

Vol. 26, No. 6, November/December 2011

# FRAUD<sup>®</sup>

M A G A Z I N E

## MINING FOR HOTLINE GOLD

HELP YOUR CLIENTS UNEARTH HIDDEN FRAUD TIPS

### PLUS

Corporate Smartphones in Danger, PG. 19

The Spinster and the Dubious  
Investment, PG. 24

Falsifying Government Claims, PG. 38

Data Breaches, Part 2, PG. 48



# MINING FOR HOTLINE GOLD

## HELP YOUR CLIENTS UNEARTH HIDDEN FRAUD TIPS

BY ROBERT TIE

**M**aybe the tip was penny-ante. But possibly it was the tip of a fraud iceberg. Lead Investigator Ian Richard and his three colleagues specialize in finding out such things. All are CFEs in the fraud unit of the office of the city auditor in a major American municipality.

In August 2009, they received an anonymous hotline call stating that an employee at a community center owned and operated by the city was stealing a significant amount of food provided by the center's supplier. Unfortunately, the caller did not identify the employee by name or position, mention when and how he was stealing the food or whether he had accomplices.

"This wasn't predication for a full investigation, but a background check was called for," Richard said. He learned from the community center's website that the center hosted a community meal program with food provided by the supplier the caller had named — a food pantry.

By inquiring discreetly over the web, Richard had ensured the center's staff remained unaware of the hotline call. He marked the vague tip for follow-up and turned to other pending cases that had stronger and more specific evidence. Richard hoped the anonymous tipster would call again with additional information. Time would tell.

A few weeks later, someone provided a second anonymous tip about the community center. Because the city auditor's office

is not a large organization, regardless of the way a tipster contacts it, a combination of procedurally integrated channels ensures that all investigators have access to the same tip. This one came in via the office's online complaint reporting form and stated that a manager at the community center was violating cash handling policies.

"That was worth a phone call to the human resources manager of the city department that oversees the community center," Richard said. He informed HR that the city auditor was beginning a fraud investigation that had to remain confidential until completed. With the manager's help, Richard obtained the job description for every employee at the community center. This told him who handled cash and signed for food from the supplier.

Three employees — the center's manager, an assistant manager and a clerk — performed these functions and could have been the person(s) the caller and writer had described. So, Richard had gathered more information about the alleged frauds, but still no one at the community center knew he was watching.

Just days after that, the telephone hotline rang again with yet another anonymous tip. The tipster did not know an investigation was underway, but now he had raised the stakes. The latest report alleged that the center's manager was renting out the building secretly, keeping the fees for himself and not entering



A good lead is an investigator's best friend. But the relationship sours when a tip goes unrecognized or is misinterpreted, which allows a fraud to continue. Encouraged by anti-fraud legislation, more companies are setting up multi-channel hotlines. As the volume of tips increases, so has the number mishandled when related allegations are received via unintegrated email, websites, telephone and "snail mail." Here are the techniques and technologies knowledgeable CFEs use to overcome that challenge.

those transactions in the city's central rental database. If true, this had the potential to cause the city greater financial losses than the other alleged violations.

Accordingly, Richard deepened his investigation and learned that the center indeed was available for rental to generate income for the city. But, of course, there was a risk that someone could fraudulently rent out the center "off the books." The caller had also mentioned that the manager was the only person who ever scheduled rentals and that he kept a private schedule book in his possession at all times. The information Richard had gathered thus far made two things clear. First, any of the three suspects could have stolen food and mishandled cash. Second, only the manager could have committed the possible embezzlement alluded to in the last tip. Overall, he was the primary suspect, and the alleged potential rental fraud posed the most serious risk to the city.

Looking for more hard facts to shed light on the allegations, Richard checked the city's central rental database, which showed that the center had been rented infrequently. Richard and his colleagues also obtained records of the center's weekly cash receivables and attempted to reconcile them with the center's bank deposits. The two sets of entries were similar but not identical. The total amount deposited in the bank matched the center's records, but the bank's tally of how much was deposited in cash and how much in checks did not agree with the center's version. A superficial examination would not have detected the discrepancy.

