number of claims.

Provider waives co-pays or deductibles.

Provider regularly resubmits denied claims.

Laboratory is under the same ownership as another facility making claims.

Provider has a high number of patients in common with other providers.

Provider's utilization of certain procedures far exceeds the average utilization of similar providers.

Provider has unusually high billing per patient.

Spotlight on Fraud: Misrepresenting Services

An acupuncturist recruited company employees and then fraudulently billed Amtrak's health care plan for services that were medically unnecessary or were not provided. The acupuncturist also regularly waived co-payments and deductibles, which the plan did not permit. The acupuncturist ultimately billed the company's plan more than $7.1 million—an amount comparable to large research hospitals and medical institutions. Of this, $3.8 million was deemed fraudulent. Proactively monitoring claims for fraud indicators would help mitigate the risk of similar fraud schemes.

FRAUD RISK: EMPLOYEE WRONGDOING

The company has more than 19,000 employees and plans to hire an additional 3,100 in fiscal year 2023. Such rapid expansion increases fraud risk because it may take time for new employees to develop enough institutional knowledge to identify potential fraud and, in some cases, demonstrate whether they fit into a culture of integrity. Employees who are tempted to engage in wrongdoing can defraud an organization through one or more schemes (see the non-exhaustive list of examples on the next page).

Results from an industry survey of more than 2,000 cases where an individual committed fraud against their employer showed that asset misappropriation—stealing or misusing a company's assets—was the most common fraud with a median loss of $100,000 per case.[24] This research also found that billing schemes—such as when employees create fictitious vendors and then fraudulently bill victim organizations—are the most common form of asset misappropriation. Typically, more than one employee is involved in committing fraud, and in many cases, they engage in multiple fraud schemes as part of their crime.[25] Employees who conspire with corrupt contractors or health care providers pose a particularly pernicious level of financial harm to an institution because of their ability to bypass or manipulate internal controls. These actions can—and do—damage an organization's reputation and put taxpayer dollars and revenue earnings at risk.

Employee Wrongdoing at Amtrak

Since 2017, our investigations have led to convictions, employee terminations, and resignations due to fraud. For example:

- A supervisor fraudulently claimed 686 hours of overtime, resulting in a loss of more than $71,000 to the company.
- Six employees resigned during an investigation that showed they misused their company badges or created counterfeit badges that they swiped for one another to claim fraudulent work hours.
- Since June 2017, a total of 13 employees either resigned or were terminated for engaging in outside employment while on leave under the Family Medical Leave Act (FMLA).
- Several ticket agents resigned after stealing cash from the company by waiting until a conductor electronically scanned a ticket then returning it for a refund.
- A foreman was terminated for misusing a company fuel card to make more than $7,400 in fuel purchases for his personal vehicle and those of his family members.

Mitigations

Industry research and our prior work suggest several areas to mitigate these forms of internal fraud/theft risks.[26] Without these mitigations, unethical employees are more likely to commit the types of fraud we have seen over the years, exposing the company to increased legal, safety, and financial risks. These actions include the following:

Maintaining rigorous hiring practices. Hiring individuals who align with company values and have personal integrity can mitigate fraud risks. For example, we previously reported that checking backgrounds before employees start employment can help reduce the risk of unknowingly hiring individuals with an extensive criminal past.[27] More broadly, confirming prior work history and references can help identify individuals who may pose fraud risks.

Establishing accountability. Organizations can ensure accountability for employee behavior by carrying out timely and consistent discipline and providing incentives for adhering to ethical standards. Targeted and timely communications that inform employees about ethical standards and publicize the consequences of unethical actions can also help dissuade employees from engaging in fraud.

Encouraging and incentivizing reporting. Given that tips from employees are the most common

method by which employee fraud schemes are detected,[28] organizations can encourage reporting of suspected fraud (see Employee Fraud Indicators) by communicating the protections they grant to whistleblowers and ensuring that those providing tips do not suffer retribution.[29]

Using advanced technology. Organizations use various technologies to reduce employee fraud risks. For example, in areas with valuable inventory, organizations may use remote monitoring or radio frequency identification tags on products and equipment to ensure that they are not lost to theft. Controlling access to the physical locations where the company stores such inventory can also help. To prevent or detect timekeeping fraud, organizations sometimes use video surveillance, advanced time-keeping systems, or biometric identification systems, such as those that include fingerprints or facial recognition.

EMPLOYEE FRAUD SCHEMES

Skimming
Removing cash before it is recorded in the accounting system.

Fictitious Voids and Refunds
Recording a sale, then voiding it and taking the cash from the register.

