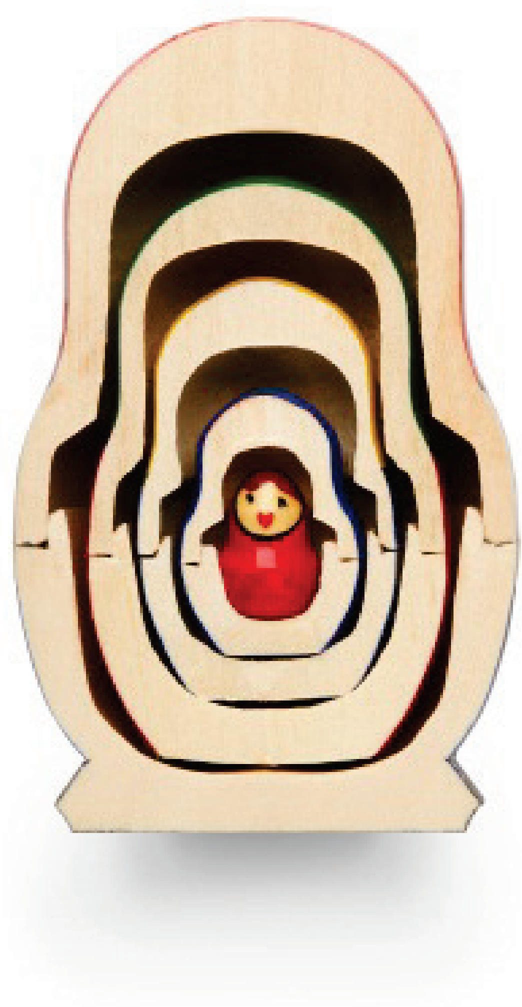
Shrinking retail shrink

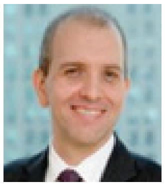
Using analytics to help detect fraud and grow margins



Deloitte Forensic Center

Contents

Authors



Darren James is a partner in the Deloitte member firm in Canada, Deloitte & Touche LLP ("Deloitte Canada"), with over 20 years of experience in the areas of risk and control, audit, data analytics and fraud detection. His focus is the use of data analytics to detect data and transactional integrity issues. Darren is a Certified Information Systems Auditor (CISA) and has managed and delivered many engagements involving the assessment of risk and evaluation of controls across a broad range of IT environments. Darren may be reached at **djames@deloitte.ca** or +1 416 601 6567.

Robert Fowlie is a partner in the Forensic practice of Deloitte Canada. He has more than 20 years of experience providing investigative and forensic accounting services. He has conducted investigations in many jurisdictions including Canada, the United States, Mexico, England, Japan and Colombia. He is a Chartered Accountant, a specialist in investigative & forensic accounting (IFA) and has testified as an expert witness in fraud and damages matters. Rob may be reached at **rfowlie@deloitte.ca** or +1 416 601 6451.

Chantal Hicks is a senior manager and retail industry specialist in the Enterprise Risk Services practice of Deloitte Canada. She is a Chartered Accountant and Certified Information Systems Auditor (CISA) with more than 14 years of experience providing enterprise risk management, internal audit, IT audit and governance services to retail clients. Chantal may be reached at **chicks@deloitte.ca** or +1 416 601 5951.

Kim MacDonald is a senior manager with 15 years public accounting experience serving public companies in the consumer business, manufacturing and distribution industries. She is also the Retail Sector specialist in the Assurance and Advisory practice of Deloitte Canada. In this role she provides industry insights and trends to our clients and our client service teams. Kim may be reached at **kimmacdonald@deloitte.ca** or +1 416 643 8413.

The authors gratefully acknowledge the assistance provided by colleagues Scott Foster, Justin Medakiewicz and Mike Murney in preparing this article.

