FOLLOW THE CLUES:
A NONPROFIT FINANCE SLEUTH UNCOVERS FRAUD

Click sections above to navigate

CHAPTER 1

THE SCENE

“I never thought it could happen to us.”

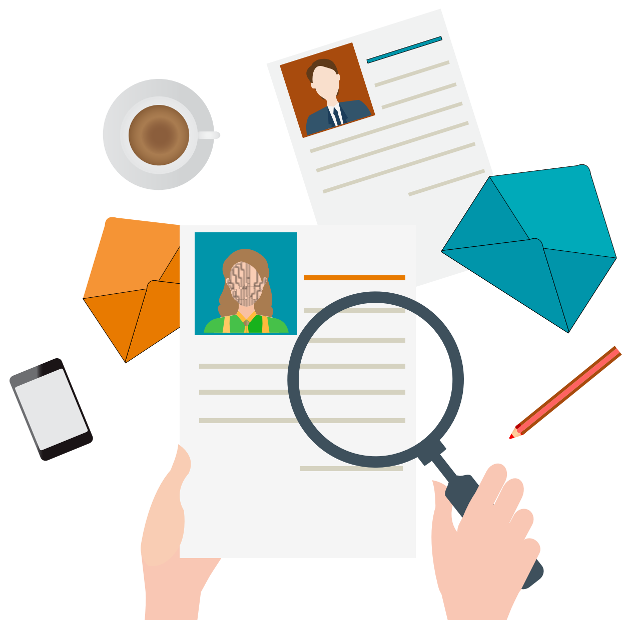
In the quiet seaside town of Charity Cove, the latest in a string of disturbing frauds at nonprofits had just come to light. Henry Gonzales, the finance director for Eastern Shore Legal Advocacy, sat at his desk, his face in his hands. Sitting across from him was Audie Money, famous in her field as the world’s greatest consulting detective for nonprofit fraud.

“How could Sheila have done this?” Henry asked.

Like the rest of the ESLA staff, the finance chief was shocked to find out how Sheila Jones, their longtime office manager, had used a check-tampering scheme to embezzle hundreds of thousands of dollars from the nonprofit. Over the course of years, Audie found, Sheila diverted checks intended for ESLA’s main account into a secret account she had opened in the organization’s name, using the money to pay her credit card bills, rent, and other personal expenses.

Audie knew the ESLA staff had lots of work ahead of them to determine the exact extent of Sheila’s fraud, and to deal with the public fallout connected to it. She also knew from experience how hard it might be to restore the faith of donors and volunteers, once word got out.

Unfortunately, the incident was a classic case of **fraud emerging from weak internal controls**. As office manager, Sheila had access to all the documents necessary to open bank accounts. She was able to hide bank statements, then issue false quarterly financial statements to the board of directors to hide her actions. ESLA’s simplest mistake with Sheila might have been the worst of all: as office manager, she had both check-writing and check-signing privileges – duties that should always be separated, so that one person doesn’t have so much opportunity to defraud the organization.



The Scene
The Shock
The Betrayal
The Response
The Confrontation
The Road to Recovery
The Anti Cheat Sheet
Click sections above to navigate

NONPROFIT FRAUD MYTHS UNCOVERED

MYTH 1

Fraud rarely happens

Debunked: In reality, fraud at nonprofits happens more often than you might think. Many nonprofits keep this quiet, so as not to create a stigma for the organization or deter potential donors.

MYTH 2

Only "bad" people commit fraud

Debunked: Unfortunately, the reality is good people can still do bad things, driven by necessity, greed, or opportunity.

MYTH 3

We only hire good people, so that won't happen to us

Debunked: No one intentionally hires someone who will commit fraud, and it may be hard to spot the signs of a perpetration until it's too late.

MYTH 4

Audits easily and always catch embezzlement and fraud

Debunked: Auditors do address fraud, typically by evaluating how well an organization's leadership assesses risks, what steps are taken to detect and prevent financial irregularities, and what documentation processes are in place that might help catch fraud. But, while audits can at times help identify fraud, they aren't specifically designed to do so.