Falsifying Wages
Falsifying timesheets to receive payment for hours not worked.

Theft of Property
Taking property of an organization without permission.

Expense Reimbursement Schemes
Mischaracterizing or overstating expenses or requesting payment for fictitious expenses.

Credit Card Misuse
Using company credit cards to purchase personal items.

Inventory Misuse
Using company equipment or supplies for personal use.

Family and Medical Leave Act (FMLA) Fraud
Falsely claiming medical issues that prevent an employee from working.

EMPLOYEE FRAUD INDICATORS

Behaviors

Experiencing financial difficulties, to include legal problems.

Complaints about inadequate pay.

Living beyond apparent means.

Furtive behavior to hide fraudulent activity, such as defensiveness in response to questions.

Intimidation or bullying to silence potential whistleblowers.

Indicators

Accessing accounts or facilities outside normal work hours.

Access to cash transactions.

Overtime far in excess of others in comparable positions.

Frequent use of FMLA leave following or preceding a weekend or holiday, or after being denied vacation on similar days.

Employee on FMLA leave talks about outside employment.

Fuel purchases in excess of a tank's capacity.

Failure to submit proper documentation for purchases.

EMPLOYEES WHO CONSPIRE WITH CORRUPT CONTRACTORS OR HEALTH CARE PROVIDERS POSE A PARTICULARLY PERNICIOUS LEVEL OF FINANCIAL HARM TO AN INSTITUTION BECAUSE OF THEIR ABILITY TO BYPASS OR MANIPULATE INTERNAL CONTROLS.

Spotlight on Fraud: Employee Theft

A senior engineer in New Jersey stole 114 chainsaws and 344 chainsaw parts from Amtrak over an 8-year period. The former employee checked the items out of a company warehouse, then sold them on an online auction site at a total loss to the company of more than $76,000. He was sentenced to 18 months in prison, 3 years of supervised release, and full restitution.

FRAUD RISK: CYBERCRIME

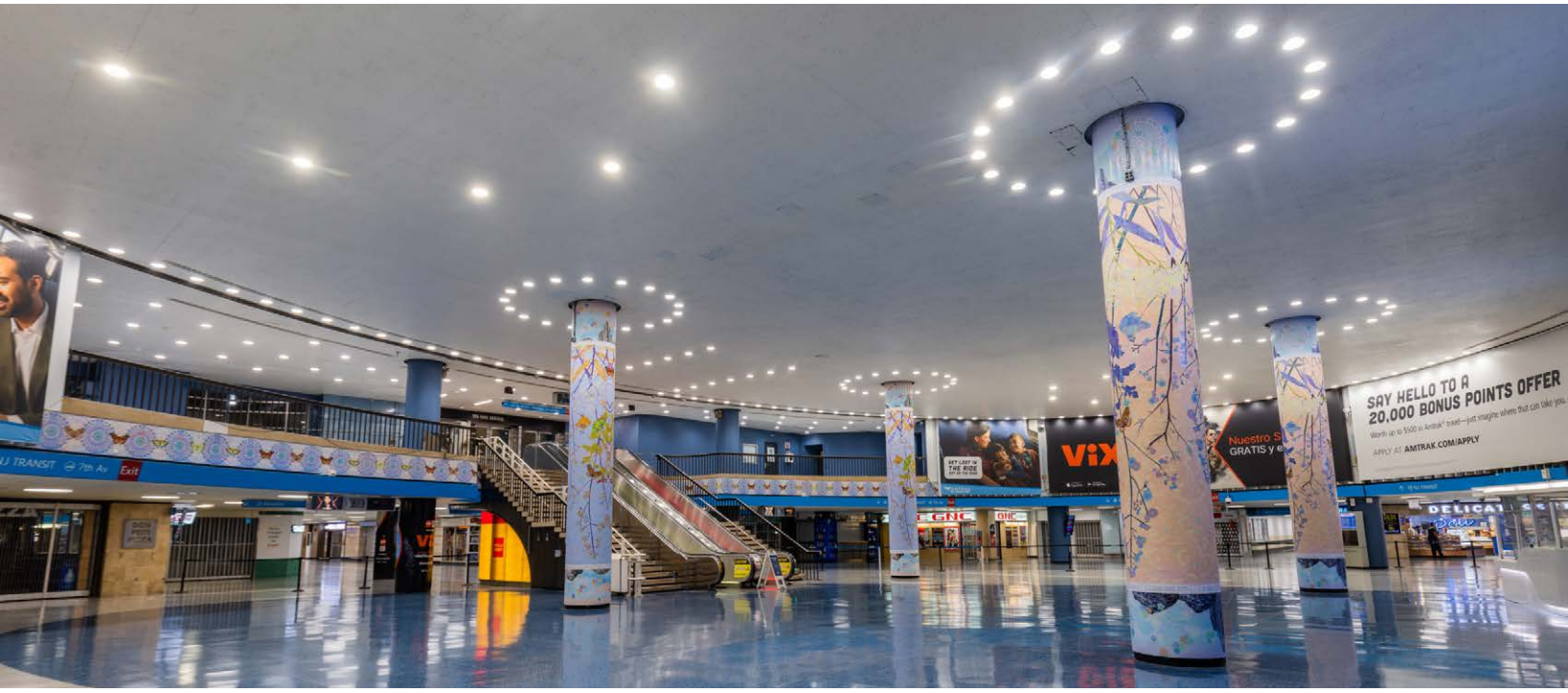
In fiscal year 2023, the company has more than 340 different information technology systems that process its business data or operational technology that control its trains. Criminals commit cybercrime when they use a computer or the internet to carry out one or more fraud or criminal schemes (see Cybercrime Fraud Schemes). This includes deceiving computer users or exploiting weaknesses in information systems to obtain sensitive information and cause harm.

