

# New Tools for FRAUD Detection

Tom Quin, CPA

No one would argue these are tough times. And what do tough times bring? Resourceful individuals who believe they have been placed between a rock and a hard place. This economy has made more desperate people who can only see the way out by doing more desperate things. It seems wherever you turn in the profession, there it is in front of you: *Fraud, FRAUD, FRAUD.* And those newly minted desperate people are working at your clients!

Here's what I know from experience as a practitioner, peer reviewer and qualified expert witness regarding fraud.

- All fraud has a personal motive.
- We're doing a lousy job in looking for it. *"That's true"* I can hear you saying, *"but our engagement letter clearly reminds the client that it's not our job!"* I would say professionally you're on shaky ground and more importantly, most clients think that it's part of your job to watch the henhouse.
- Searching for fraud is like looking for a needle in a field of haystacks. We won't have much success if we attempt to do it manually, and computerized fraud tools are limited and in their infancy.

## **Personal Motive**

Fraud takes many forms but either involves a theft of assets or fraudulent reporting to achieve some gain. All fraud gets the perpetrator something. Fraud will almost universally involve these elements:

- Some form of personal pressure or incentive
- The control environment may allow nefarious activity to go undetected
- Rationalization of the fraud by the fraudster

Can the auditor comprehend the individual motives of all the employees in the company? Of course not! Approaching the required fraud "team meeting" as part of the audit, I will often hum a song with the appropriate title; "Little People Make Big Mistakes" found on the 1988 Eden Alley CD by a now forgotten group, Timbuk 3. It sets my mind to be alert to personal motive at every level and to rotate fraud awareness emphasis among departments and systems each year.

A second thought for the meeting is mindfulness of *professional skepticism*. In my peer review travels, this is one question not asked on any checklist: Is the practitioner/firm skeptical in their approach to the audit? The smaller the client and the longer the firm has had that client, the more we convince ourselves fraud can't happen. Yet the vast majority of our clients suffer from segregation of duties issues and/or a concentration of authority issue. Our trust in past results as predictors of the future ignores human behavior where rationalizing fraud for personal need can occur at any time.

### **Professional Requirements / Client Expectations**

We are required in SAS 99 regarding fraud, and now as part of the "Risk Suite" of SAS 104 – 111, to understand the entity's operating environment (control and inherent risk); meet and discuss motives and incentives at the entity and individual levels; and to develop testing to detect material items that penetrated the control armor.

An earlier article, (SUM News Summer II 2009) alerted readers of the need to sharpen their audit skills with the use of CAATTs tools. But the language in the "Risk Suite" does not mandate use of CAATTs. Rather, the language says, "When the information is in electronic form, the auditor *may* carry out through CAATTs certain of the audit procedures described ...." For those still clinging on to the word *may*, think about what an opposing expert witness at your trial would do to your audit approach for failing to detect a fraud while using a manual approach to the audit. I contend jurors will hold to a misunderstanding that auditors are responsible for fraud detection. Clearly if your approach to testing isn't iron clad, or meeting industry standards, you may not stand a chance.

The issue of client/public expectations regarding the role of the auditor has a fascinating history. Early in the 70's the Cohen Commission coined the term "Expectations Gap." The concepts were advanced through the Dingell Committee and then the Treadway Commissions Committee of Sponsoring Organizations issuing its "Internal Control – Integrated Framework." However, these commissions were largely focused on the very public and material fraud issues involving "Earnings Manipulations." Most of us reading this article would agree that Earnings Manipulation is not the garden variety of fraud at play for the majority of our clients. And, along the way, right or wrong, big business "Earnings Manipulation" and small business "Garden Variety Fraud" became merged through "one size fits all" common professional pronouncements.

I'm concerned about the expectation of our **clients** regarding theft of assets or, in the non-profit 501(C) world, the additional concern of **donors** regarding assets entrusted to be safeguarded toward some purpose. So what do you do if you either sense or stumble upon fraud as part of your testing? You should, as an initial step, have a frank discussion with those in governance as to your feelings or testing results. Depending upon the nature and materiality involved you may want counsel involved before proceeding further.

