



THE Enemy *Within*

Texas Association of School Boards offers cautionary tale for workers' comp risk pooling standards and practices following dramatic discovery of massive fraud by trusted employee

It was right out of a movie or riveting crime novel. Dubravka Romano was in London for meetings with reinsurance underwriters in March 2013 when the phone rang. "Are you sitting down?" a caller asked the associate executive director for risk management services with the Texas Association of School Boards.

Whenever such a foreboding rhetorical question is posed, it's almost always followed by terrible or shocking news. In this case, a red flag waved wildly back in the Lone Star State. Roughly \$200,000 worth of self-funded workers' compensation payments made to a medical provider were curiously traced to one of TASB's most trusted, respected and affable employees – in a supervisory role, no less.

Hmm, she thought. There must be much more to the story than meets the eye. Indeed, there was. Suspicious activities led investigators to uncover a series of brazen crimes committed intermittently over a decade using three separate theft schemes and two fictitious vendors.

The culprit was none other than Herman G. Wilks, director of TASB's workers' comp claims administration who later pled guilty to charges of embezzling more than \$1 million from the fund's workers' comp and employee benefit programs. It was a fox-guarding-the-henhouse moment that shattered trust and stirred emotion right alongside the terrible toll it took on time, financial matters and morale.

Romano was dumbfounded. When she first confronted Wilks, there was a long and uncomfortable silence – confirming her fear that serious wrongdoing had been committed.

“Fraud really can and does happen,” she recalls one of TASB's board members, a retired IRS agent, saying prior to this revelation. *“It was such a shock to our organizational consciousness because we see ourselves as a bunch of do-gooders in the world.”*

Fraud-prevention strategies

What makes this story even harder to comprehend is that massive fraud took place at TASB in spite of rigorous annual audits, regular external reviews by reinsurance partners, an active internal audit function and regularly scheduled policy reviews that adhered to industry standards.

Could a similar scenario occur within other self-insured entities? Apparently so, according to Romano. Upon hearing the details of her account, several people have sheepishly admitted to uncovering fraudulent activity in their own organization, though on a smaller scale.



She has given about 10 presentations on the topic (aptly entitled “The Enemy Within”) in hopes that it helps prevent a reoccurrence of the TASB debacle. Each talk deepens the level of catharsis that helped power her organization through this crisis.

Romano suggests that employers pay particularly close attention to reviewing their vendor-management process, as well as verify the legitimacy of all service providers and remove those with whom they no longer do business. Another tip is to verify system security, which TASB now does on a quarterly basis. In addition, she says there must be an audit trail with detailed records, which can be bolstered by a response plan and crisis communications strategy.

Her dramatic account of this story, which Romano gave at SIIA’s national conference last fall and a recent webinar, was “incredibly heartbreaking” to Freda Bacon, who administers the Alabama Self-Insured Worker’s Compensation Fund and is on SIIA’s Workers’ Compensation Committee. “To have that type of fraud occur right under your nose, it’s an eye-opener,” she says.

This is especially true for fellow public entities that she believes are expected to go the extra mile from a fiduciary standpoint. “You have to have very firm guidelines that you can

present to your board of trustees or the public that you’re doing everything you can to detect and prevent fraud,” Bacon explains. After nearly 40 years in business, Bacon has never heard of anything quite like TASB’s tale occurring among peers.

Fraudulent or criminal behavior in this sector is exceedingly rare, reports Ann Gergen, executive director for the Association of Government Risk Pools. The group’s mission is to provide public entity risk pool education and networking, as well as operational and best practices support, to more than 200 members in the U.S. There are 78 AGRiP recognition standards that are based upon a self-audit process for these pools to follow and continually improve over time.

LEARN. PLAN. SAVE. PROTECT.

**RECOVERY
DOLLARS
MULTIPLIED**

Subrogation & Overpayment Recoveries

**PLAN
DOCUMENTS
PERFECTED**

Phia Document Management
- PDM



**THE
PHIA
GROUP**

EMPOWERING PLANS

**FIDUCIARY
DUTY
SHIFTED**

Plan Appointed Claim Evaluator - PACE

**LEGAL
EXPERTISE
SECURED**

Independent Consultation & Evaluation - ICE

Register online to join us monthly for our free, industry acclaimed webinars.