Editor

Toby Bishop is the director of the Deloitte Forensic Center for Deloitte Financial Advisory Services LLP. He is co-author of the book *Corporate Resiliency: Managing the Growing Risk of Fraud and Corruption* and a related article in Harvard Business Review. He is a member of the Board of Editors of Business Crimes Bulletin, the Center for Audit Quality's Anti-Fraud Working Group, the Committee of Research and Education Advisors for the Institute of Internal Auditors, and the Advisory Council of the Association of Certified Fraud Examiners. Toby may be reached at **tobybishop@deloitte.com** or +1 312 486 5636.

Deloitte Forensic Center

The Deloitte Forensic Center is a think tank aimed at exploring new approaches for mitigating the costs, risks and effects of fraud, corruption, and other issues facing the global business community. The Center aims to advance the state of thinking in areas such as fraud and corruption by exploring issues from the perspective of forensic accountants, corporate leaders, and other professionals involved in forensic matters. The Deloitte Forensic Center is sponsored by Deloitte Financial Advisory Services LLP.

Retail fraud up, detection down?

Global retail shrinkage increased 6.6 percent to U.S. $119 billion in 2011, an average of 1.45 percent of retail sales.[1]

In some companies, fraud remains a big concern for senior executives. But with economic conditions weak in many parts of the world, other pressing issues may have edged fraud management to the side. Many companies are working overtime just to sustain their competitive position in the current market environment. This may be one reason why, according to the Centre for Retail Research, global inventory shrinkage increased 6.6 percent for the year ended June 2011 to more than U.S. $119 billion, representing 1.45 percent of global retail sales at retail sales value.[2]

By way of comparison, this study reported a shrinkage rate for the U.S. of 1.59 percent, somewhat higher than the 1.42 percent for calendar year 2011 stated in the final report of the longer-running [U.S.] National Retail Security Survey.[3] The difference in shrinkage rates reported by the two studies is less important than the potential opportunity for loss reduction and margin improvement.

Fraudsters are perpetually seeking new ways to steal from retailers or to take greater advantage of existing weaknesses. Fraud methods in new and established areas, such as organized retail crime (ORC), point-of-sale (POS) manipulation, refund fraud, employee and customer theft, credit card fraud, fraudulent transactions over mobile devices and vendor fraud have all evolved over the past decade, adapting to new retail technology and changes in fraud prevention measures. The Centre for Retail Research reported that 47.5 percent of retailers globally reported increased ORC losses for the year ended June 2011, 35.9 percent reported increased actual or attempted shoplifting and 24 percent reported increased employee theft.[4]

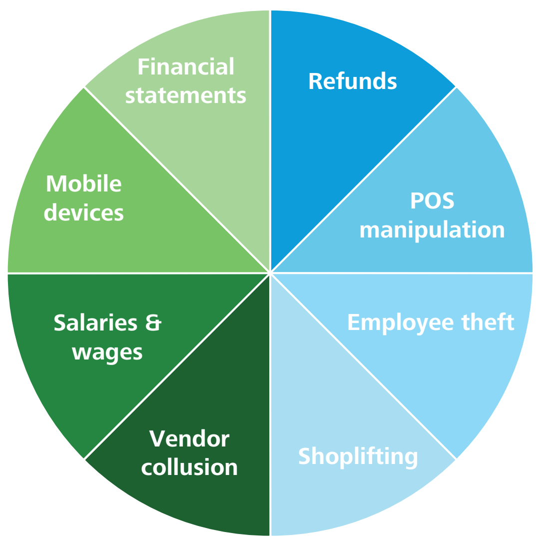
In the retail industry at least, implementation of innovations in fraud prevention may have slowed just as criminal activity and innovations in committing fraud speeded up. The 2012 Lexis-Nexis True Cost of Fraud Report indicated that merchants prevented fewer fraudulent transactions in 2012 than in 2011, both in absolute numbers and relative to the number of successful fraudulent transactions detected.[5]

Retailers will likely have to step up the pace of innovation in their fraud prevention and detection activities if they are to recover more of the margin currently being lost to fraudsters. It is time for the retail industry to consider how new technologies such as data analytics may help to detect more fraud and improve margins in an increasingly challenging economic environment.