Click sections above to navigate

CHAPTER 2

THE SHOCK OF FRAUD PERPETRATED BY OUTSIDERS

Similar stories were emerging across Charity Cove as Audie worked with other nonprofits stung by fraud. At Hometown Healthcare Organization, a member of the accounting team received an email from the organization's executive director requesting a financial transaction – specifically, a rather large expense reimbursement to her. Because it came from the top, the transaction was expedited, and the money was paid quickly. In reality, it didn't come from the ED at all. In fact, a hacker had gained access to the organization's email system – a classic example of IT fraud. The cyber crimes unit of the Charity Cove Police Department was handling that investigation now, though Audie would be returning to train the staff on what to watch for in the future.

Meanwhile, Town Square Humane Society was still trying to untangle the lies told by a smooth-talking fraudster. The receptionist at Town Square took a call from a very displeased vendor accusing the nonprofit of being delinquent in paying for electrical work completed at the society's new shelter. The receptionist answered a few questions, then directed the caller to the finance team. The "vendor" gleaned just enough information during those conversations to beef up an email requesting payment. After running it through their internal checks and balances – which, unfortunately, proved to be inadequate – the finance team paid the vendor. It wasn't until a few weeks later, when the actual electrician called to request payment, that TSHS realized it had fallen victim to a fictitious vendor scheme.

And, on the other side of town, the staff of the Northside Youth Club was reeling after its annual golf tournament had ended in tears. During the event, a volunteer working the registration booth sold lots of "mulligans" – a printed pass allowing a golfer to redo a shot – at $50 a pop! But, when all the cash was counted, the numbers weren't nearly as impressive as they should have been. The NYC had fallen victim to a common form of fraud called skimming, in which cash is pocketed before it's ever recorded on a receipt or in a ledger. Audie had questioned the staff to find out what had happened and make sure none of them was in on the scheme. No one seemed to remember that volunteer from previous events ... and, of course, he was never seen again.

Although **team members should be your first line of defense against fraud**, she found what she expected. Team members on the NYC's lean staff had been wearing too many hats during the event. With many competing responsibilities and constant interruptions, no one was specifically accountable for monitoring all the cash transactions. "I was so distracted," the volunteer coordinator had said. "There were people around all day, so I thought we were keeping an eye on that guy," the accounting manager added. Despite their personal integrity and passion for the organization's cause, the pros at the NYC were unaware of fraud being carried out right under their noses.

THE MOST COMMON NONPROFIT FRAUDS

1 Misappropriation of Assets

- **Cash**
  - Skimming (taking cash before it's reported)
  - Cash larceny
- **Check tampering**
  - Forged check stock, signatures, or endorsements
  - Altered payees or amounts
- **False expenses reimbursement**
- **Billing schemes, for example fake invoices, or paying a legitimate invoice twice then asking the vendor for a refund that is diverted to a fraudulent account**
- **Payroll schemes, for example falsifying wages**

2 Corruption

- **Bribery, kickbacks, and bid rigging**
- **Conflicts of interest, for example purchasing schemes**

3 Financial Statement Fraud

- **Overstatement or understatement of revenues, expenses, asset valuations, etc.**
- **Misclassification of restricted donations, grant expenses, etc.**

Click sections above to navigate
BACK
NEXT PAGE

CHAPTER 3

THE BETRAYAL OF INSIDER FRAUD

Back at Eastern Shore Legal Advocacy, finance director Henry was grieving. And Audie sat back and reflected that, as bad as those other cases had been, at least the fraud had been perpetrated by outsiders – strangers who treated the nonprofits as easy marks. Henry and his colleagues were going through something much harder to take: betrayal by a trusted colleague who had been with the organization for years. Audie wished she hadn't seen it so many times before.

"Sheila believed in our mission," Henry said. "She grew up in tough conditions herself, and she always said she identified with what our clients go through when they need legal help." He shook his head as he stared at the floor. "She just doesn't seem like the type of person who would do this."

"I hear you, Henry," Audie said. "Unfortunately, **fraud perpetrators don't fit any particular mold**, and anyone might be tempted into it."

"Should we have seen it coming?" Henry asked. "What are the warning signs?"

"There are a few different ones," Audie said. "You've probably seen cop shows on TV, so you know with any crime suspect they look for means, motive, and opportunity. With fraud, we talk about it a little differently, and call it **'the fraud triangle.'**"

1. The person perceives there's an opportunity to get away with fraud.
2. The person is experiencing some kind of pressure, like if he or she need lots of money to support a drug habit or gambling addiction.
3. The person rationalizes that committing fraud is justified.