"That was key," Richard said. "It was a red flag that the manager was running a check-for-cash substitution scheme." When the investigation team attempted to confront the manager with this evidence, he left the facility and resigned the next day. The reported schedule book was never recovered. However, when the investigative team interviewed center staff, it learned of several long-standing, undocumented renters. One, a private basketball league, appeared to have rented the center almost every Saturday for the past three years. As proof, the president of the basketball league provided the investigators with three years of bank statements that listed checks paid to the city. During that period, the manager had reported and deposited the income from a mere 15 rentals.

Sometimes renters had paid by check, but most had used cash. When the manager received a check, he would not deposit it until he received an equivalent amount of cash rental income. Then he would report one rental but not the other, deposit the check and keep the cash. Direct evidence proved that the manager had embezzled \$12,000 during the previous five years. Circumstantial evidence indicated he had stolen approximately \$50,000 over a 10-year period. While none of the stolen money has been recovered, he has been indicted for second-degree theft and is awaiting trial.

*(Note: Because the case is pending in criminal court, the names of those involved and certain other details of identification have been changed. However, the tips and investigation did take place as described.)*

Richard said his team detected the scheme not only because of their investigative persistence, but because they had a well-integrated hotline system and procedures that enabled them to connect tips from disparate reporting channels. "The two go hand in hand," he said.

In FY 2010 the office of the city auditor received 173 tips through five reporting channels: the two described above, plus direct contact with an investigator by phone, email or in person; referral from other city agencies; and from audit findings. The office expects to have received a similar number by the end of FY 2011.

In such smaller organizations, investigators benefit from clearer visibility of all operations and potential sources of tips. Time-tested procedures for them often are the backbone of an operationally effective and economical hotline system.

"We produce results on every tip we receive," Richard said. "Some we refer to other agencies because they don't fall within our purview. On everything else, we do whatever is possible and warranted."

But what about larger organizations that receive many more tips from a wider range of sources? This challenge increases when the number of investigators does not keep pace with the higher caseloads that some hotlines generate. For such entities, integrated communications systems are necessary to gather and share leads among numerous departments, many of which are relatively unfamiliar with each other.

Even so, as the following discussion illustrates, automated systems cannot carry the day alone. For the foreseeable future, organizations will have to augment them with well-integrated analytical procedures and techniques if they hope to fully connect, assess and act on all the tips they receive.

**TOO LITTLE, TOO LATE**

A large manufacturer engaged Bethmara Kessler, CFE, CISA, PI, and Lynne Frishman, CFE, managing directors of The Fraud Risk Advisory Group, a consultancy in Melbourne, Fla., to determine whether, as reported on its hotline, one of its managers had a conflict of interest involving a vendor.

The allegation named the manager but not the vendor. So Kessler and Frishman compared the manager’s activity to that of her peers and found significant differences. For example, the suspect appeared to have an unusually close relationship with certain vendors. Additionally, when interviewed, numerous employees and vendors expressed concerns about the manager’s ethics because she socialized with several vendors. Many of her co-workers also acknowledged calling the hotline with tips about the manager but had done so anonymously because they feared her.

The company had not developed those leads because they seemed too imprecise to warrant an investigation. But Kessler and Frishman found the hotline complaints had been tagged inconsistently and thus were routed to investigators in a variety of departments — HR, compliance and security — that communicated with each other only sporadically. That was particularly unfortunate, Kessler added, because there was enough detail in the complaints — if viewed together — to provoke an investigation.

Kessler and Frishman checked ownership records, and they discovered that the manager had interests in several vendors with friends and relatives and was overpaying for materials her employer bought from them. The scheme already had cost the company \$2.5 million. But most of it had occurred after other employees had called in the tips that, if connected and investigated together, would have limited the company’s losses to \$500,000.

“To make matters worse,” Frishman said, “when their hotline calls had no effect, the employees who had made them now thought management was corrupt and would not stop fraud even if told about it. If those workers had revealed this to others, it might have emboldened some to commit fraud themselves.”

**ALL TOGETHER NOW**

Many organizations do not have sufficient resources to coordinate and interpret the enormous amounts of data flowing into

their hotline systems. So they often give statistical summaries and a few representative tips and complaints to audit committee members and other key stakeholders.

“That doesn’t offer executives and investigators any useful insights on fraud,” Kessler said. “These systems might capture lots of valuable information, but their standard reports are based on a superficial analysis of it. That does not help you understand individual fraud risks and schemes. Nor does it tell you which fraud prevention measures work and which don’t.”

