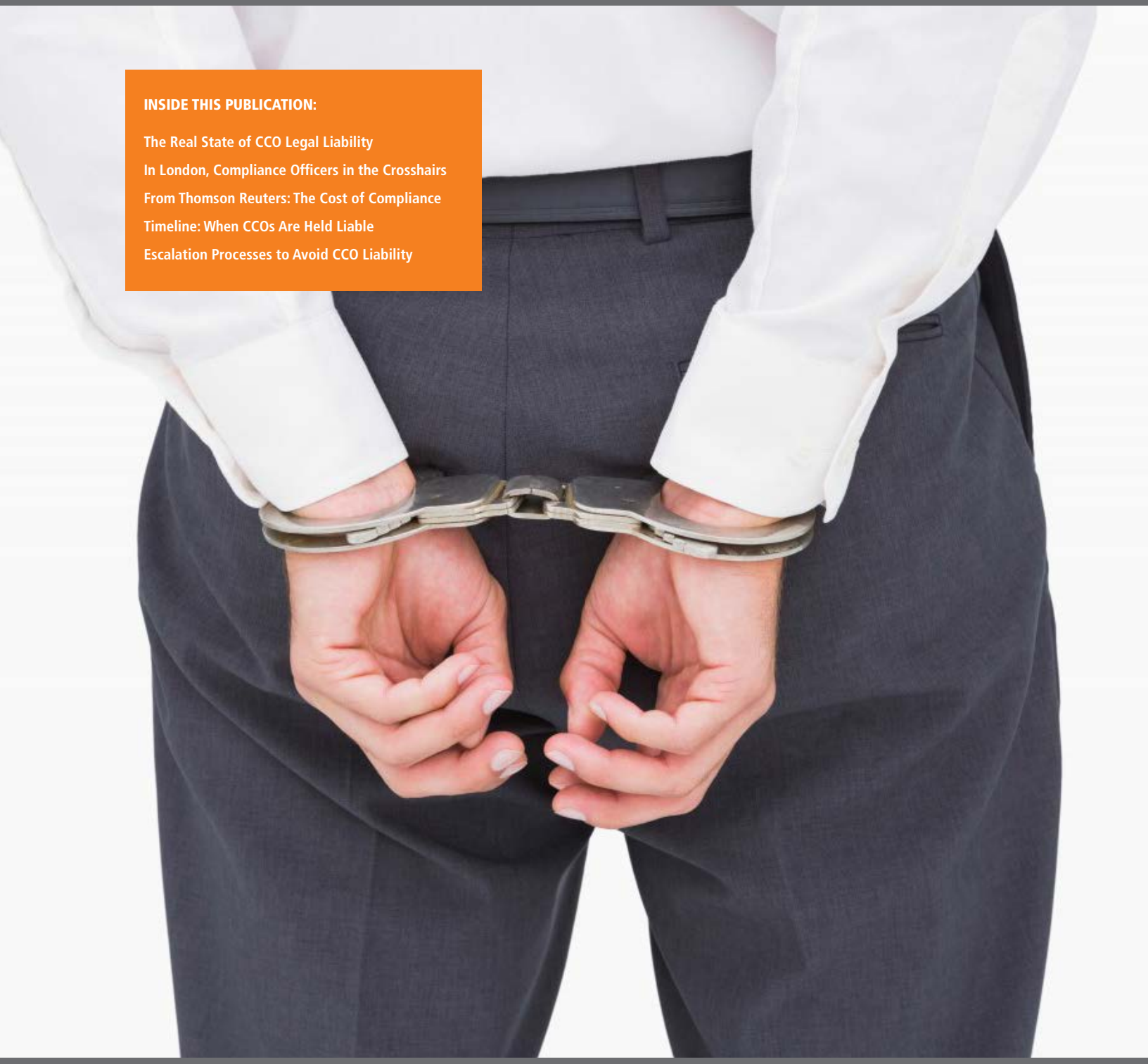
Brought to you by the publishers of COMPLIANCE WEEK



INSIDE THIS PUBLICATION:

The Complexities of
CCO Liability

An e-Book publication sponsored by THOMSON REUTERS™

COMPLIANCE WEEK

Compliance Week, published by Wilmington Group plc, is an information service on corporate governance, risk, and compliance that features a weekly electronic newsletter, a monthly print magazine, proprietary databases, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has quickly become one of the most important go-to resources for public companies; Compliance Week now reaches more than 26,000 financial, legal, audit, risk, and compliance executives.

