



EXCERPTS OF RECENT MEDIA COVERAGE

FORENSICS

A SAMPLING OF BDO THOUGHT LEADERSHIP IN THE MEDIA FOR Q2 2016

LAW360

THE MANY USES OF SHELL COMPANIES

By [Glenn Pomerantz](#) and [Brian Mich](#)

Most of the publicity surrounding the Panama Papers has focused on the important role that the use of shell companies has played in the laundering of the proceeds of criminal activity and in tax evasion. But there are many other ways individuals and organizations can use shell companies, and not all of them are illegal...

Circumvention of Export Controls...

Offshore shell companies may be set up to serve as a third-party mechanism for transferring money and pose as a legitimate target for payment...

Insider Disbursement Fraud...

One of the most common methods of misappropriating cash from an organization involves disguising a fraudulent disbursement as a legitimate one. A shell company is the perfect vehicle for this purpose...

Pass-Through Disbursement Schemes...

Bid-Splitting...

Masking Collusion Among Vendors...

Conduit for Paying Bribes...

In this scenario, a shell company is established, perhaps posing as a vendor or charity. The company transfers funds

to the shell, supported by apparently legitimate documentation...

While previous efforts have failed, the Panama Papers leak and other recent high-profile incidents of tax evasion and money laundering may be what finally moves the needle — not only in the United States, but globally.

TODAY'S GENERAL COUNSEL

INFORMATION GOVERNANCE CAN MAKE DATA AN ASSET

By [Karen Schuler](#) and [Douglas Herman](#)

E-discovery is not a new phenomenon. Computers, e-mail, network shared drives and portable USB storage devices have been common sources of preservation and electronically stored information (ESI) collection for years, and for the most part organizations seem to have figured out how to preserve and manage these more traditional electronic sources in a reasonable manner...

Our firm's recent "Inside E-Discovery" survey found that the volume, variety and velocity of disparate data are a major concern of corporate counsel. Not only is the data universe growing, so are the number of places where data is stored. There is a pressing need, therefore, for sound information governance. Its importance for e-discovery simply cannot be overstated....



BDO CONSULTING GLOBAL FORENSICS PRACTICE

Experienced in conducting high-profile investigations and utilizing resources in more than 150 countries, BDO's Global Forensics practice helps multinational organizations identify and mitigate risks associated with fraud and corruption, providing investigation, due diligence, anti-corruption compliance and fraud prevention services.

BDO CONSULTING FORENSIC TECHNOLOGY SERVICES PRACTICE

BDO's experienced Forensic Technology Services professionals provide value-added solutions to clients across the globe, including information governance, digital forensics and cyber investigations, e-discovery, data analytics and national security compliance/CFIUS.

Organizations should consider the following to build a corporate-wide information governance program:

- ▶ **Due Diligence and Planning...**
- ▶ **Data Quality Standards...**
- ▶ **Security, Integrity and Privacy...**
- ▶ **Availability and Transparency...**
- ▶ **Management and Enforcement...**
- ▶ **Alignment...**
- ▶ **Governance...**

These elements drive a comprehensive approach to bringing industry and regulatory standards to the information governance program, and they result in discovery being easier and more cost-effective.

PROPERTYCASUALTY 360

EMPLOYEE FRAUD: 6 STEPS TO SUBSTANTIATING YOUR CLAIM AND RECOVERING LOSSES

By [Matt Hanson](#)

How do you effectively manage fraud claims to substantiate allegations, recoup your losses and prevent future wrongdoing?...

Step 1: Preserve and gather the evidence...

Step 2: Interpret the evidence...

Step 3: Exhaust the search...

Step 4: Interview the witnesses...

Typically, the first interview is with someone other than the suspect, such as a co-worker. You will likely only have one shot at asking the suspect questions to address the full scope of the claim, so you will want to first gather enough information to make a credible allegation against the employee in question. A proper interview will help you get a statement, establish facts or validate allegations, and decide where to go next in terms of additional interviews or evidence...

Step 5: Take appropriate action...

Decide whether to terminate or suspend the suspected employee(s), and consider referring the matter to law enforcement. This is a sensitive part of the claims process that should be considered from the beginning...

Step 6: Prepare for the adjustment process...

Document everything to a level of detail that enables re-performance.

MERGERS & ACQUISITIONS

BDO'S JOHN LASH SAYS DEFENSE AND SECURITY COMPANIES ARE MOST LIKELY TO COME UNDER U.S. SCRUTINY IN FOREIGN TRANSACTIONS

By [John Lash](#)

Foreign direct investment (FDI) into the United States has continued unabated in 2016, with Chinese buyers leading the charge. Most of these acquisitions fall into the \$1 billion-plus range, but China is also looking to the middle market to gain a strategic foothold in the U.S. And as foreign investment in the U.S. continues to swell, so too does regulatory scrutiny of cross-border transactions.

A critical element of FDI is the involvement of the committee on foreign investment in the United States (CFIUS). Chaired by the U.S. Secretary of the Treasury, this interagency task force within the U.S. government is responsible for the review of FDI that could result in the control of a U.S. business or critical assets, evaluating the impact of such transactions on national security...