Such analytical myopia and its symptoms are far from rare. According to the 2010 ACFE Report to the Nations (p. 47), “Nearly one out of five [fraud] victims retained the same control system — or lack thereof — that was ineffective in preventing the reported fraud schemes.” The Report notes that only 7.9 percent of organizations modified their hotlines after discovering fraud.

“As we have seen,” Frishman said, “a hotline system can remain persistently uncoordinated, with tips and leads repeatedly tagged inaccurately and referred to staff who do not understand their significance or know how to handle them. Some tips do not contain the keywords that will cause them to be routed to an appropriate investigator. For example, a hotline call that said, ‘I’m scared I might get in trouble,’ might be routed to HR, while one that said, ‘I’m worried I might be retaliated against,’ could be referred to the legal department. Although two such calls might relate to identical situations, the slight differences in their wording could greatly vary the responses they receive.”

To counteract this tendency, Kessler and Frishman began speaking with clients about mining their hotline data to ensure that data ambiguities and inconsistencies would not prevent them from seeing important connections between tips. Such analysis has become an innovative service for them.

The firm also recommends that clients periodically test their hotlines. To illustrate this, Kessler will call in a complaint and observe how the system classifies and routes it. “Sometimes they get it wrong,” she said. “But training can quickly resolve such deficiencies, as long as someone detects them. Companies periodically check their fire and smoke alarms. They should do the same for their hotline systems.”

It is also important to determine whether any reporting channels are not integrated with the hotline. “It’s a recipe for missed leads when the person who manages the hotline is not also responsible for its ancillary systems,” Frishman added.

**PARSING FRAUD TIPS**

Every hotline system Kessler and Frishman have worked with is text-based. But that does not guarantee uniformity of data formats.

Date	Timezone	Caller	Severity	Category	Location	Investigator	Comments
12/29/13 10:24	EST	HR Issue	3	HR Issue	HR Issue	S. Brown	Caller states that BOB 'JOHN' does not like him and is harassing CALLER with that in their job responsibility.
12/29/13 10:42	Anonymous	3	HR Issue	Field Office 2	S. Brown	Caller states that PERSON INVOLVED 'JOHN' was making a mistake from another Field Office INVOLVED 'JACKSON' and the two men were making comments that hurt the feelings of several women, including WITNESS 'MELBA' and WITNESS 'TALY'.	
12/29/13 10:46	Carol Clark	2	HR Issue	Field Office 1	A. Johnson	Caller states that BOB 'JACKSON' was with her comments that she disagrees and needs to return.	
12/29/13 11:13	Anonymous	3	HR Issue	Field Office 2	S. Brown	Caller states that they are being denied work hours by BOB 'BROWN'.	
12/29/13 11:40	Anonymous	3	HR Issue	Field Office 2	S. Smith	Caller states that PERSON INVOLVED 'MELBA' has been making a lot of errors and leaving the building. CALLER and WITNESS 'SPENCER' have been instructed to manager 'BROWN' and nothing has been done.	
12/29/13 11:46	Anonymous	3	HR Issue	Home Office	S. Brown	Caller states that BOB 'SPENCER' is having an affair with PERSON INVOLVED 'CONNIE M.'. CALLER saw the two taking long lunches together, arriving and leaving in the same car and PERSON INVOLVED 'CONNIE M.' does not get in trouble for being late to work.	
12/29/13 12:03	Anonymous	2	Theft	Field Office 3	A. Johnson	Caller states that PERSON INVOLVED 'MELBA' was seen with the handling of a monetary PERSON INVOLVED 'MELBA'.	
12/29/13 12:16	Anonymous	1	Fraud	Home Office	C. Tompkins	Caller states that BOB 'BROWN' asked CALLER to make a journal entry without backup. CALLER fears that this was wrong and that BOB may have been trying to hide it from HR. CALLER cannot give anyone details because they are afraid to get in trouble. 'SPENCER' have been instructed to manager 'BROWN' and nothing has been done.	
12/29/13 12:22	Shari Hodge	3	HR Issue	Field Office 2	S. Brown	Caller states that their work hours were affected by not by PERSON INVOLVED 'BROWN'.	
12/29/13 12:42	Anonymous	3	Fraud	Field Office 3	S. Brown	Caller states that they were asked by BOB 'BROWN' to put false expenses on an expense report. CALLER said that the expense report was for a trip to another field office but CALLER was afraid to give other details.	
12/29/13 12:58	Anonymous	3	HR Issue	Field Office 1	S. Brown	Caller states that PERSON INVOLVED 'JOHN' was making the Field Office and was inappropriate through people's desks. CALLER saw PERSON INVOLVED 'JACKSON' get severe from a few desks in his workplace.	
12/29/13 1:03	Anonymous	3	HR Issue	Field Office 2	S. Smith	Caller states that PERSON INVOLVED 'CONNIE M.' was making the Field Office and was inappropriate through people's desks. CALLER saw PERSON INVOLVED 'JACKSON' get severe from a few desks in his workplace.	
12/29/13 1:03	Anonymous	3	Theft	Home Office	S. Brown	Caller states that PERSON INVOLVED 'BROWN' heard shouting people's names from the 3rd floor conference room and then went to it to stop.	