"Sometimes, employees will commit fraud because they're angry with their boss or feel the organization has treated them unfairly, or just because they need the money and intend to pay it back later," continued Audie. "From what I can tell, in Sheila's case she had the opportunity to get away with it, because there wasn't a second set of eyes on some of the checks she generated and signed. And, she seemed to think her contributions to the organization were so valuable that taking money on top of her salary was justified."

BACK NEXT PAGE

Click sections above to navigate

"But, we kept giving her raises!" Henry protested.

"I know," Audie said. "But the truth is, nonprofit professionals are usually paid less than those in the for-profit sector, yet the expectations and responsibilities on them are still very high. If somebody in that situation develops the attitude that the rules don't apply to them – well, it's trouble waiting to happen."

Audie's phone buzzed in her pocket; it was set to alert her only when she got a text from the office, and her staff knew to contact her only in cases of emergency.

"Please excuse me one moment, Henry." He nodded as she unlocked her phone.

The text was blunt: **"THE RANDOLPH FOUNDATION NEEDS YOU A.S.A.P."**

Red Flags for Fraud

These are some telltale signs that a person connected to your nonprofit could be involved in fraud. According to a 2016 global study by the Association of Certified Fraud Examiners, 91 percent of fraud cases were marked by at least one of the following red flags, and 57 percent of cases had two or more red flags. What are these clues that an employee might be misappropriating your organization's assets?

- **Living beyond their means.** Employees who engage in behaviors their salary won't cover could be at risk. Addiction, a gambling habit, or indulging in expensive lifestyle habits (taking luxury vacations, driving fancy cars, and so on) may create financial pressures that tempt employees to steal. If those habits are sustained, that could reflect that the employee already has access to a secret, possibly fraudulent source of cash.
- **Unusually close associations with vendors or customers.** Pay attention to tales of weekend fun or trips with vendors or customers. Frequent dinners out with donors, vendors, or customers could create opportunities for fraud by employees.
- **A wheeler-dealer attitude involving shrewd or unscrupulous behavior.** People exhibiting this demeanor committed fraud in more than 15 percent of cases.
- **Control issues.** Employees who were unwilling to share their duties were equally likely to commit fraud, also in more than 15 percent of the case studies.

The Scene
The Shock
The Betrayal
The Response
The Confrontation
The Road to Recovery
The Anti Cheat Sheet
Click sections above to navigate

CHAPTER 4

CRISIS MODE: RESPONDING TO FRAUD WITHOUT LOSING YOUR COOL

Audie sat on the edge of her seat and picked up her shoulder bag. "It's my office - we've been contacted about another possible fraud. Are you okay for now, Henry?"

He sighed, nodded, and then responded, "I think so. I'm more concerned with the staff – they're all shell-shocked. What do we do next?"

"I'm going to lay out a plan for you," Audie said. "You're already doing the most important thing, which is to remain calm. And, you did the right thing by calling your legal counsel first, and then law enforcement once they advised you to. You've got the wheels in motion in the right direction, and we'll work together to make sure you build the internal controls you need, train your staff appropriately, and create an anti-fraud culture. That will help you prevent anyone from having the means, motive, and opportunity to commit fraud here in the future."

Henry thanked Audie and showed her out. As she sat in the backseat of a rideshare en route to the Randolph Foundation's headquarters across town, Audie called her assistant and began scribbling notes. By the time she was ushered into a conference room, she knew the basics: newly installed financial software had alerted an accounting clerk to irregularities, which she had reported to her boss – Ron Davies, the foundation's financial controller. By chance, executive director Margaret Henderson had been chatting in Davies' office at the time, so she heard the bad news in the same moment.

Now, Audie was sitting across the table from Henderson, Davies, their outside counsel, and Jonathan Randolph, current board chairman and son of the foundation's late benefactor. Henderson thanked her for coming in, then the lawyer and the controller added a few minor details about what they had done to keep a lid on the situation.

Then Randolph spoke up. "Ms. Money, help me understand why you have such a good reputation at this. Are you an auditor?"

She smiled. "With a name like Audie, you'd think so, right? But no, I'm a CPA, and I worked with outside auditors many times as I climbed the career ladder to CFO in the corporate world. I retired early, then served on nonprofit boards for a children's hospital and a veterans' assistance organization. That's what exposed me to the problem of nonprofit fraud and led me into this work. I seemed to have a knack for it from the start, and I've always kept up with the latest in terms of methods and technology to deal with it."