An industry study of 550 organizations showed that 83 percent reported more than one incident when information was lost or stolen from a technology system. Such data breaches had an average cost of nearly $5 million to victim organizations[30] and typically interrupted operations for at least 18 hours, according to another study.[31] Although many cybercriminals seek financial gain through fraudulent system penetrations, some have national security or other motives. For example, the U.S. Department of Homeland Security reported that cybercrime related to international conflicts is increasingly targeting our nation's critical infrastructure operations, which could include disrupting rail operations.[32]

Cybercrime at Amtrak

Our audits and investigations show that the company—like all organizations—is at risk of the ever-evolving threats of cybercrime, as shown in the following examples:

- Using stolen usernames and passwords, cybercriminals gained unauthorized access to personal information in certain Amtrak Guest Rewards accounts, causing the company to incur the cost of offering free identity theft monitoring for affected customers.
- Multiple investigations uncovered individuals who used stolen credit card information to purchase Amtrak tickets valued collectively at more than $1 million. The individuals then returned the tickets to the company in exchange for electronic vouchers for future trips, which they then sold on the internet.



Mitigations

Protecting the company from such threats requires a layered approach with multiple levels of defense. To that end, the company adopted guidelines set forth by the National Institute of Standards and Technology,[33] which publishes leading industry standards for cybersecurity. Implementing a strong cybersecurity framework can help prevent, detect, and respond to cyber risks. We highlight several mitigations our industry research and prior work identified.[34] Absent the following actions, bad actors are more likely to attack company systems for their own gain or objective, exposing the company and its customers to financial and safety risks:

Raising cyber awareness. Industry research states that using compromised or stolen log-on credentials is a common way for cybercriminals to infiltrate an organization's systems.[35] Training employees on the fraud indicators (see Cybercrime Fraud Indicators), as the company does, and other actions to protect sensitive data can help reduce risks. In addition, continuing to provide employees guidance on how they should physically protect company technology assets may help mitigate the risk of data compromise.[36]

Deploying technology. Using available technologies to strengthen access controls, help monitor and flag unusual network activity, encrypt sensitive data, and detect and block potential intruders can help protect an organization from cybercrime.

Using strong processes to protect data. We reported that a weak exit process allowed a former company contractor to copy sensitive data to a personal storage device and remove it from company premises.[37] Continually assessing such vulnerabilities and deploying safeguards against evolving threats would help mitigate such risks.

Being prepared. Developing robust and well-communicated plans for prevention and response to cybercrime incidents and forming incident response teams can mitigate the cost of a data breach and allow for a quicker response.

CYBERCRIME FRAUD SCHEMES

Identity Theft
Stealing personally identifiable information for financial gain.

Credit Card Fraud
Use of counterfeit cards or unauthorized use of legitimate cards, stolen cards, or skimmed cards.

Spoofing and Phishing
Disguising an email address or other data to trick users into giving information.

Ransomware
Installing malicious software that prevents access to files, systems, or networks and demanding a ransom to restore access.

Network Intrusions
Unauthorized access to computers or networks.

Email Compromise
Infiltrating legitimate business email accounts to conduct unauthorized wire transfers.

Access Device Fraud
Eliciting transfers of funds involving credit and debit cards or other types of account access devices.

