ahia
Assoc. of Healthcare Internal Auditors

NEW PERSPECTIVES

on Healthcare Risk Management, Control and Governance

www.AHIA.org Journal of the Association of Healthcare Internal Auditors Vol. 41, Number 6, 2022

Internal Audit Benchmarks in Healthcare Organizations

Learn where you stand
page 8

Audit the Remote Worker's Toolbox

Test endpoint security
page 21

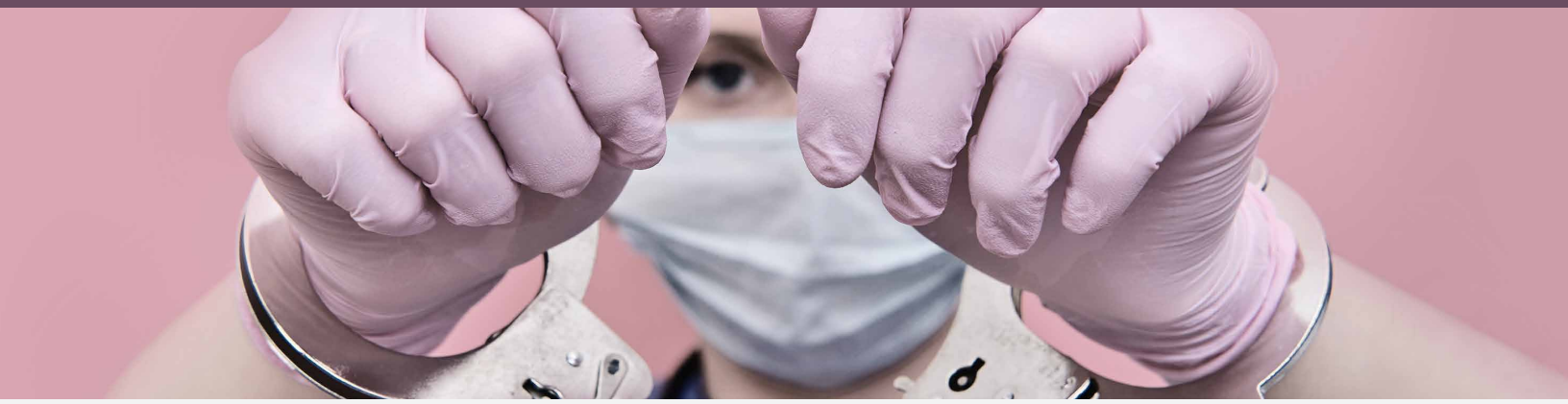
ESG in Healthcare

Focus on internal audit's vital role
page 33

Report Fraud to Law Enforcement

Know when, where and how

By Victor Hartman, JD, CPA, CFF, CFE



Is your organization susceptible to fraud? Would your organization report fraud to an appropriate regulator or law enforcement agency? How would you report the fraud? Become prepared to deal with fraud.

Think your organization is not vulnerable to fraud? Consider several plausible scenarios that you might encounter.

A healthcare imaging center is the victim of a ransomware attack. A dental office has been defrauded when its accounts payable clerk sent payments to a fictitious vendor as part of a business email compromise fraud. An employee of a nursing home has been stealing credit cards of residents. A bookkeeper of a medical practice has been embezzling funds through a check forgery scheme. An internal audit has discovered Medicare fraud when auditing a hospital's cost reporting procedures.

Fraud controls

How your organization handles an allegation of fraud is a function of two different types of internal controls—hard controls and soft controls. The hard (tangible) controls may be found in your organization's code of ethics, employee handbook, fraud policy or other standing procedures. A best practice is for a policy that states all employees have an affirmative duty to report fraud. Further, an escalation protocol will ensure that any allegation of fraud makes its way to a decisionmaker that is knowledgeable about handling fraud matters.

Although your organization has appropriate antifraud protocols, the red flags of fraud may still not be reported internally. An organization's soft (intangible) controls will determine whether an employee can identify suspicious conduct, feels comfortable reporting it, and knows how to get the information to the right official. Even when potential wrongdoing is identified, the employee may choose to report outside the organization and not internally. In short, the culture of an organization will have a big impact on the discovery and disclosure of fraud.