Is it time to update your strategy for fraud?

Traditionally, retailers have focused on implementing manual control activities to help mitigate potential losses from different types of fraud in the retail industry (See Figure 1). Some retailers have a small, dedicated team of loss prevention specialists to oversee their fraud-related activities and to create awareness around the company. Some of these existing fraud activities are outdated and proving insufficiently effective for many global retailers.

Figure 1: Some types of retail fraud



While designing and implementing strong internal controls around key risk areas is an important part of fraud management, it may not be enough to recover more of the margin currently being lost to fraud. The limitations of traditional fraud prevention activities include:

Resource constraints and inefficiencies

The resources to prevent and detect fraud are often limited and concentrated on traditional activities. But are internal audits and other traditional detection techniques, used for the sake of simplicity and economy, really that effective?

When a retailer has many locations, selecting the ones to be inspected or audited has often been a matter of experience, but staff reductions often lead to a loss of personnel with that experience. New analytics technology can not only flag for investigation locations with greater anomalies but also can learn from its experience and retain that knowledge.

Outdated technologies and limited data analytics

In this age of technology, retailers appear to be playing catch-up. According to the Global Retail Theft Barometer 2011 survey, 55 percent of retailers increased their spending on crime prevention hardware and software in 2011 and 35 percent planned further additions.[6] Aside from the large number of retailers apparently not adding new technology, a key question is whether retailers are taking advantage of the data that is already being collected or could be collected using new technology, such as video and text mining, to help prevent losses due to fraud.

The 2011 [U.S.] National Retail Security Survey reports that only 19.8 percent of respondents use Internet protocol (IP) analytics–just half of the 39.6 percent who have implemented remote IP closed circuit television systems. Also, while 67.3 percent of respondents have implemented point-of-sale (POS) data mining software, that still leaves many retailers without this valuable tool and it raises a question of how effectively the POS tool is being used.[7]

One fraudster famously deprived retailers of more than U.S. $600,000 over a three-year period by placing counterfeit bar codes on high-end toys, greatly reducing their price. He would then sell the items online for nearly full value. After monitoring sales reports for trends and anomalies, one retailer's loss investigators caught the man—but it took three years.[8]

Basic POS analytics only take you so far. By incorporating predictive analytics, such as the anticipated sales volume of a given stock keeping unit (SKU) and anticipated sales of products in the secondary marketplace, retailers could have a greater chance to identify certain product sales as outliers and alert stores to increase their scrutiny of such sales.

Inadequate control activities

Internal thefts also pervade the retail industry. Some of the most significant frauds are committed by employees who hold high positions. These employees can override some internal controls to achieve their goals.

A commissioned employee can abuse her power by selling below the company's discount limit to reach her personal sales quota. And franchise owners may be tempted to underreport sales or buy supplies from someone other than the franchisor in order to reduce franchise fees and procurement costs.

No system of controls is perfect, but data analytics can provide a new level of transparency and insight that can be a powerful tool for detecting, and deterring, overrides of internal controls and exploitation of control weaknesses.

Oversight and lack of continuous monitoring

Traditional fraud prevention techniques tend to be historical rather than predictive - oversight is often labor intensive and overstretched. In contrast, the credit card industry uses real-time alerts to flag many unusual customer transactions, triggering a hold on the transaction and avoiding a loss. Human intervention can be focused on high value transactions and those requiring more sensitive handling, such as those involving highly profitable customers.

Although 96.5 percent of U.S. retailers report experiencing the return of stolen merchandise and 80.7 percent report employee return fraud or collusion with external sources[9], the retail industry has fallen behind in implementing continuous monitoring techniques. Many retail companies have a significant amount of data at their disposal, captured daily through operations. But turning that data into insight, through continuous monitoring and real-time feedback, remains a challenge.