"But don't we have good methods, and good technology?" Randolph said. "I'm sure I don't know everything, but I've been a CEO for years, and I know how to read a financial statement. We don't know how much of a gap this is, but it looks bad. Why didn't we spot it before now?"

"In my experience," Audie said, "board members are most often highly dedicated to the organization's mission – but they don't have a specialized background in finance. You have a small organization, so there may not have been the right checks and balances in place. That's what I'll dig into first."

"All right," Randolph said. As Henderson nodded beside him, he added, "We'll give you whatever help you need."

First Steps After Discovering Possible Fraud

- Consult your legal counsel. Do not confront the individual who you believe committed the fraud until after you have done this.
- If instructed by legal counsel, inform law enforcement.
- Inform your insurance carrier.
- Preserve any documents or other evidence.
- Correct the system that allowed the fraud to occur.

Tips for Managing a Fraud Crisis

- Remain calm; do not overreact.
- If your organization has a whistleblower policy, follow it.
- If there is no whistleblower policy, engage only people who are your superiors, unless they're suspected of wrongdoing, in which case you should engage only those who supervise them.
- If you're in charge, engage your professionals to verify your suspicions of the fraud.
- If you work at a large organization, you may want to engage a public relations firm.

CHAPTER 5

CONFRONTING THE UNTHINKABLE

For the most part, the staff made good on Randolph's promise, though in the days that followed Audie noticed certain patterns of behavior that aroused her suspicions. Working alongside a forensic accountant from her team, she interviewed staff members, consulted with the foundation's outside counsel, and reviewed stacks of financial documentation. By the time she reconvened the same group around the conference table, she had a clear picture of what had happened.

"The good news is," she began, "you've built a culture of trust among the staff, and recruited people of high integrity ... with one crucial exception." Randolph, Henderson, and Davies all exchanged looks. "The bad news is, you've been too trusting, and that has kept you from implementing the internal controls that might have prevented this from happening."

"And, what exactly is 'this,' Ms. Money?" Randolph asked.

"Fraud on the order of $4 million." Audie sat with her hands folded, letting that sink in. Randolph looked ashen, while Henderson's jaw was clenched in anger.

Audie turned to the controller. "Ron, when's the last time you took a vacation?"

"Beg pardon?" the controller asked.

"A vacation. Or any time off. How long has it been?"

"Oh, uh, not for ages," he said. "Ask anybody here – I'm married to this job, 24/7/365."

"Right. And, when's the last time someone other than you did reconciliation on the foundation's bank statements?"

Davies looked puzzled. "I don't understand your question. That's part of my job."

"So much so, that no one else ever handles it, or has the opportunity to check your work."

"Well of course anyone could check on it. I, I mean, we keep good records –"

"Which you also control." Audie's tone was cold. Now Davies looked afraid as he stared back at her. Audie continued: "The fact is, you don't allow anyone else to see reconciliations as they happen."

"Sure I do –"

She silenced him by holding up her hand. "Another fact is, you resisted the implementation of the new financial software."

"I thought we didn't need it –"

"Another fact is, you spend every weekend on your boat."

"What does that have to do with –"

"Your very *nice* boat that you keep at your private dock next to your very nice, recently renovated home. Much too nice for a single man with no obvious means of support beyond his modest nonprofit salary."

Davies was silent.

"I don't expect you to say anything, Ron, and in fact you might not want to," Audie said. "But, we have a lot of evidence that leads us to believe you perpetuated a lack of internal controls, and overrode the internal controls that were in place. I hate to think how long this might have gone on if it hadn't been caught." She turned to Henderson – "And, it's probably lucky you were in the room when it was reported." Henderson shuddered.

The lawyer went to the door of the conference room and opened it. A uniformed police officer and two plainclothes detectives stepped in. "Ron Davies," the lead detective said, "you are under arrest for fraud and grand larceny. You have the right to remain silent ... "

Basic Safeguards Against Fraud

- **Lock it up.** This, of course, applies to cash and any other valuable assets that could be taken, but you should also apply this rule to check stock, which might otherwise be tampered with.
- **Don't pre-sign checks.** It only makes life easier for a would-be fraudster.
- **Safety in numbers.** Have multiple people present when cash is counted.
- **Checks and balances.** Different people should handle different cash functions, including deposits, check writing, and bank reconciliations.
- **Stay current.** This applies especially to bank reconciliations.
- **Don't be too trusting!**

Click sections above to navigate

BACK NEXT PAGE

CHAPTER 6

THE ROAD TO RECOVERY

"Well, *that* was brutal," Randolph said. An hour had gone by, and now he and Audie were sitting in Henderson's office to review the situation and decompress. "But, you must be used to this."