Point of Sale System Compromise
Unauthorized access to checkout or cashier systems that process electronic transfer of payments for services.

CYBERCRIME FRAUD INDICATORS

For Employees

Unrecognized emails or messages requesting urgent action or confirmation of sensitive information.

Emails or messages that appear to be from other company employees seeking atypical urgent action.

Difficulty accessing or editing computer files or, in the worst case, inability to log in.

Questionable pop-ups or messages that appear unrelated to user activity.

For Organizations

Unexpected or unusual activity in network traffic.

Reported breach or incident of a vendor or other third party.

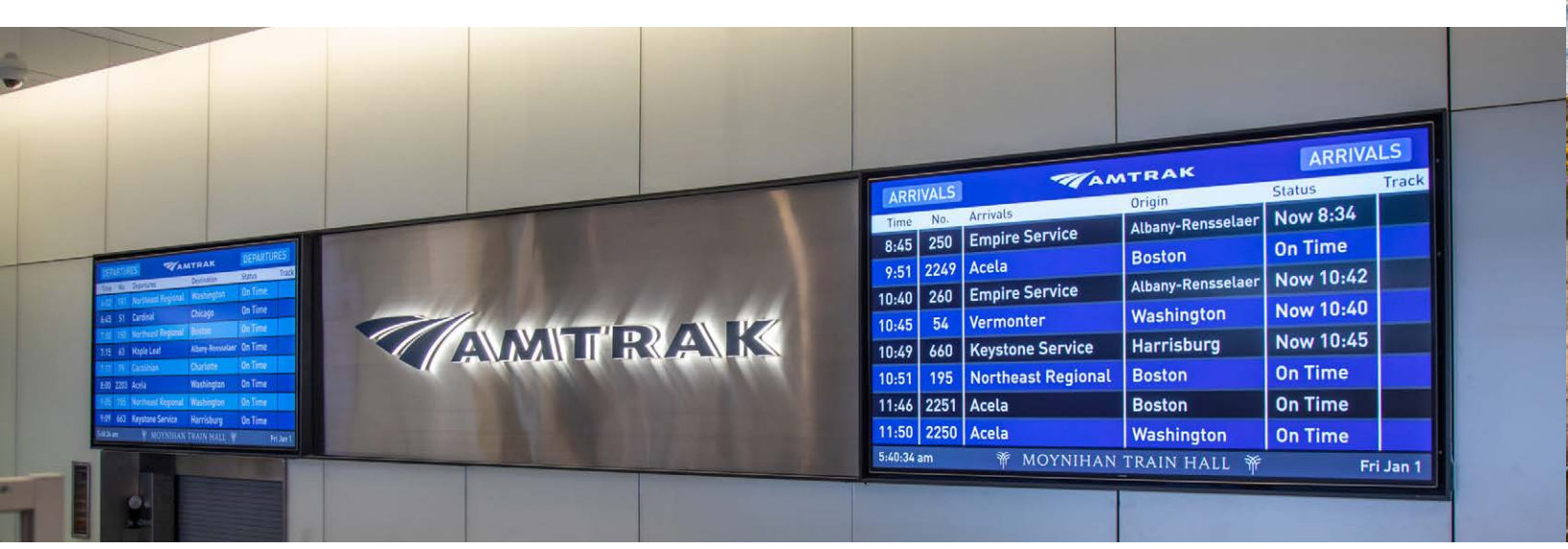
Unpatched systems or unsupported computer software.

Outdated antivirus or antimalware software.

Weak user authentication controls.

Unusually high activity from one customer account.

Atypical customer complaints regarding purchased tickets.



Spotlight on Fraud: Credit Card Fraud

An individual illegally obtained information from more than 1,100 credit card holders and used it to purchase Amtrak tickets online. The individual then cancelled the tickets, received electronic vouchers for the travel, and sold the vouchers online at a fraction of their face value. These actions caused Amtrak to lose more than $540,000.

Conclusion

While this is an exciting time for the company, the sheer size and nature of its expansion will unquestionably increase its fraud risk. This report has highlighted four specific areas of fraud risk facing the company, but we also acknowledge that fraud risks are fluid in nature, as criminals continually adjust and persist in targeting any perceived vulnerability in the company's programs and operations.

Industry experts and our work have also shown that an organization's insiders or external vendors—or a combination of both—pose an ongoing and ever-evolving fraud threat. To its credit, the company has an opportunity with its nascent Integrated Risk and Compliance Program to bolster—enterprise-wide—its fraud defenses, culture of integrity, and employee awareness of fraud schemes and indicators. As the company enhances its anti-fraud posture, the OIG remains committed to aggressively continuing our oversight mission, which includes actively investigating and prosecuting fraud cases, identifying opportunities to improve related internal controls, and proactively sharing our insights on fraud risks for company consideration.