Screen shot No. 1

“The resources that the ACFE has provided to me to support education in fraud examination for college students over the past 10 years have been wonderful.”

**Heather S. Rogers, CPA**

ACFE Member Since 2003

*Associate Professor of Accounting*

*Chair, Department of Economics  
and Business*

*Whitworth University*

I work as a full-time professor at Whitworth University and also maintain a private CPA practice. The training and education I have gained as a member of the ACFE (both nationally and in my local Spokane, WA chapter) have provided me with essential tools needed to assist clients and law enforcement with issues related to fraud.



Learn more about how ACFE membership can help you in your career.

Visit [ACFE.com/member-benefits](https://www.acfe.com/member-benefits)

In fact, the tip files they analyze are so varied in format that Frishman has to analyze them with a data analysis software application. The aim is to illuminate inter-tip relationships that would otherwise escape the notice of investigators.

First, with the hotline manager's blessing, Kessler and Frishman assemble an electronic text file (screen shot No. 1 on page 34) of tip and complaint data from all available sources — for example, hotline and complaint databases, investigation case management tools, outside hotline and compliance systems, department spreadsheets and email or hard-copy messages to senior management.

Next, Frishman imports the text file into the software (screen shot No. 2 below) to normalize the raw data into a user-friendly format (screen shot No. 3 below) and give Frishman more flexibility and capability to work with the data than the hotline reporting systems do. This reveals previously unidentified commonalities (e.g., date, location or suspect's name) between tips. For example, using the software's analytical functions, she summarizes the data (screen shot No. 4 on page 37), revealing that of all the individuals named in the tip and complaint text file, only one — Jackson — has been involved in more than one incident.

Now investigators can focus more closely on all the data pertaining to the four incidents involving Jackson, and, if warranted, investigate further. Fully analyzed in this manner, large volumes of tips become the valuable informational asset they should be, rather than the cumbersome burden they have so often been in the past.

**CLOSER LOOKS**

While not analogous to hotlines — no tipster wants to be filmed delivering a fraud lead — massive video logs present an analytical challenge similar to that posed by large quantities of hotline transcripts. Each medium is a “haystack” that might contain hard-to-find, but informative, “needles.”

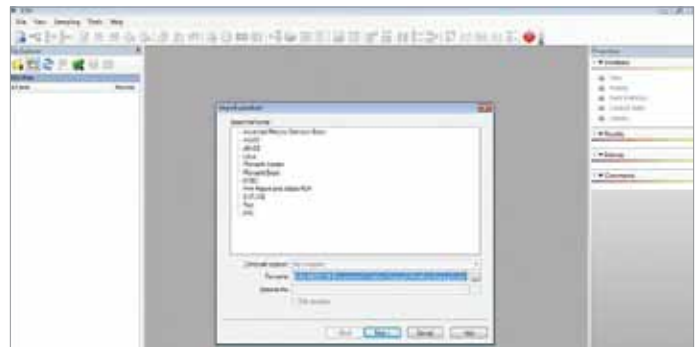
Over the last few decades, many organizations have created enormous libraries of digital and analog surveillance video. But

few have been willing to spend much time finding out whether they contained any useful evidence or intelligence. Stuck in illogical ruts, some companies simply record over earlier video without ever examining it. Often, when there is an urgent need to search a video log, the record has been overwritten.