Audie gave a little laugh. "This one was pretty dramatic, even for me."

Henderson spoke up from the other side of the desk: "I took your advice and called that PR firm you recommended. I have a call with them at 3 p.m."

"Good," Audie said. "They know what to do in cases like this."

"What do we do now?" Randolph asked.

"I'm going to give you a checklist to review, and then I'm going to work through it with Margaret and the staff in the coming weeks," she said. "Once you've uncovered fraud like this, it's vital that you help the staff get over the shock of it, reestablish trust, and learn what they need to know, so it can't happen again."

"It feels like we're starting over at zero," Henderson said.

"That's understandable," Audie said. "But, keep this in mind: You had an alert, conscientious staff member who reported the problem as soon as she spotted it, and she was able to do that because you have good technology in place now. From talking with the staff, I can tell you how much they believe in the foundation's mission. They want this organization to be strong, and they seem ready to do the work. And, the two of you, I know, are ready to convey the right message of vigilance from the board level, down through the layers of management, and to every member of the team."

"That's my top priority," Randolph said. "It's my name – my dad's name – on the building, and everyone will know how seriously we're taking this."

"That's right, Jon," Henderson said. She turned to Audie. "One thing I don't understand: I've known Ron for years, and I know we did a background check on him, like we do on everyone we hire. His record was squeaky clean."

"I'm not surprised," Audie said. "Most nonprofit fraud is conducted by people with no prior criminal record, so background checks often don't help. Keep doing them, of course, but now the focus is on backing them up with stronger internal controls and transparent communication."

"We have a big job ahead of us," Henderson said.

Audie smiled. "I'm here to help, so let's get to work."

Click sections above to navigate
BACK
NEXT PAGE

YOUR ANTI CHEAT SHEET FOR PREVENTING NONPROFIT FRAUD

Make an Organizational Commitment to Prevent Fraud

Fraud preparedness is not a one-person show – it must be addressed at every level of your nonprofit. Board members have a fiduciary responsibility to prevent fraud; you may need to bring in new board members with more financial expertise to meet this responsibility. Management has a corresponding duty to engage in vigilant oversight of fraud prevention measures, so make sure they're trained and supported to carry out that duty. Staff and volunteers must be trained to spot fraud and respond appropriately, as well.

Understand and Communicate Fraud Risks

Think through the specific fraud risks your organization may face, based on your own business operations, vendors, employees, service providers, and transaction activity levels. Improve your insights by getting input from all parts of the organization, and then communicate your findings transparently to improve understanding and foster trust at every level. *Everyone* should feel safe to express any concerns.

Strengthen Your Internal Financial Controls

Educate your staff on the red flags that could indicate fraud, and implement financial best practices to minimize fraud risks. For each significant operation or activity, for example – handling money or cutting checks to vendors – ensure key finance staff members know the answers to these questions:

- How does this process work?
- Who is involved in this activity, both inside and outside the organization?
- Who initiates transactions?
- Who authorizes transactions?
- Who reviews transactions?
- Have we had anything go wrong here before?
- Why did it go wrong? What can we do to ensure the processes and outcomes are correct?
- How are staff members in the department feeling and functioning?

Practice vigilance! Continually assess incentives, pressures, opportunities, and attitudes that may lead to fraudulent behavior within the organization. Put whistleblower and HR policies in place to reduce fraud risk, and keep your employee handbook up to date.

Click sections above to navigate

Above all, create checks and balances that separate key finance functions. For instance, separate individuals should write checks and sign them, and no one person should be in a position to falsify bank reconciliations or financial reports without oversight. (For a full list of internal controls, visit the Greater Washington Society of CPAs site.)