6
8
10
Shipt

End Notes

1. This report contains findings from prior audits and investigations and provides our perspectives on the types of fraud risks facing the company. It is not an audit performed under Generally Accepted Government Auditing Standards. We provided management with a draft of this report prior to issuance.
2. *Infrastructure Investment and Jobs Act*, Pub. L. No. 117-58, 135 Stat. 429 (2021).
3. De Jong, M., et.al., *Eliminating Corruption in Our Engineering/Construction Industry*, Leadership and Management in Engineering, Volume 9(3), 105-111, 2009; Stateline, https://stateline.org/2022/02/03/fraudsters-set-to-pounce-on-massive-infrastructure-money/, accessed on May 2, 2023; CoST-the Infrastructure Transparency Initiative, https://infrastructuretransparency.org/about-us/our-mission-and-vision/why-cost/, accessed on May 2, 2023.
4. *Waste, Fraud, and Abuse Go Viral: Inspectors General on Curing the Disease*, U.S. House of Representatives Committee on Oversight and Accountability Subcommittee on Government Operations and the Federal Workforce (2023) (testimony of Larry D. Turner), https://www.oig.dol.gov/public/testimony/03092023.pdf.
5. Federal Bureau of Investigation, *Internet Crime Report*, 2022.
6. This figure was derived from OIG Semiannual Reports to the United States Congress from April 2017 through September 2022, and includes restitution amounts to other parties such as health care providers after investigations we conducted in coordination with other federal law enforcement agencies.
7. Government Accountability Office, *A Framework for Managing Fraud Risks in Federal Programs*, GAO-15-593SP, July 2015; Association of Certified Fraud Examiners, Inc, *Managing the Business Risk of Fraud: A Practical Guide*.
8. Association of Certified Fraud Examiners, Inc, *Occupational Fraud 2022: A Report to the Nations*, 2022.
9. Amtrak Policy P/I 2.1.4, *Office of Inspector General*.
10. Transparency International, *Programmatic Approaches to Address Corruption in the Construction Sector*, August 2010.
11. *Acquisition and Procurement: Company's Electronic Procurement System Limits Effective Contract Oversight* (OIG-MAR-2022-013), August 16, 2022; *Governance: Company Needs a Comprehensive Framework to Successfully Manage its Commitments to the Gateway Program* (OIG-A-2022-006), February 4, 2022; *Governance: Better Planning and Coordination Could Help the Company Achieve its Aggressive Timeline for ADA Compliance* (OIG-A-2021-012), September 2, 2021; *Governance: Early Planning and Oversight Deficiencies Led to Initial Program Failures and Continued Risks to the Moynihan Train Hall Program* (OIG-A-2020-014), August 17, 2020; *Acquisition and Procurement: Weaknesses in Contract Oversight Pose Financial, Operational, and Legal Risks* (OIG-A-2019-004), March 4, 2019.
12. OIG-A-2021-012.
13. OIG-A-2019-004.
14. Association of Certified Fraud Examiners, Inc, *Occupational Fraud 2022: A Report to the Nations*, 2022.
15. OIG-A-2022-006, OIG-A-2021-012, OIG-A-2020-014.
16. OIG-MAR-2022-013.
17. National Health Care Anti-Fraud Association, https://www.nhcaa.org/tools-insights/about-health-care-fraud/the-challenge-of-health-care-fraud/, accessed on February 23, 2023.
18. United States Sentencing Commission, *Quick Facts: Health Care Fraud Offenses*, 2021.
19. United States Department of Justice, https://www.justice.gov/archives/jm/criminal-resource-manual-976-health-care-fraud-generally, accessed March 29, 2023.
20. *Governance: Stronger Controls Would Help Identify Fraudulent Medical Claims Sooner and Limit Losses* (OIG-A-2020-003), December 10, 2019; *Governance: Opportunities to Improve Controls over Medical Claim Payments* (OIG-A-2018-005), March 14, 2018.
21. OIG-A-2020-003.
22. OIG-A-2020-003.
23. OIG-A-2020-003, OIG-A-2018-005.
24. Association of Certified Fraud Examiners, Inc, *Occupational Fraud 2022: A Report to the Nations*, 2022.
25. Association of Certified Fraud Examiners, Inc, *Occupational Fraud 2022: A Report to the Nations*, 2022.