Data breaches and ransomware attacks

Healthcare providers are suspectable to a wide variety of frauds. Providers are more vulnerable to data breaches and ransomware attacks because they are data-rich organizations that possess personally identifiable

Have a policy that requires all employees to have an affirmative duty to report fraud.

Law enforcement may be more apt to work with a victim they already know through prior contacts.

information. Ransomware attacks create complicated issues for healthcare organizations. For example, some healthcare providers may feel compelled to pay a ransom because of the potential harm to patient care.

A general rule of criminal law is that no affirmative duty exists to report criminal conduct. However, important exceptions can apply, especially in the healthcare industry. If a legal analysis has concluded that a data breach involves protected health information of a HIPAA-covered entity, a legal duty exists to notify Health and Human Services, the victims and potentially the media.

As if the healthcare regulatory requirement is not bad enough, the payment of a ransom to certain bad actors on the U.S. Department of Treasury's Office of Foreign Assets Control sanctions list can result in strict liability to the payer. For these and operational reasons, a victim of a ransomware attack should have strong incentives to timely contact federal law enforcement.

Business email compromise

The business email compromise is currently the most virulent fraud facing all organizations worldwide. The fraud involves a communication—usually via an email—to an employee responsible for paying vendors or making a large purchase such as real estate.

The bad actor convinces the employee to change the automated clearing house or wiring instruction account number of the recipient so the funds can be misapplied. A victim of this fraud usually has 24 to 72 hours to contact both the financial institution involved and law enforcement if any hope exists of recovering the funds. Here again, a strong incentive should exist to report fraud outside the organization.

Fraud against government healthcare programs

Healthcare providers receive a substantial portion of their revenue from federal healthcare programs. These federal programs closely scrutinize payments because they are vulnerable to fraud. Under certain circumstances, a Medicare rule requires that providers report and return an overpayment to the federal government within 60 days of identifying an overpayment. The failure to repay overpayments can result in substantial penalties, and in the case of willful concealment, a participant may be criminally liable.

The federal government aggressively pursues healthcare fraud using both civil and criminal enforcement actions. The qui tam provisions of the False Claims Act allow the government to recover treble damages plus more than $25,000 per claim from a healthcare provider.

An important feature of qui tam actions is that anyone who undercovers and reports a fraud, often referred to as a whistleblower, can personally receive up to 30 percent of the recoveries. The awards can be substantial, which incentivizes anyone knowledgeable about healthcare fraud to retain an attorney and report outside the organization under the qui tam provisions of the False Claims Act.

In antitrust enforcement, the U.S. Department of Justice has a leniency policy to encourage antitrust violators to be the first to report.

Occupational fraud

Healthcare organizations, like any business, can be victimized by their employees and other fraudulent actors. The most common schemes are abuse of purchase cards (credit cards), travel or expense reimbursement schemes, and embezzlements. Management may be eager to report the fraudster to law enforcement in part because reporting sets a strong tone that fraud will not be tolerated in the organization.

Also, a law enforcement report can assist in the defense of a wrongful discharge action brought by the former employee. Further, the courts can assist in recovery of losses through asset forfeiture and restitution orders.

Disincentives to report fraud

In contrast, factors exist that will discourage an organization from reporting fraud. A charitable organization that relies on donations as its chief source of revenue can be negatively impacted by the publicity of a fraud event that demonstrates the organization has not safeguarded charitable assets.

Other factors that discourage reporting are when the fraudster has a familial relationship with those in charge of governance, a potential whistleblower fears retaliation, or the bad actor is a prominent citizen outside the organization. Occasionally, legal counsel might opine that

referral of a fraud matter to law enforcement could slow or jeopardize an ongoing parallel civil litigation.

Ultimately, whether an organization learns of fraud through internal reporting or by an outside enforcement action will be a function of the strength of an organization's hard and soft controls. Further, the soft controls, such as a positive organizational culture, will likely have the greatest impact.

