INSIDE JOB

Fighting internal fraud in state benefit programs

By Sophia Carlton, CFE, and Suzanne Carlson

While external fraudsters who absconded with billions of dollars in pandemic relief have dominated headlines, less attention has been paid to employees scamming those very same programs. Here we spotlight internal fraud at state agencies and what organizations can do to fight this pernicious type of fraud.

In the two years since the advent of the COVID-19 pandemic, news headlines have been awash with sensational stories about international crime gangs and con artists who stole billions of dollars in government relief money. But while these stories captured the public's attention, another type of fraudster was plying their trade in state benefit agencies across the U.S. — the internal fraudster.

Take Brandi Hawkins, a contractor in Michigan's state unemployment insurance office. She pleaded guilty to defrauding the agency of $3.8 million in pandemic aid by entering numerous false claims into the state's employment insurance agency system, often using stolen identities. Hawkins accepted bribes in return for releasing payments on more than 700 claims to external accomplices. (See "State Contractor Pleads Guilty in $3 million Unemployment Fraud Scheme," U.S. Department of Justice (DOJ), June 30, 2021, tinyurl.com/2hb4javh.) And, Reyes De La Cruz III, who was employed in the Washington State Employment Security Department as an intake agent, filed fraudulent claims paid out to debit cards, impersonated claimants and accepted bribes in exchange for engineering benefit payments for friends, family and acquaintances. (See "Former Employment Security Department employee indicted for filing false claims and demanding kickbacks," U.S. DOJ, Sept. 24, 2021, tinyurl.com/2p88red2.) These examples may have filled U.S.DOJ press releases but not the big national headlines. In the case of state benefit programs, internal fraud is the threat few are talking about.

Tip of the iceberg

Indeed, fraud against government agencies was big business during the pandemic with the U.S. Department of Labor estimating in September 2021 that about $87.3 billion in unemployment insurance (UI) had gone to fraudulent payments. (See "DOL-IG Oversight of the Unemployment Insurance Program," U.S. Department of Labor Office of the Inspector General, Jan. 3, tinyurl.com/yhenf33e.) The U.S. Secret Service reported in December 2021 that fraudsters had stolen almost $100 billion of the $5 trillion in pandemic stimulus funds distributed to the states by the U.S. government. (See "Criminals have stolen nearly $100 billion in Covid relief funds, Secret Service says," by Eamon Javers and Scott Zamost, CNBC, Dec. 21, 2021, tinyurl.com/3b5shvew and "Where $5 Trillion in Pandemic Stimulus Money Went," by Alicia Parlapiano, Deborah B. Solomon, Madeleine Ngo and Stacy Cowley, The New York Times, March 11, tinyurl.com/32upwv67.) These reported losses are staggering on their own if we're only considering the external frauds, but taken with possible losses from internal fraud, we might only be seeing the tip of the iceberg.

Time to focus on internal fraud

Organizations often focus on the threat of external actors. It's easier to make sense of a bad actor from outside the organization than it is to understand trusted employees or colleagues as bad actors. Organization leaders often wear rose-colored glasses, preferring an optimistic view of the people they entrust to carry out the day-to-day tasks of essential state business. While it's understandable to think the best of employees, this view hinders meaningful actions to prevent, detect and mitigate internal threats.

Perfect conditions for internal fraud

State benefit programs are just as vulnerable to internal threats as any other organization. No matter how strong the controls and processes or how "good" the people are, there's no such thing as zero internal fraud risk. The pandemic and the influx of government aid disbursed to state benefit programs intensified the risk factors that can lead to internal fraud. Those risk factors included:

- New programs rolled out overnight, such as the Pandemic Unemployment Assistance (PUA) program.
- An unprecedented number of UI claims and states relying on legacy systems too outdated to withstand the onslaught.
- Benefit programs outsourced to contractors/vendors, such as leveraging contractors for surge support to accommodate the overnight increase in claims. In some cases, states relied on these contractors to verify work quality or adherence to controls.
- Swift adjustment to controls, processes and the way states interacted with claimants as a result of the pandemic. This meant changing processes to accommodate the quick shift to remote work, implementing overrides for key controls to expedite claims or shifting to all-digital interaction with claimants when previously in-person interaction was the norm.