26. *Background Checks Process Has Improved, but Some Inefficiencies and Gaps Persist* (OIG-A-2019-001), November 1, 2018.
27. OIG-A-2019-001.
28. Association of Certified Fraud Examiners, Inc, *Occupational Fraud 2022: A Report to the Nations*, 2022.
29. Association of Certified Fraud Examiners, Inc, *Managing the Business Risk of Fraud: A Practical Guide*.
30. IBM Corporation, *Cost of a Data Breach Report 2022*, 2022.
31. McAfee, *The Hidden Costs of Cybercrime*, December 2020.
32. Department of Homeland Security, *Secure Cyberspace and Critical Infrastructure*, https://www.dhs.gov.
33. National Institute of Standards and Technology, *Cybersecurity Framework*, https://www.nist.gov.
34. *Information Technology: Better Identifying and Tracking Operational Technology Assets Across the Company Would Improve Cybersecurity* (OIG-A-2023-002), November 7, 2022; *Former Contractor Violated Policy by Wrongfully Uploading Sensitive and Proprietary Company Data*, (OIG-WS-2020-328), May 28, 2020; *Information Technology: Mobile Device Security Needs to Improve to Better Protect Company Data from Compromise* (OIG-A-2020-010), May 8, 2020; *Information Technology: Improving Cybersecurity and Resiliency of Train Control Systems Could Reduce Vulnerabilities* (OIG-A-2019-008), July 19, 2019.
35. IBM Corporation, *Cost of a Data Breach Report 2022*, 2022.
36. OIG-A-2020-010.
37. OIG-WS-2020-328.

Appendix A - Audit Reports Identifying Weak Fraud-Related Controls June 2017 - September 2022

- *Information Technology: Better Identifying and Tracking Operational Technology Assets Across the Company Would Improve Cybersecurity* (OIG-A-2023-002), November 7, 2022
- *Acquisition and Procurement: Company's Electronic Procurement System Limits Effective Contract Oversight* (OIG-MAR-2022-013), August 16, 2022
- *Financial Management: Improving Payment Request Controls Could Provide a Better Value for Purchases and Protect the Company's Interests* (OIG-A-2022-010), June 15, 2022
- *Governance: Company Needs a Comprehensive Framework to Successfully Manage its Commitments to the Gateway Program* (OIG-A-2022-006), February 4, 2022
- *Governance: Better Planning and Coordination Could Help the Company Achieve its Aggressive Timeline for ADA Compliance* (OIG-A-2021-012), September 2, 2021
- *Governance: Early Planning and Oversight Deficiencies Led to Initial Program Failures and Continued Risks to the Moynihan Train Hall Program* (OIG-A-2020-014), August 17, 2020
- *Information Technology: Mobile Device Security Needs to Improve to Better Protect Company Data from Compromise* (OIG-A-2020-010), May 8, 2020
- *Asset Management: More Effective Management of Vehicle Fleet Would Improve Safety and Reduce Costs* (OIG-A-2020-007), March 17, 2020
- *Safety and Security: Addressing Security Weaknesses and Operational Impacts of Amtrak Express is Critical to the Program's Future* (OIG-A-2020-005), January 22, 2020
- *Governance: Stronger Controls Would Help Identify Fraudulent Medical Claims Sooner and Limit Losses* (OIG-A-2020-003), December 10, 2019
- *Governance: Improving Controls Over the Use of Procurement Cards Could Better Ensure Compliance and Limit Potential Misuse* (OIG-A-2019-013), September 30, 2019
- *Asset Management: Improved Inventory Practices Could Help the Company Better Manage its Maintenance-of-Way and Rolling Stock Equipment* (OIG-A-2019-010), July 25, 2019
- *Safety and Security: Physical Security Vulnerabilities at Washington Union Station and Ivy City Yard* (OIG-A-2019-009), July 22, 2019
- *Information Technology: Improving Cybersecurity and Resiliency of Train Control Systems Could Reduce Vulnerabilities* (OIG-A-2019-008), July 19, 2019
- *Acquisition and Procurement: Weaknesses in Contract Oversight Pose Financial, Operational, and Legal Risks* (OIG-A-2019-004), March 4, 2019
- *Train Operations: Opportunities Exist to Improve Private Railcar Management and Business Practices* (OIG-A-2019-003), February 6, 2019
- *Human Resources: Background Checks Process Has Improved, but Some Inefficiencies and Gaps Persist* (OIG-A-2019-001), November 1, 2018
- *Safety and Security: Longstanding Physical Security Vulnerabilities in Philadelphia Pose Risks* (OIG-A-2018-007), April 24, 2018
- *Governance: Opportunities to Improve Controls over Medical Claim Payments* (OIG-A-2018-005), March 14, 2018
- *Acquisition and Procurement: Contracts Included Key Provisions to Reduce Risks, but the Company Lacks an Efficient and Effective Contract Management System* (OIG-A-2018-003), February 22, 2018

