

LEGAL & REGULATORY



ECONOMIC DOWNTURN BRINGS A RETURN TO 'CLASSIC FRAUD'



REPRINTED FROM:
JULY 2010 ISSUE

© 2010 Financier Worldwide Limited.
Permission to use this reprint has been granted by the publisher.

www.financierworldwide.com



LEGAL & REGULATORY

WHITE-COLLAR CRIME

Economic downturn brings a return to ‘classic fraud’ | BY DAVID GANNAWAY

The mid-2000s financial bubble has run its course. Enron and MCI/Worldcom are history, Bernard Madoff has been sentenced, other major frauds have been exposed, and the world has moved from irrational exuberance to a new challenge: coping with the effects of what might become a prolonged downturn.

Does that mean that fraud is no longer a pressing issue? Sadly, the opposite is true. Fraud has always been part of the business landscape, and probably always will be. Businesses need to remain vigilant for signs of fraud, and know when to turn to professionals who can conduct assessments, lead investigations, and work with executives and regulators once it has been determined that a fraud has occurred.

What kinds of fraud should businesses watch for? The pattern of fraud in a downturn is different from the pattern of fraud at the height of a bubble. In a bubble, dramatic Ponzi schemes like Madoff’s are widespread as exuberant investors try to better their already improbably high returns. Ponzi schemes are then exposed when the bubble bursts and investors demand the return of their nonexistent funds. Bubbles also produce the kind of accounting fraud typified by Enron, in which companies falsify their books in order to pump their earnings.

In a prolonged downturn, the pattern of fraud is different and more mundane, but no less costly. Ponzi schemes and other investment-related frauds diminish (though they never disappear entirely). This reduction serves to expose an ongoing level of classic or perennial fraud: misappropriations such as embezzlement, in which employees who are under personal financial pressure take cash or other assets. There is also an uptick in other forms of theft – of the employer’s intellectual property and of confidential financial information that will be used for the employee’s personal gain. The explanation is simple. Employees are under financial pressure. They have lost hours or benefits, and their spouses have lost jobs. They have a strong incentive to try to make up their losses by taking readily available cash and other assets.

Statistics bear this out. According to the Association of Certified Fraud Examiners 2002 Report to the Nation: ‘Occupational Fraud and Abuse,’ the cost of fraud for 2002 – the year of the last major economic downturn – was projected at \$600bn, or 6 percent of revenues based on

US Gross Domestic Product (GDP). That’s six cents on every dollar a business took in. Over 85 percent of these frauds involved asset misappropriation, according to the report. In the Association’s 2008 report, detailing activity from 2006–2008 (that is, at the height of the bubble), asset misappropriation fraud was even more common. It accounted for 88.7 percent of 2008 cases (a figure that was still off slightly from its 2006 high of 91.5 percent). But it didn’t get as much attention because corruption (such as bribery) and financial statement fraud had surged. Overall, though, fraud had escalated – in 2008, it was projected at 7 cents per dollar of revenue, or \$994bn.

In the face of these levels of fraud, what are executives to do? The first step is to recognise that fraud is common. The second is to understand its impact on the bottom line. At a time when businesses are trying to cut costs in every way possible – cutting employees, cutting hours, cutting benefits – undetected fraud represents massive additional costs. Assets disappear readily. In over 25 percent of 2008 cases, the cost of each fraud was over \$1m. In another 28 percent of cases, it ranged from \$100,000 to \$500,000. Many of these losses – especially in the \$100,000 to \$500,000 tier – were for very basic crimes: billing fraud (creating false vendors, submitting personal invoices for payment) accounted for nearly a quarter of cases. Close behind were cheque tampering (taking blank cheques, or diverting cheques to a personal account) and skimming (accepting payments from a customer and not reporting them), as well as noncash theft (of inventory). Asset misappropriation takes place whenever assets are readily available and controls are relatively loose.

Recognising the risks and the stakes, the next move for business leaders is to perform a fraud risk assessment. The key components of the assessment are Assess, Design, Detect, Evaluate and Respond: (i) Assess – review current internal controls and rank the potential vulnerabilities to fraud; (ii) Design – remove temptation by taking a risk-based approach to minimising the opportunity for fraud to occur; (iii) Detect – identify possible fraud when it happens; (iv) Evaluate – re-visit the changes made to re-assess effectiveness; and (v) Respond – take corrective action to strengthen internal controls to reduce the opportunity ▶▶

for fraud or investigate any fraudulent activity discovered.

A fraud risk assessment is critical. While conducting investigations is a job for experienced outside professionals, fraud prevention begins with the executive team – as it should, recognising the enormous impact of fraud on revenue. Management should evaluate risk areas across the entire organisation and obtain input from process owners in order to assess opportunities for fraud and weaknesses in internal controls.

Prevention can be enhanced through stricter due diligence or control procedures. It is also a matter for ‘tone at the top’. Creating a code of conduct that defines acceptable business practices, then conducting annual (or more frequent) staff training sessions can go a long way toward creating a low-tolerance atmosphere, and keeping borderline fraudsters from acting on their impulses.

The discovery of a suspected fraud is the time to turn to the outside for help. Actually, there is a case to be made for calling on outside assistance even earlier. Control procedures should be developed or at minimum tested by fraud experts – attorneys, investigators and forensic

accountants.

Once a fraud is detected, the assistance of an experienced fraud investigator is essential. He or she can conduct the investigation in concert with the general counsel or outside attorneys, and work with regulators and the executive team to see the investigation through to its conclusions.

But the most important lesson is this: while the dramatic frauds of the bubble years may be a thing of the past, fraud is still with us – it always has been and it always will be. Old-style misappropriation fraud (involving employees who simply take assets) continued through the boom years, and may even be on the increase now that the downturn has employees feeling financial pressure. Businesses are under financial pressure as well, and that is reason enough to work hard to stop the very significant losses that fraud creates. By remaining vigilant, improving communications and controls, and turning to outside experts to manage investigations, business leaders can protect themselves and their investors. They can survive the downturn in much healthier shape by acting now to keep fraud firmly in check. ■



David Gannaway, MBA, CFE, CAMS, EA is a director at Marks Paneth & Shron LLP. He can be contacted on +1 (212) 710 6206 or by email: dgannaway@markspaneth.com.

David Gannaway is a former special agent with the Criminal Investigation Division of the Internal Revenue Service (IRS), he brings a deep understanding of the rigors of the investigative process to his role. He focuses on tax controversy and white-collar crime and is also experienced in providing comprehensive litigation consulting services in the areas of forensic accounting, healthcare fraud and money laundering.