How do all of these factors come together to impact internal fraud? We can use Dr. Donald Cressey's Fraud Triangle to better understand how the confluence of factors described above heightened the risk of internal fraud. The three components of the triangle — perceived unshareable financial need (often expanded to mean "pressure,") perceived opportunity and rationalization — are the conditions necessary for fraudulent behavior. (See ACFE.com/fraud-triangle.)

In the case of pandemic-era state benefit programs, there was ample opportunity for unscrupulous internal actors to take advantage of a difficult situation. Fast rollouts, increased work volumes, outsourcing and changes to processes left little room for diligent oversight and created an environment perfect for internal fraudsters.

CONTINUED ON PAGE 30

Internal fraudsters' MOs

Every fraudster has a modus operandi (MO), or a method by which they commit fraud. When it comes to the MOs of internal fraudsters, we've seen the following:

Collusion with claimants. The internal actor colludes with claimants to increase the benefit amount of an otherwise legitimate claim or fraudulent claim.

Account takeover. The fraudster abuses their access to the state's system to take over active or dormant claimant accounts. From there, they might increase benefit amounts and redirect benefits to their own bank account or an accomplice's account.

Fabricated accounts. The fraudster abuses their access to create fake accounts that directly benefit their own bank account or an accomplice's account.

Family and friends. A variation of collusion with claimants but in this case the fraudster colludes with their family or friends.

Fraudster's own claim. The internal actor abuses their access to the program system and submits a benefit claim on their own behalf to receive fraudulent payouts.

Information theft. The internal actor abuses their access to the program system to steal personally identifiable information (PII) or other sensitive information for nefarious purposes, such as selling it on the dark web or committing identity crime.

6 strategies to fight the inside job

Internal actors are making their mark and taking advantage of their access to get big payouts for themselves and their accomplices. So, what can we do about it? We suggest the following six strategies to reduce risks and identify losses from fraud.

1 **Acknowledge the risk.** Fraud can't lurk in the shadows if you acknowledge that the risk exists. This may entail a culture shift to ensure fraud isn't a four-letter word, and when it comes to internal fraud, ensuring it's not avoided simply because it's uncomfortable to think about.

2 **Understand where you're vulnerable.** Assess where in your controls and processes you're vulnerable to internal fraud. Where are the gaps? Where are the overrides? Where's there a lack of oversight? How's access to your organization's system managed and monitored?

3 **Identify red flags.** Internal fraudsters often engage in certain practices that can be flashing red-light warnings of fraud. In our experience, internal fraudsters often work late into the night or on weekends to perpetrate their frauds when co-workers or supervisors are less likely to observe them. In some cases, an internal bad actor might go out of their way to perform tasks that aren't part of their job description to better carry out a scheme. Determining what might be a red flag in your program can help you better identify bad actors and stop them in their tracks. It's important to remember that red flags may differ depending on the state or program.

Here are some specific examples of how internal fraud can appear in state benefit programs and their MOs:

BACKDROP FOR INTERNAL FRAUD	MO
A state contractor hires one or more subcontractors to support call-center and claims adjudication tasks for an agency's UI program. The subcontractor doesn't follow security measures for user logins and allows employees to use any login, thus hundreds of username and password combinations can be compromised. One or more subcontractor employees may take advantage of this loophole and commit fraud across various logins to cover their tracks.	**All**
A state employee uses social media to advertise their role as an adjudicator in the state's UI or disability insurance (DI) program and offers to approve anyone's UI or DI claims for a fee.	**Collusion with claimants**
A contractor who's a member of a surge support team is recruited by an identity theft ring. The contractor then leverages their access to the state benefit program to get sensitive information, such as addresses, Social Security numbers and bank account details, which they then share with the crime ring for use in other identity crimes. This scheme can be difficult to discover since the internal fraudster is only searching and viewing multiple claimant profiles without raising any obvious red flags.	**Information theft**
A state employee abuses their access to approve family members' and friends' UI or DI claims. This could include fraudulently increasing the payment amounts and submitting and approving their own claims.	**Family and friends**
A contractor working in a state's disability insurance program looks to increase their payout from an ongoing fraud they've been perpetrating. To do so, they recruit other insiders — such as state employees or other contractor resources — to take part in the fraud over the course of several months. This group continues to commit fraud and works together to obscure their tracks and hide the evidence.	**All — This scheme focuses on collusion among insiders to commit fraud and any of the MOs could apply.**
A contractor is terminated but access to the state's program system isn't terminated. The contractor has been committing fraud and continues to do so after termination, leveraging their continued access.	**All — This scheme focuses on system access and any of the MOs could apply.**

4 **Assemble an investigative team.** To understand whether internal fraud has occurred in your organization and where it's occurring, you'll need to put together a team that can investigate leads and referrals — such as hotline tips and referrals from a supervisor, law enforcement and/or a lead identified through proactive detection mechanisms. This investigative team can work in tandem with any existing fraud investigative groups or be a stand-alone team. There's no right way to assemble the team as long as proper processes and governance are in place. For example, this should involve documentation that outlines the investigative process end to end, a team charter and an organizational chart to show how the team will coordinate and report into other functions and leadership.

5 **Get proactive.** Investigative teams often rely on reactive detection, only investigating fraud after receiving a tip from an employee, supervisor or even law enforcement. The problem with relying on reactive detection is that many frauds end up getting through the system unfettered. But proactive detection — detection that can root out fraud as it's occurring — should be baked into your anti-internal-fraud strategy. An example of proactive detection is a data analysis tool that scans systems for any of your previously identified red-flag behaviors. You can create a scoring system that prioritizes any red flags the analysis tool identifies to ensure that the investigative team focuses on high-value leads.

6 **Don't forget external fraud.** Even though stories about internal frauds were overshadowed by headlines about external frauds, it's important to remember that external fraud and internal fraud often go hand in hand and are generally seen in situations where an insider teams up with an outside fraudster. If you have separate internal and external investigative teams, ensure that they communicate with each other.

Taking the fight against internal fraud to the next level

Along with the strategies we detailed above, state agency leaders can enhance their anti-internal-fraud operations with the following tactics.

Focus on prevention. Prevention is best achieved with strong controls and processes. Leverage the insights you gained from the analysis of your vulnerabilities to identify the controls you need to strengthen.

Make internal fraud part of training and awareness initiatives. Many times, organizations focus their employee training and fraud awareness efforts on external fraud threats. But employees need to know about internal fraud and how to spot it. Be sure to include examples of internal frauds in employee training and explain the role they play in internal fraud risk management and how they might go about reporting tips or suspicious behavior.

Reassess your risks. Risk assessment isn't a one-and-done activity. Risk assessment should be periodically revisited, whether you do it every year or every other year. It's also important to reassess your risks on an ad hoc basis whenever a major event affects your fraud landscape. From your assessments, you might determine that you need to reorganize the department or implement a new system, for example.

Define it in your fraud policy. Your fraud policy should include a definition of internal fraud and examples of what constitutes internal fraud. This internal fraud policy should also include the ramifications or actions taken if fraud is identified — such as termination of the employee.

Act now. Effectively managing internal fraud risk is a long-term journey. Any organization can benefit from determining where it might be vulnerable to internal fraud and develop strategies for detecting and preventing it. It's imperative to focus on managing internal fraud holistically, with an eye on proactive and strategic internal fraud risk management. ■ FM

Sophia Carlton, **CFE**, is a manager in the fraud and financial crimes practice at Accenture. Contact her at Sophia.Carlton@Accenture.com.

Suzanne Carlson is director, fraud consulting at Accenture. Contact her at Suzanne.e.Carlson@Accenture.com.