Where to report fraud

Once a decision has been made to report fraud, what should that look like? Your organization should realize that when filing a fraud complaint with a law enforcement agency, they are competing for resources. Fraud allegations are unfortunately not only common but resource intensive to investigate, and some agencies may not have the resources to timely address the allegation.

For large healthcare providers, the organization may have the resources to have attorneys, internal auditors and/or compliance officers work with regulators and local, state and federal law enforcement before a fraud allegation ever occurs. Established connections can assist with fraud prevention, detection and investigation. When fraud does occur, law enforcement may be more apt to work with a victim they already know. For smaller organizations, prior contacts with law enforcement may not be practical.

Get your complaint accepted

A fraud victim will want to make its complaint attractive to law enforcement. The first step is to present the complaint to the right agency. An organization must decide whether to present the complaint to a federal or local agency.

At the federal level the United States Attorney's office and the investigative agencies such as the Federal Bureau of Investigation, the Department of Health and Human Services' Office of Inspector General, the Drug Enforcement Administration, and the United States Secret Service are possibilities. The choices at the state level may include the attorney general's office, the local district attorney's office and local law enforcement.

Each law enforcement agency will have varying priorities and limited resources. Understanding these factors will guide your organization in the decision as to where the complaint should be filed.

Consider the priorities of the law enforcement agency involved. If possible, structure your complaint to fit their priority. Your fact pattern may involve an employee that made $50,000 in unauthorized credit card charges and sold forged doctor prescriptions for controlled substances like oxycodone.

The two distinct criminal violations will resonate differently depending on the law enforcement agency involved. From a law enforcement policy perspective, the drug addiction crisis is more important than a low-level fraud that was entirely preventable. Knowing these distinctions will enable you to focus on the relevant facts. Exhibit 1 provides a summary of factors for getting your complaint accepted.

Exhibit 1 – Criminal complaint acceptance factors

1. Present case to the correct agency
2. Meet with a decisionmaker
3. Focus complaint on the agency's priorities when possible
4. Identify suspect(s)
5. Provide prior investigative work
6. Provide written report, executive summary and comprehensive fact pattern
7. Identify and provide evidence
8. Submit a three-ring binder with tabs and an electronic copy of the report
9. Commit continued organizational resources from investigation through prosecution
10. Make witnesses readily available

How to report

The complaint should preferably be made in person. Take the time to figure out who in the agency is a decisionmaker and attempt to set up an appointment with that official. Prior to the meeting, organize the presentation. If resources are available, consult with an attorney or a former law enforcement officer who is knowledgeable of the laws that may have been violated. Pairing the facts of a case with the elements of a criminal statute demonstrates knowledge of the criminal process and will encourage law enforcement to take the case.

Make your complaint attractive by presenting to the right agency, pairing facts with criminal statutes and sharing your investigation results.

Reporting to law enforcement sets a strong tone that fraud will not be tolerated in your organization.

Bring several copies of the written complaint. If your organization has already conducted an internal investigation, let the law enforcement official know that much of the work has already been done. The fact will go a long way to getting the complaint investigated because your complaint will require fewer resources prior to bringing formal charges.

Conclusion

The decision to report fraud to a law enforcement agency should be made with legal counsel. In most instances, reporting is in the best interest of your organization. Before fraud can be reported, it must be discovered. Discovering fraud is directedly correlated to the strength of an organization's internal controls.

Once a decision to report has been made, the organization should reach out to the appropriate law enforcement agency and provide as much assistance as needed. Prosecuting fraud offenders sets the appropriate tone and is a deterrence from future acts of fraud. **NP**

Victor Hartman, JD, CPA, CFF, CFE, is Principal of The Hartman Firm, LLC, specializing in forensic accounting and internal investigations. He was an FBI Special Agent. He is now an Adjunct Professor at Georgia State University and serves on Georgia Southern University's Forensic Accounting Advisory Board. Vic can be reached at 404-369-0616 and Vic@HartmanFirm.com.