For those organizations that have retained large libraries of security video, the cost of mining that data has most often exceeded its benefit. But recent technological advances have made it possible to search video quickly and efficiently.

BriefCam is a system that compresses video, intelligently eliminating hours of worthless static images so that an analyst can quickly find dynamic footage of significant events. The product proved its value at a 2010 security trade show in Dallas, Texas, where a night-shift cleaning crew stole an exhibitor's unsecured laptop. In the morning, exhibitor staff using BriefCam browsed an entire night's worth of security video in minutes, identifying the thieves and enabling police to quickly recover the laptop.

AISight software applies artificial intelligence (AI) algorithms to live video feeds, discerning suspicious activity “on the fly,” so that security breaches can be addressed as they take place. A fraud-related application might be detecting suspicious behavior at a secure location, such as a warehouse entry gate. While it is normal for a delivery vehicle to stop for clearance, it is not normal for someone to slip out of its passenger-side door



Screen shot No. 2

ID	DATE	TIMESTAMP	CALLER	SEVERITY	CATEGORY	LOCATION	INVESTIGATOR	DESCRIPTION
1	2/20/2011	08:34:00	Rick Howe	3	HR Issue	Home Office	B. Brown	Caller states that BOSS 'KIM' does not like them and is assignin
2	2/20/2011	19:52:00	Anonymous	3	HR Issue	Field Office 2	C. Diamond	Caller states that PERSON INVOLVED 'KING' was hosting a visit
3	2/21/2011	10:41:00	Carol Clark	2	HR Issue	Field Office 1	A. Johnson	Caller states that BOSS 'JACKSON' has made lewd comments t
4	3/23/2011	11:13:00	Anonymous	3	HR Issue	Field Office 1	R. Dewey	Caller states that they are being denied work hours by BOSS 'U
5	3/23/2011	21:02:00	Anonymous	3	HR Issue	Field Office 2	S. Smith	Caller states that PERSON INVOLVED 'NEWMAN' has been taki
6	3/23/2011	08:46:00	Anonymous	3	HR Issue	Home Office	B. Brown	Caller states that BOSS 'MCFADDEN' is having an affair with PE
7	3/23/2011	15:23:00	Anonymous	2	Theft	Field Office 1	A. Johnson	Caller states that PERSON INVOLVED 'WHITE' was seen with th
8	3/24/2011	14:16:00	Anonymous	1	Fraud	Home Office	E. Trembly	Caller states that BOSS 'UNKNOWN' asked CALLER to make a j
9	4/18/2011	12:22:00	Sean Mobly	3	HR Issue	Field Office 2	C. Diamond	Caller states that their work hours were unfairly cut by PERSON
10	4/26/2011	16:12:00	Anonymous	2	Fraud	Field Office 1	G. Minick	Caller states that they were asked by BOSS 'UNKNOWN' to put
11	5/17/2011	12:16:00	Anonymous	3	HR Issue	Field Office 1	R. Dewey	Caller states that PERSON INVOLVED 'LISA' has offensive body
12	6/3/2011	08:38:00	Anonymous	3	HR Issue	Field Office 2	S. Smith	Caller states that PERSON INVOLVED 'JACKSON' was visiting th
13	6/15/2011	15:21:00	Anonymous	3	Theft	Home Office	B. Brown	Caller states that PERSON INVOLVED 'UNKNOWN' keeps stealin

Screen shot No. 3

while the guard is focused on the driver. AISight can recognize such potentially fraudulent activity and alert security personnel without human assistance.

Once an organization achieves such insights, the challenge is to maximize their usefulness. Derek Brink, a vice president in the Aberdeen Group, a market research consultancy in Boston, Mass., authored a 2010 white paper, “The Eyes Have IT.” Brink observed that most companies that excel in video analytics share certain best practices, including:

- Systematic collection, normalization and correlation of video data.
- Standardized audit, analysis and reporting on video data.
- Communication of video-tracked events and resolutions to key stakeholders.

Each of these data analysis and utilization practices would also serve hotline managers well, which supports the notion that the right anti-fraud techniques can be effective in more than one arena.