- *Governance: Better Adherence to Leading Practices for Ethics Programs Could Reduce Company Risks* (OIG-A-2017-012), June 26, 2017
- *Governance: Opportunities Exist to Strengthen Controls to Ensure that Utility Accounts Are Deactivated After Real Estate Transactions* (OIG-A-2017-010), June 15, 2017

Appendix B - Fraud-Related Investigation Case List April 2017 - December 2022

Contracts and Procurements

- *Contractor Pays Over $3 million to Resolve Contract Billing Issues* (OIG-WS-2023-307), December 19, 2022
- *Manager Terminated for Discussing Bid Strategies with Vendor* (OIG-WS-2022-319), March 30, 2022
- *Alpha Painting & Construction Company Sentenced in Multi-Million Dollar Fraud Scheme* (OIG-WS-2020-306), November 14, 2019
- *President of Michigan Electric Company and Three Construction Firms Agree to Pay $466,500 to Settle False Claims Act Allegations*, April 22, 2019
- U.S. Department of Justice, *U.S. Attorney's Office Reaches $260,000 Civil Settlement with HNTB, Inc.*, March 1, 2019
- *Vendor's Employees Plead Guilty in $7.6 M Contract Steering Scheme* (OIG-WS-2019-312), February 5, 2019
- U.S. Department of Justice, *U.S. Attorney Reaches Settlement for False Claims Act Violations on Project Management Oversight Contract*, October 11, 2017

Health Care

- *Florida Doctor Sentenced to 20 Years in Prison for Substance Abuse Treatment Fraud Scheme*, January 13, 2023
- *New York Doctor Pleads Guilty to Defrauding Amtrak's Health Care Plan, Drug Distribution, and Unlawful Possession of a Firearm*, July 7, 2022
- *Acupuncturist Pleads Guilty to Charges in Scheme that Caused Millions of Dollars in Losses to Amtrak's Health Care Plan*, October 11, 2019
- *Owner Sentenced to More than 27 Years in Prison for MultiMillion Dollar Health Care Fraud and Money Laundering Scheme Involving Sober Homes and Alcohol and Drug Addiction Treatment Centers*, May 17, 2017

Employee Wrongdoing

- *Former Amtrak Employee Sentenced to Prison for Fraudulently Obtaining, Selling $76,000 Worth of Chainsaws and Chainsaw Parts*, April 26, 2022
- *Six Employees Resign After Participation in a Time and Attendance Fraud Scheme* (OIG-WS-2022-317), March 15, 2022
- *General Foreman Terminated for Misuse of GSA Fuel Card* (OIG-WS-2021-341), June 18, 2021
- *Former Employee Pleads Guilty for Stealing Ticket Funds* (OIG-I-2019-307), February 25, 2019
- *Time and Attendance Fraud* (OIG-WS-2017-306), June 8, 2017
- *Employee Resigns Prior to Administrative Hearing* (OIG-WS-2023-308), December 20, 2022
- *Foreman Terminated for Abuse of Medical Leave* (OIG-WS-2023-306), November 9, 2022
- *Employee Terminated for Engaging in Self Employment While on Medical Leave of Absence* (OIG-WS-2022-338), August 18, 2022
- *Employee Resigns Prior to Administrative Hearing* (OIG-WS-2022-327), July 18, 2022

- *Employee Terminated for Engaging in Outside Employment While on Leave Approved Under the Family Medical Leave Act* (OIG-WS-2022-324), May 3, 2022
- *Employee Terminated for Engaging in Outside Employment While on a Medical Leave of Absence* (OIG-WS-2021-350), September 2, 2021
- *Two Employees Resign from Company for Engaging in Outside Employment While on FMLA Leave* (OIG-WS-2021-320), January 21, 2021
- *Employee Terminated for Engaging in Outside Employment While on a Medical Leave of Absence* (OIG-WS-2021-315), December 2, 2020
- *Employee Terminated for Engaging in Outside Employment While on Sick Leave and Leave for Union Business* (OIG-WS-2020-345), September 15, 2020
- *Employee Resigns After Engaging in Outside Employment While on FMLA Leave* (OIG-WS-2020-322), April 14, 2020
- *Employee Terminated for Inappropriate Use of Leave* (OIG-WS-2020-318), March 16, 2020
- *Employee Resigns After Admission of Engaging in Outside Employment While on FMLA Leave* (OIG-WS-2019-318), July 5, 2019