Building more effective fraud risk management

Today's business landscape is evolving, and fraudulent techniques are evolving with it. Retailers can benefit from implementing a holistic fraud framework (see Figure 2), continuously innovating in fraud management strategies. Rather than simply augmenting traditional activities, this model takes a fresh approach to improving retailers' ability to prevent and detect fraud.

Figure 2: A holistic fraud framework

This framework contains four key components:

Cultural assessment

The first step is to assess your company's culture; specifically its business ethics and actions. You can gather anonymous feedback from a large group of people simultaneously using an established web-enabled survey tool. Such an assessment can give you valuable insights into your ethical culture and help to quantify the internal impact of your fraud and ethical risk management activities.

A survey may include six principal areas:

1. Awareness of relevant policies and follow-through
2. Corporate culture
3. Observed unethical or questionable actions
4. Issues that either facilitate or reduce the likelihood of fraud occurring
5. Respondents' perceptions of the desired outcomes of ethics and compliance efforts
6. Specific risk issues

Such a survey not only provides critical insights but also the process of sending the survey to staff and management also has the benefit of raising the profile of ethics and integrity risk.

By evaluating the results of the survey, companies can better identify areas of fraud risk using objective data rather than the potential biases and misinformation of decision-makers. This insight can help you focus your fraud management efforts and apply data analytics to key areas.

Technology and data analytics

Often simple rules-based solutions, such as real-time POS transactional monitoring, may not be enough for many companies to achieve their fraud risk management goals. Knowing the specific fraud-related issues in your company can help you focus your efforts and implement a tailored technology solution.

You may be able to discover your specific areas of exposure by leveraging the rich data environment common in retail companies. This includes data from daily transactions and activities such as purchasing, accounts payable, POS, sales projections, warehouse movements, employee shift records, returns and store-level video and audio recordings. Rigorous and regular sample-based analysis of data across your company can help you to:

- Identify fraudulent activity
- Develop appropriate priorities for case management and investigation
- Reduce the false positive rate of your detection and prevention strategy.

For example, a fast food franchisor that suspects franchisees of underreporting, rather than carrying out random audits, could identify high-risk franchisees through analytics. By combining external data such as population base served and proximity to competitors, it could create a predictive model with the expected reporting figures for each franchisee. The franchisees whose reported figures vary most from expected figures could then be the focus of internal auditing efforts. By focusing on high-risk areas, staff can enhance efficiency and create more value.

Some companies carry out this analysis in-house, while others team with companies that have worked with multiple vendors in the retail market. Engaging an experienced service provider can provide the knowledge and experience you need to decide, for example, whether to enhance and fine tune your current system or select and implement new technologies and data analysis tools.

Effective control activities

Many companies begin to build control frameworks and processes after a large and public fraud has caused significant negative financial and non-financial damage. But even companies with established control activities can benefit from reviewing the existing environment and processes, and helping to ensure they are supported with leading edge innovation. Preventing a critically damaging event before it occurs by mitigating the risk of fraud is far preferable to scrambling to react and reduce losses.

One way of evaluating your control environment is a series of facilitated stakeholder workshops, which can help you to:

- Assess the likelihood and potential impact of different types of fraud in your business
- Assess the ability of your current control environment to mitigate these risks adequately
- Identify limitations in your control environment, such as potential management override.

With franchisee under-reporting, fraudsters can manually circumvent the traditional control of the POS system by taking cash and not entering the sale in the system. Analytics-based control activities can quickly help to identify and mitigate this kind of fraud by comparing expected to reported sales and flagging unusual reporting patterns.

Continuous monitoring and innovation

Fraudulent individuals continuously monitor and adjust their activities to try to circumvent your fraud prevention and detection activities. If you want to fight fraud, your company needs to do the same. When you know what fraudsters are up to, you are better able to react quickly and help save your company significant sums of money.