The Phia Group, LLC | 163 Bay State Drive, Braintree, MA 02184 | Phone: 781-535-5600 | www.phiagroup.com



“An audit is designed to identify process improvements,” Gergen says. “We see pools actively engaging in conversation to share how they’re improving their own operations. Our pool members are highly collegial and very collaborative. They view themselves as extensions of the public entities that they serve, and by and large, they’re people who are passionate about providing local government public entity service.”

Peeling back the onion

When TASB investigated Wilks’ wrongdoing, Romano and her crew wondered how he went undetected for so long. Eventually they learned that he had requested a report on large hospital bills to identify actual workers’ comp claimants who received medical implants.

The information was then used to create fictitious medical bills with codes for implantables into the claims system with a slightly altered date of service to circumvent system controls that were in place to detect duplicate payments. Payments were surreptitiously entered, adjudicated and released after work hours. Wilks also changed the address for a claimant’s explanation-of-benefits form in the system to his own so that it would not go to the employee, then changed back the address after the check was issued to himself.

The crime triggered a comprehensive probe by a former FBI agent whom Romano describes as “straight out of Central Casting with a crew cut, blue suit, white shirt and dark tie.” Since TASB is a public entity with dismayed taxpayers to consider, this theft necessitated the involvement of additional law enforcement officials.

In addition, two separate internal control audits by a Big 4 accounting firm were done to determine how the theft occurred before a U.S. attorney began prosecution. TASB soon discovered that Wilks was able to circumvent a four-step claims adjudication process because of his intimate knowledge of the system.

But he obviously tripped himself up along the way. The dead giveaway was having an employee with his own LLC, surmises Stu Thompson, CEO of The Builders Group, a construction self-insured group started in 1997, and member of SIIA’s Workers’ Compensation Committee. “I was amazed at how much he was able to get away with, especially over a long period of time,” he says of Wilks.

A key takeaway from Romano’s presentation is to know who’s being paid, whether they’re staffers or contractors, according to Thompson, and ensure that all necessary forms that must be filed are accurate, including name, address, federal ID number, etc.

“We have Positive Pay,” he explains, “so if there’s any type of questionable payment from our bank, they alert us, and then we can say yes or no.”



The TASB crimes made him reevaluate his own operation, which pays more than \$20 million in claims each year. He believes that having a TPA to adjust and pay claims adds another layer of protection. When Thompson returned home from the SIIA conference he made sure he had an updated certificate of insurance from his TPA so he knew what their fidelity limit was in the unfortunate event of a crime occurring.

TASB has since taken corrective steps to prevent this type of fraud from ever happening again. They included changes to the vendor set up and maintenance process, IT system security and set up, and segregation of duties. Other actions involved greater focus on fraud awareness, as well as TASB ethics and values.

Wilks pled guilty to 10 counts of mail fraud in January 2014 and was sentenced to 63 months in federal prison just two months later when he also was ordered to pay full restitution for his crimes. He also wrote a letter of apology to his supervisor and will be eligible for release in November of this year.

One of the painful lessons TASB staffers learned was that internal controls are everyone's responsibility, not just the finance department, which reviewed its internal-control recommendations from purely a financial and not also operational lens. While compliance can be burdensome, it's also seen as necessary.

But beyond that, Romano says collateral damage actually can be much worse than financial losses. She cites a long list of unfortunate consequences that included a profound sense of shock and disbelief, loss of trust and confidence, resentment and extra work to review processes.

She also mentions that Wilks' actions triggered serious betrayal, shame and embarrassment, particular among his fellow African-American employees for whom feelings of disappointment perhaps ran deepest among all TASB staffers. In short, she says many of them were at once mortified and apologetic. Romano recalls how Wilks was genuinely remorseful, but that did not change the fact that unraveling his crimes proved to be time-consuming for her staff as well as emotionally draining on a personal level.

Her sage advice to others: *“Be prepared with a response plan, be prepared with a crisis communication plan, which we did not have, and be prepared for a recovery plan.”* ■

Bruce Shutan is a Los Angeles freelance writer who has closely covered the employee benefits industry for nearly 30 years.