Cybercrime

- *Michigan Man Sentenced for Wire Fraud and Making False Statements* (OIG-WS-2022-332), August 3, 2022
- *California Man Sentenced for Theft of Amtrak eVouchers* (OIG-WS-2022-321), April 25, 2022
- *New York Resident Pleads Guilty in Amtrak eVoucher Scam* (OIG-WS-2021-358), August 30, 2021
- *Pennsylvania Man Pleads Guilty in Amtrak Ticket Fraud Scheme* (OIG-WS-2021-323), January 12, 2021
- *Former Contractor Violated Policy by Wrongfully Uploading Sensitive and Proprietary Company Data* (OIG-WS-2020-328), May 28, 2020
- *New York Resident Pleads Guilty in Amtrak eVoucher Scam* (OIG-WS-2020-314), February 20, 2020
- *Scheme to Defraud Amtrak Results in Guilty Plea* (OIG-WS-2020-312), December 20, 2019
- *New York Resident Pleads Guilty in Amtrak eVoucher Scam* (OIG-WS-2020-304), October 24, 2019
- *New York Resident Pleads Guilty in Amtrak eVoucher Scam* (OIG-WS-2020-301), October 10, 2019
- *Scheme to Defraud Amtrak Results in Guilty Plea and Forfeiture* (OIG-WS-2019-324), August 14, 2019

Appendix C - General References

- United States Department of Justice, *Price Fixing, Bid Rigging, and Market Allocation Schemes: What They are and What to Look for*, 2005, revised 2021.
- United States Department of Justice, https://www.justice.gov/atr/red-flags-collusion, accessed on February 14, 2023.
- United States Department of Justice, *An Antitrust Primer for Federal Law Enforcement Personnel*, 2022.
- Government Accountability Office, *A Framework for Managing Fraud Risks in Federal Programs*, GAO-15-593SP, July 2015.
- United States General Services Administration, *Procurement Fraud Handbook*, 2012.
- United States Housing and Urban Development, Office of Inspector General, *Fraud Risk Inventory for the CDBG and ESG CARES Act Funds* (2022-FO-0801), October 12, 2021.
- United States Department of Defense Office of Inspector General, *Fraud Detection Resources for Auditors*, https://www.dodig.mil/resources/fraud-detection-resources/fraud-red-flags/, accessed on November 17, 2022.
- United States Department of Transportation Office of Inspector General, *Common Fraud Schemes*, https://www.oig.dot.gov/investigations/common-fraud-schemes, accessed October 18, 2022.
- National Healthcare Anti-Fraud Association, *The Challenge of Healthcare Fraud*, https://www.nhcaa.org/tools-insights/about-health-care-fraud/the-challenge-of-health-care-fraud/, accessed February 23, 2023.
- United States Department of Justice Federal Bureau of Investigations, *Health Care Fraud*, https://www.fbi.gov/investigate/white-collar-crime/health-care-fraud, accessed March 29, 2023.
- Association of Certified Fraud Examiners, Inc, *Occupational Fraud 2022: A Report to the Nations*, 2022.
- Association of Certified Fraud Examiners, Inc, *Managing the Business Risk of Fraud: A Practical Guide*.

MISSION

The Amtrak OIG's mission is to provide independent, objective oversight of Amtrak's programs and operations through audits and investigations focused on recommending improvements to Amtrak's economy, efficiency, and effectiveness; preventing and detecting fraud, waste, and abuse; and providing Congress, Amtrak management and Amtrak's Board of Directors with timely information about problems and deficiencies relating to Amtrak's programs and operations.

OBTAINING COPIES OF REPORTS AND TESTIMONY

Available at our website **www.amtrakoig.gov**

REPORTING FRAUD, WASTE, AND ABUSE

Report suspicious or illegal activities to the OIG Hotline **www.amtrakoig.gov/hotline** or **800-468-5469**

CONTACT INFORMATION

Kevin H. Winters, *Inspector General*

Mail: Amtrak OIG | 10 G Street, NE, 3W-300 | Washington D.C. 20002

Phone: 202-906-4600

amtrakoig.gov

twitter.com/amtrakoig

National Railroad Passenger Corporation
Office of Inspector General
10 G Street, NE, Suite 3W-300, Washington D.C. 20002