Continuous monitoring can include:

- Watching product and inventory movement for unusual patterns that may indicate shrink and store associate theft before it becomes significant
- Monitoring exceptions and trends, such as the number of invoices from suppliers over time, unusual invoice number sequencing, and the amount of money spent for goods and services purchased from a particular vendor, to alert management when unusual items are being processed before the assets leave
- Building a model for a predicted number of product returns per shift; when numbers exceed a set threshold for returns by product or by individual, manager verification can be invoked.

By continuously monitoring for potential fraudulent activities, a manager's time can be better focused on areas of concern and fraud management can become proactive rather than reactive, helping retailers to reduce losses and improve margins.

Conclusion and recommended actions

Staying one step ahead of the fraudsters is the key to protecting your company's hard-earned assets and reputation. Implementing data analytics into all elements of your fraud framework can help you find patterns, trends and anomalies in your data. It can help you to detect a broader range of exposure, including previously unknown risks, and uncover new patterns of fraud.

Actions we recommend

Our recommendations to specific clients will depend upon their fraud risk profile and the current state of their controls and their use of data analytics. Some actions to help you consider your own situation are:

1. Read your company's fraud risk assessment and ask yourself whether it effectively identifies the different and evolving fraud and theft scenarios your company faces today. If it is outdated, get it refreshed. If you don't have a fraud risk assessment, it would be wise to prepare one. A suitably experienced professional advisor can help you with good practices for developing one.

2. Consider the manual and technology controls implemented in your company to mitigate the risk of fraud and theft and ask yourself these questions: Do the controls as designed reduce the risk of fraud and theft to a level the board of directors or others charged with governance consider acceptable? Do weaknesses require controls to be enhanced for specific fraud scenarios? Does testing indicate the controls work as intended throughout the enterprise?

3. Evaluate the data analytics technology used by your company to prevent and detect retail fraud and theft and ask yourself these questions: Is it achieving the results we want? Does it leverage the data collected by the company? Do employees know how to use the technology effectively? Does it proactively or predictively detect trends meriting further investigation?

Data analytics can be a powerful tool to accelerate retailers' efforts to get ahead of shrink. With retail margins under pressure, data analytics provide an attractive new opportunity for shrinking shrink and growing the bottom line. Are you taking full advantage of that opportunity?

Deloitte Forensic Center

This article is published as part of ***ForThoughts***, the Deloitte Forensic Center's newsletter series edited by Toby Bishop, the director of the Deloitte Forensic Center and a director of Deloitte Financial Advisory Services LLP. ***ForThoughts*** highlights trends and issues in fraud, corruption and other complex business issues.

To subscribe to ***ForThoughts***, or for more information, visit **www.deloitte.com/forensiccenter**, scan the code below, or send an email to **dfc@deloitte.com**.

Endnotes

1. Centre for Retail Research *The Global Retail Theft Barometer 2011,* (Checkpoint Systems, Inc., 2011). Retrieved from **http://www.retailresearch.org/grtb_currentsurvey.php.** Survey data for the 12-month period ending in June 2011 was provided by 1,187 retail corporations around the world, with a combined total of 251,895 stores and sales of U.S. $986 billion.

2. Centre for Retail Research *The Global Retail Theft Barometer 2011*

3. University of Florida 2011 National Retail Security Survey Final Report. Retrieved from **http://soccrim.clas.ufl.edu/files/nrssfinalreport2011.pdf.** Survey data for the calendar year 2011 was provided online by 101 corporate retail chains in the U.S.

4. Centre for Retail Research *The Global Retail Theft Barometer 2011*

5. LexisNexis *2012 True Cost of Fraud.* Retrieved from **http://solutions.lexisnexis.com/forms/CE12Retail2012TRueCostofFr10206.** Survey data cited was provided online by a merchant panel of 1,030 risk and fraud decision-makers and influencers in the U.S. in a survey commissioned in May 2012 from Javelin Strategy & Research.