#### MUST-HAVE: AN INTEGRATED HOTLINE SYSTEM

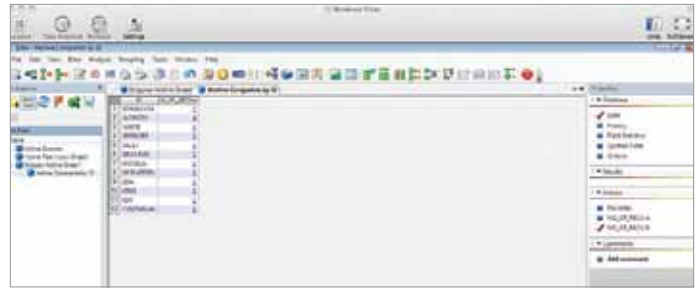
It has always been a good idea for organizations to give their employees and other stakeholders a way to safely report potential fraud to management. On Aug. 12, 2011, it became an even better idea. That day the Securities and Exchange Commission (SEC) issued a final rule implementing whistleblower provisions the Dodd-Frank Wall Street Reform and Consumer Protection Act had added to the Securities Exchange Act of 1934. Under those provisions, retaliation against whistleblowers is prohibited and heavily penalized and large bounties are potentially available for reporting securities fraud to the SEC. Based on past experience and increased volume since the passage of Dodd-Frank, the SEC expects to receive approximately 30,000 tips, complaints and referral submissions each year.

To manage these reports, the SEC has launched a new Tips, Complaints and Referrals Portal (<https://denebleo.sec.gov/TCRExternal/disclaimer.xhtml>). Thousands of SEC employees have access to information already in the portal’s database and can add more. It remains to be seen how effective the new system is and whether the SEC has enough investigators to deal with the tip avalanche it anticipates.

However, the SEC’s system is not the only one under pressure to perform. Tipsters can be eligible for a bounty even if they give a lead to the SEC instead of doing so internally. Thus, companies that employ such whistleblowers might suffer greater harm from fraud charges — true or not — than ever before.

For example, if a tip given to the SEC but not to the company turns out to be false, the company still might incur legal expenses greater than it would have if the whistleblower had had enough confidence in the company’s ethical culture and hotline system to first submit the tip internally.

Alternatively, if a tip given to the SEC but not to the company is well-founded, the company will not only bear great legal expenses associated with the confirmed fraud. It also might face higher penalties because of its possible failure to comply with the



Screen shot No. 4

U.S. Sentencing Guidelines mandate (in section 8B2.1) to “have and publicize a system, which may include mechanisms that allow for anonymity or confidentiality, whereby the organization’s employees and agents may report or seek guidance regarding potential or actual criminal conduct without fear of retribution.”

The SEC’s whistleblower program will have the greatest impact on public companies, which issue securities and thus are exposed to the kinds of fraud that fall within the SEC’s jurisdiction. But because the SEC regards anyone working for a private subsidiary or affiliate of a public company as a potential securities fraud whistleblower, those employees too might be tempted to tip off the SEC before reporting fraud internally. And that would expose those nonpublic companies to the same disadvantages as public companies whose ethics and compliance programs — and hotline systems — do not inspire employee confidence or trust.

Interestingly, the 2010 ACFE Report to the Nations said (on p. 18) that among the 1,843 cases it analyzed, “privately owned companies tended to have the fewest frauds detected by tip and the most frauds caught by accident, both of which were also true” in [the 2008 ACFE] Report. The 2010 Report added (on p. 42) that “Hotlines were the control with the greatest associated reduction in median loss, reinforcing their value as an effective anti-fraud measure.”

The Ethics Resource Center’s latest National Business Ethics Survey, released in 2009, reported (p. 30) that nearly 15 percent of U.S. workers observed some “red flag” behavior during the survey period. Yet 30 percent of those employees said they did not report their observations. Furthermore, hotlines were the least frequently used reporting channel in 2009 (p. 35); only 3 percent of reports were made by hotline.

These striking considerations and findings persuasively indicate that most organizations would benefit from having a well-integrated hotline system. Of course, once a tipster has reported a fraud internally, it is up to the employer to develop that information to its fullest practical value. To investigators, few things are more tragic than an important tip whose crucial relationship to another lead goes unrecognized, hindering insight and allowing a fraud to continue while losses mount. And yet it happens. 🔍

---

**Robert Tie** is a New York business writer. His email address is: [bob@robertie.com](mailto:bob@robertie.com).

---