Use the Right Tools to Help Spot Fraud

The right technology can help an organization be both proactive and appropriately reactive when it comes to detecting and deterring fraud. It will do so by:

- Creating thorough and accurate audit trails
- Promoting sound accounting policies and procedures
- Using built-in functionality to assign users, permission rights, alerts, and more
- Supporting and promoting proper segregation of duties
- Taking advantage of robust reporting tools to dig deeper and investigate suspicious behavior further, as needed

Develop a Clear Plan of Action for Responding to Fraud

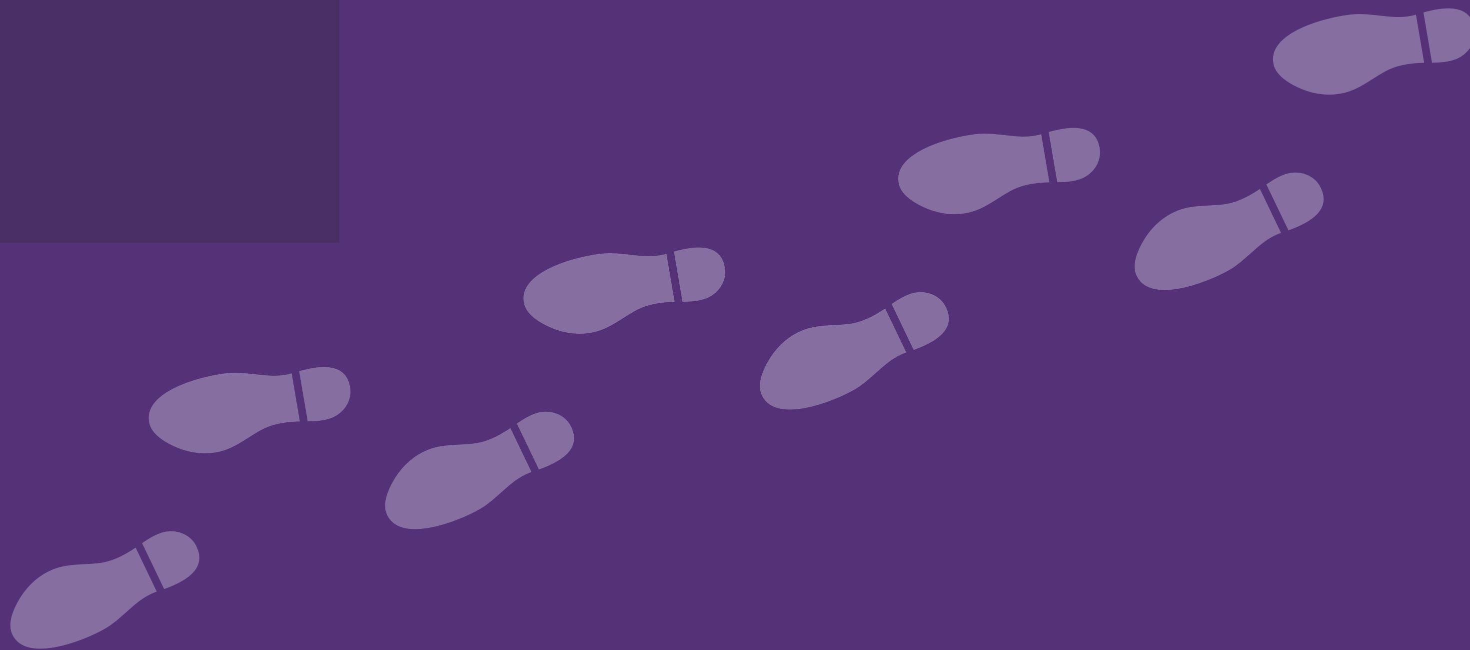
You should have a crisis management and disaster recovery plan that addresses the who, what, when, where, and how, so your organization can deal effectively with any fraud that occurs. This plan will help you understand the decisions that must be made quickly, so your organization can respond appropriately to any crisis. In particular, you should think ahead about when to engage outside experts such as attorneys, forensic accountants, fraud examiners, law enforcement, and PR professionals.

Once you've developed your plan, test your organizational readiness by conducting fraud drills. Actually simulate fraudulent behavior within your fund accounting system to see what it looks like when it goes through, discover how easy it might be to perpetrate, and understand what controls or processes may need to be put in place to spot it and prevent it from succeeding.

Respond Actively to Change

Keep looking forward. Be aware of the fraud implications when your organization gains opportunities for larger fundraising programs, new funding sources, or other new initiatives. Stay alert especially during times of change – in operations, programs, systems, or key personnel – that might impact your anti-fraud controls and processes.

Click sections above to navigate



- The Scene
- The Shock
- The Betrayal
- The Response
- The Confrontation
- The Road to Recovery
- The Anti Cheat Sheet

Click sections above to navigate