6. Centre for Retail Research *The Global Retail Theft Barometer 2011*

7. University of Florida *2011 National Retail Security Survey Final Report*

8. Zimmerman, Ann. "As Shoplifters Use High-Tech Scams, Retail Losses Rise." Wall Street Journal Online October 25, 2006. Retrieved from **http://people.ischool.berkeley.edu/~hal/Courses/StratTech09/Lectures/Transactions/Articles/shoplifters.html**

9. National Retail Federation *Return Fraud Survey 2012*. Survey data was provided by 60 U.S. retail participants in November 2012. Retrieved from **http://www.nrf.com/modules.php?name=News&op=viewlive&sp_id=1472**

Deloitte Forensic Center

The following material is available on the Deloitte Forensic Center website **www.deloitte.com/forensiccenter** or from **dfc@deloitte.com.**

Deloitte Forensic Center book

- Corporate Resiliency: Managing the Growing Risk of Fraud and Corruption
  - Chapter 1 available for download

ForThoughts newsletters

- New FCPA Resource Guide: Ten things for legal and compliance officers to consider
- The Internal Audit Fraud Challenge
- Look Before You Leap: Navigating Risks in Emerging Markets
- Reducing Claims Fraud: A Cross-industry Issue
- Growth Strategy and M&A: Environmental Issues Impacting Strategic Decisions
- International Business Partner Due Diligence: How Much is Enough?
- Internal Investigation Costs: Securing Elusive Insurance Coverage
- The Tone at the Top: Ten Ways to Measure Effectiveness
- Visual Analytics: Revealing Corruption, Fraud, Waste and Abuse
- Anti-Corruption Practices Survey 2011: Cloudy with a Chance of Prosecution?
- Fraud, Bribery and Corruption: Protecting Reputation and Value
- Ten Things to Improve Your Next Internal Investigation: Investigators Share Experiences
- Sustainability Reporting: Managing Risks and Opportunities
- The Inside Story: The Changing Role of Internal Audit in Dealing with Financial Fraud
- Major Embezzlements: How Can they Get So Big?
- Whistleblowing and the New Race to Report: The Impact of the Dodd-Frank Act and 2010's Changes to the U.S. Federal Sentencing Guidelines
- Technology Fraud: The Lure of Private Companies
- E-discovery: Mitigating Risk Through Better Communication
- White-Collar Crime: Preparing for Enhanced Enforcement
- The Cost of Fraud: Strategies for Managing a Growing Expense
- Compliance and Integrity Risk: Getting M&A Pricing Right
- Procurement Fraud and Corruption: Sourcing from Asia
- Ten Things about Financial Statement Fraud - Third edition
- The Expanded False Claims Act: FERA Creates New Risks
- Avoiding Fraud: It's Not Always Easy Being Green
- Foreign Corrupt Practices Act (FCPA) Due Diligence in M&A
- The Fraud Enforcement and Recovery Act "FERA"
- Ten Things About Bankruptcy and Fraud
- Applying Six Degrees of Separation to Preventing Fraud
- India and the FCPA
- Helping to Prevent University Fraud
- Avoiding FCPA Risk While Doing Business in China
- The Shifting Landscape of Health Care Fraud and Regulatory Compliance
- Some of the Leading Practices in FCPA Compliance
- Monitoring Hospital-Physician Contractual Arrangements to Comply with Changing Regulations
- Managing Fraud Risk: Being Prepared
- Ten Things about Fraud Control