If the decision is made to enter into an investigation, the next step is to decide who will actually do it. Fraud investigations require fraud expertise that most auditors don't have so the decision has usually been to bring in forensic auditors. But "fraud-aware" tools are now becoming available. Fraud expertise is built into these tools, so they may offer another option.

### **Tools for Fraud Detection**

As I do my Peer Reviews, I see more auditors using CAATTs software for their audits. Unfortunately, existing CAATTs software, while powerful for arranging internal company data and performing selection for audit testing, falls short when my "*Spidey sense*" starts to tingle during an audit. Remember your basic college level auditing course where it was stressed the differentiating feature of an audit was verification of company data against an external source? That hasn't changed.

The current CAATTs tools are reliable and at QRG, LLP we find they save time in recurring audits. But as good as these general-purpose audit test tools are they all share two important fraud-detection deficiencies:

- "Fraud expertise" isn't built into them and, because of that, users need to supply that fraud expertise themselves. What are the most common fraud schemes? What data might expose those schemes? What exactly am I looking for? Where do I look for it? Fraud could be anywhere.
- The tools primarily analyze internal documents like registers, A/P ledgers or A/R ledgers. Though lots of fraud schemes can be uncovered by looking at these sources alone, uncovering many of the most common frauds also requires searching external data such as bank statements, payroll service reports and credit card statements. If existing tools had easy ways of accessing this data, they'd be much better fraud-finding tools. But they don't.

The good news is that technology is never stationary. A new breed of "fraud-aware" CAATTs tool is becoming available. At QRG we've used one tool from a Massachusetts company, TraceTech Solutions ([www.tracetechnologies.com](http://www.tracetechnologies.com)) and we were favorably impressed. It is not a general-purpose CAATTs tool; it was specifically designed to look for fraud. It can run about fifty pre-programmed tests, each of which was designed to uncover traces of specific fraud schemes, and the tests can incorporate both internal and external data.

An example of such software being built fraud aware is the common scheme of altering a vendor check. The perpetrator writes a check to him/herself – but records the check as vendor payments. Another common scheme is the fraudster skims cash from deposits before the deposits are made. In both cases the theft of assets is concealed by falsifying internal data, and since general-purpose CAATTs tools typically examine just internal data, they wouldn't provide clues to either scheme.

The fraud-aware tool, though, knows about “bank statements,” and the tool includes software that simplifies the process of getting bank statement data into a form that can be tested. To help expose the check-tampering scheme, the tool compares statement data to the ledger, and (a) reports any differences (payee and amount) in checks between the statements and the ledger, (b) reports any cashed checks that are not recorded in the ledger and (c) summarizes all checks (totals and averages) made to every employee. And since online banking is becoming prevalent, the tool can do the same with wire transfers.

To help uncover the deposit-skimming scheme, the tool reports any differences in deposits between the statements and the ledger. Under certain conditions it can go even further. If the client normally records the composition of each deposit (cash vs. checks) as part of its control procedures, the tool compares the statement to that too. It reports every deposit in the statements whose amount matches the checks-only component of a deposit, which may indicate that the cash was swiped before the deposit was made.

As with general-purpose CAATTs tools, the new tool is not meant for every engagement but it may provide additional comfort to the audit, or if the tip of the iceberg has been uncovered the tool can prove an invaluable aid in detecting the “how much” and “how accomplished” aspects.

**Summary:**

You can hide under professional guise and it *may* protect you from judgment. However the client has other expectations when it comes to fraud. As professionals we have to keep up with the times. Statistics show fraud is almost universally present. As auditors, our literature requires us to design our testing to detect material misstatements, and for the most part current CAATTs software will get you that far. More pernicious and potential deadly non-material fraud schemes need more help in diagnosing. If any of the fraud triangle elements are present (PRESSURE – OPPORTUNITY – RATIONALIZATION) consider new tools that are just coming online to root out the cause.

**Tom Quin, CPA**, is a partner with QRGACPA, LLP, a peer reviewer and member of the RAB for the MSCPA, a former adjunct professor for Stonehill College, and a qualified expert witness for both federal and Massachusetts state courts. Tom can be reached at [TQUIN@QRGACPA.COM](mailto:TQUIN@QRGACPA.COM)