What constitutes a national security threat? U.S. businesses that may come under scrutiny include those that: Are in the defense, security and national security-related law enforcement sectors; Provide products and services to the government with potential security or defense applications; Constitute "critical

infrastructure," e.g., energy production or transportation; Have access to classified or sensitive government information; Engage in activities subject to U.S. export controls; Are in proximity to U.S. government facilities...

To bridge the gap between depth and breadth of experience within operating segments, organizations should leverage all personnel resources, including: Compliance; Cybersecurity; Logical security; Physical security; Network / Information Technology; and Supply Chain Management / Product Lifecycle...

Organizations should evaluate the national security implications of transactions at the onset of the deal, and engage early and aggressively to address any potential issues with a coordinated strategy. Cross-border M&A has evolved to a point of multi-disciplinary teams and cross-functional projects deploying simultaneously within an organization to ensure a comprehensive security posture. With regulatory compliance remaining a key area of focus for the U.S. government, organizations should plan ahead and expect to deploy resources effectively to address CFIUS concerns.

HEALTHCARE DIVE

MEDICARE FRAUDSTERS BEWARE: THE GOVERNMENT IS COMING

By [Jeff Byers](#) and [Ana Mulero](#)

The Justice Department announced this week the Medicare Fraud Strike Force is pressing charges against 301 defendants in 36 federal judicial districts across the country for their alleged participation in Medicare fraud cases involving about \$900 million in false billings. The DOJ said the "coordinated takedown" is the largest in the task force's history in terms of the number of defendants and loss amount...

The biggest case in the takedown the DOJ cited as an example included five individuals in the Eastern District of New York who were charged for being involved in more than \$86 million in physical and

occupational therapy claims to Medicare and Medicaid. In this case, the defendants allegedly controlled a network of Brooklyn clinics by paying bribes and kickbacks...

Clearly, the government is setting a tone that they are going after more healthcare fraud, **Venson Wallin, consulting managing director at accounting firm BDO**, told Healthcare Dive.

He noted once the ACA was implemented, provisions were made to focus on reducing healthcare fraud as a means to reduce healthcare costs and inefficiencies of the Medicare program. **"It's not an endless supply of money," he notes.** In fact, the Board of Trustees for Medicare released its annual report emphasizing just that...

While there are clearly bad actors in the stage of Medicare fraud, **Wallin notes** the industry's push toward value can create confusing billing processes, which can lead to inadvertent fraudulent claims. When establishing quality metrics, administrators need to understand how decisions may impact overall compliance programs. One question to ask could be, **"Are you directly or indirectly incentivizing individuals to stretch the truth to meet certain quality metrics?"**

He shared three tips to avoid the DOJ from knocking on your door:

- ▶ Measure and monitor...
- ▶ Review your compliance program...
- ▶ Evaluate your partners.

GLOBAL TRADE MAGAZINE

CYBERSECURITY JUMPS TO THE TOP OF MANUFACTURERS' BIGGEST RISKS

By Peter Buxbaum

As data and connectivity transform the industry, manufacturers' intellectual property, data and products have become prime targets for cybercriminals.

More than nine in 10 manufacturers cite cybersecurity concerns in their SEC disclosures this year, according to a new report from **BDO USA, LLP, an accounting and consulting organization.** That represents a 44 percent jump from 2013—and the first time in BDO's analysis that cyber risk ranks among manufacturers' top 10 risk factors...

Manufacturers with global operations are also growing more cautious of the international regulatory environment. Seventy percent of manufacturers worry about their ability to comply with the Foreign Corrupt Practices Act (FCPA) and other anti-corruption and bribery laws, a notable increase from just 45 percent in 2013. These [regulations] ... along with a drop in U.S. labor costs since the recession, seem to be encouraging manufacturers to hire more and expand operations domestically.

Federal, state and local regulations are highlighted by 99 percent of manufacturers in their annual filings and are among the top two risks for the fourth year running. In particular, environmental regulatory risks are top of mind this year, cited by 95 percent of manufacturers. Forty-two percent mention regulations around emissions standards.

"Manufacturers are subject to various aspects of the regulatory landscape, but compliance and competitive advantage are not mutually exclusive," said Dawn Williford, south region leader of BDO's Risk Advisory Services. "When done right, risk management can be more of a boon than a burden to manufacturers by reducing costly errors and enhancing the operational foundations of the business."

Material discussed in this article is meant to provide general information and should not be acted on without professional advice tailored to your firm's individual needs.

CONTACT:

GLENN POMERANTZ
Global Forensics
212-885-8379
gpomerantz@bdo.com

STEPHANIE GIAMMARCO
Forensic Technology Services
212-885-7439
sgiammarco@bdo.com

ABOUT BDO CONSULTING

BDO Consulting, a division of BDO USA, LLP, provides clients with Financial Advisory, Business Advisory and Technology Services in the United States and around the world, leveraging BDO's global network of more than 64,000 professionals.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms.

© 2016 BDO USA, LLP. All rights reserved.

www.bdo.com