Deloitte Forensic Center

Notable material in other publications

- You've Discovered a Fraud…Now What?, *White Collar Crime Fighter*, March 2013
- FCPA Resource Guide: 10 Issues to Consider, *WSJ Professional,* February 2013
- Reducing Fraudulent Claims and Their Costs, WSJ Professional, October 2012
- Ten Year Anniversary of Sarbanes/Oxley, *Professional Liability Underwriting Society*, September 2012
- Current Developments in Fraud and Corruption, *Institute of Internal Auditors AuditChannel.tv*, August 2012
- Whistleblowing After Dodd-Frank: New Risks, New Responses, in *Corporate Crime, Fraud and Investigations Guide*, Practical Law Company, July 2012
- Third Parties: The Achilles' Heel of FCPA Compliance, Business Crimes Bulletin, July 2012
- Sarbanes-Oxley: A Decade Later, Financial Executive, July 2012
- Ten Ways to Measure the Tone at the Top, Corporate Compliance Insights, May 2012
- Incorporating Environmental Issues' Impact into Strategic Decision and M&A, WSJ Professional, May 2012
- Seven Ways to Reduce Embezzlement Risk, Employment Alert, May 2012
- How to Perform Due Diligence on International Business Partners, WSJ Professional, April 2012
- More Clues on SEC Whistleblower Office, Compliance Week, February 2012
- Anti-Corruption Practices Survey Highlights Challenges Facing Companies, Business Crimes Bulletin,
  January 2012
- Execs Not Confident In Corporate Anti-Corruption Programs, FinancialFraudLaw.com, January 2012
- 10 Ways to Measure the Tone at the Top, WSJ Professional, January 2012
- So You Want to be a Multinational?, ChiefExecutive.net, December 2011
- Execs Lack Confidence in Anti-Graft Programs, Compliance Reporter, November 2011
- Bounty Hunting: Will New Regulations Create a New Incentive for Whistleblowers?, Perspectives (University of Illinois), November 2011
- The Hidden Risks of Doing Business in Brazil, Agenda, October 2011
- Use of Third Parties' Seen as Leading Source of Corruption Risk, Ethikos, Sept/Oct 2011
- Smaller Companies Lag Behind in Anti-Corruption Programs Despite Escalating Enforcement Activity, EmploymentLawDaily.com, September 2011
- High Tide: From Paying For Transparency To 'I Did Not Pay A Bribe', WSJ.com, September 2011
- Executives Worry About Corruption Risks: Survey, Reuters, September 2011
- Whistleblowing After Dodd-Frank — Timely Actions for Compliance Executives to Consider, Corporate Compliance Insights, September 2011
- Corporate Criminals Face Tougher Penalties, Inside Counsel, August 2011
- Follow the Money: Worldcom to 'Whitey,' CFOworld, July 2011
- Whistleblower Rules Could Set Off a Rash of Internal Investigations, Compliance Week, June 2011
- Whistleblowing After Dodd-Frank: New Risks, New Responses, WSJ Professional, May 2011
- The Government Will Pay You Big Bucks to Find the Next Madoff, Forbes.com, May 2011
- Major Embezzlements: When Minor Risks Become Strategic Threats, Business Crimes Bulletin, May 2011
- As Bulging Client Data Heads for the Cloud, Law Firms Ready for a Storm, and More Discovery Woes from Web 2.0, ABA Journal, April 2011
- The Dodd-Frank Act's Robust Whistleblowing Incentives, Forbes.com, April 2011
- Where There's Smoke, There's Fraud, CFO magazine, March 2011
- Will New Regulations Deter Corporate Fraud? Financial Executive, January 2011
- The Countdown to a Whistleblower Bounty Begins, Compliance Week, November 2010
- Deploying Countermeasures to the SEC's Dodd-Frank Whistleblower Awards, Business Crimes Bulletin, October 2010
- Temptation to Defraud, Internal Auditor magazine, October 2010
- Shop Talk: Compliance Risks in New Data Technologies, Compliance Week, July 2010
- Many Companies Ill-Equipped to Handle Social Media e-discovery, BoardMember.com, June 2010
- Mapping Your Fraud Risks, Harvard Business Review, October 2009
- Use Heat Maps to Expose Rare but Dangerous Frauds, HBR NOW, June 2009