THOMSON REUTERS™

Risk Management Solutions from Thomson Reuters combine what no one else can: information, services, software and expertise to help you efficiently manage risk — and drive smarter business decisions.

This trusted combination of solutions helps you manage customer, third party, compliance, enterprise and financial risk along with corporate governance and controls across your organization. Agile, innovative, and unrivalled anywhere in the marketplace, these solutions take your business beyond mere risk avoidance. They help you proactively create and sustain a culture of compliance, and build a reputation for consistently driving the best behavior and performance from your people and operations.

With Thomson Reuters, you can turn regulatory complexity into a business opportunity – and ultimately, a compelling competitive advantage everywhere you do business.

Our offerings include market-leading solutions for enterprise governance, risk and compliance management, policy management, global regulatory intelligence, financial crime, anti-bribery and corruption, supply chain risk, enhanced due diligence, compliance training and e-learning, and Board of Director collaboration.

Audit, risk, legal and compliance professionals, business leaders and the Boards they serve in more than 10,000 companies across the globe use Thomson Reuters content, workflow technology and software solutions to navigate risk and regulation, drive a compliance culture, support good governance and act with integrity. These professionals operate in a diverse range of highly regulated industries, including financial services, insurance, pharmaceutical, oil and gas, aerospace and defense, automotive, commodities, gambling and gaming and government.

Learn more at risk.thomsonreuters.com.

Inside this e-Book:

The Real State of CCO Legal Liability

By Jaclyn Jaeger

A compliance failure in a company can feel like a personal and professional failure to chief compliance officers. The more urgent question, however, is whether it might also bring personal or professional liability.

At Compliance Week 2015, enforcement officials with the Securities and Exchange Commission and the Justice Department, as well as compliance professionals themselves, tried to answer that question and explored how CCOs can protect themselves from such risk.

During a keynote speech, Leslie Caldwell, assistant attorney general for the Justice Department's Criminal Division, tried to ease compliance officers' concerns that they may be found personally liable for compliance lapses in oversight. "We view compliance as the frontline of defense against all the problems that come to our attention," she said. "We're not out there looking to make examples of, or prosecute, compliance officers."

Stephen Cohen, associate director of the SEC's Division of Enforcement, shared that sentiment during another panel discussion. "I can promise you we are not sitting around looking for ways to charge chief compliance officers," he said. "In my opinion, we're in the same line of work; we're partners in ensuring sound and effective compliance cultures are part of the business."

Regardless, the SEC and Justice Department are enforcement agencies, and they will prosecute individuals who fail to act in good faith, or who mislead regulators in any way. CCOs are no exception to this rule, as indicated by a handful of recent cases.

In April, for example, the SEC brought charges against Bartholomew Battista, the former CCO of asset manager BlackRock Advisors, and fined him $60,000 for failing to report a "material compliance failure" to the firm's board of directors. Blackrock agreed to a related $12 million penalty.

Specifically, Blackrock and Battista failed to disclose that Daniel Rice, a top-performing portfolio manager, was managing energy-focused funds and separately managed accounts at BlackRock when he founded Rice Energy, a family-owned oil and natural gas company. Rice Energy later formed a joint venture with a coal company that eventually became the largest holding in the BlackRock Energy & Resources Portfolio.

> "We view compliance as the frontline of defense against all the problems that come to our attention. We're not out there looking to make examples of, or prosecute, compliance officers."
>
> Leslie Caldwell, Assistant Attorney General, Justice Department

"BlackRock knew and approved of Rice's investment and involvement with Rice Energy as well as the joint venture, but failed to disclose this conflict of interest to either the boards of the BlackRock registered funds or its advisory clients," the SEC said in a statement. "BlackRock additionally failed to adopt and implement policies and procedures for outside activities of employees, and Battista caused this failure."

Left to right: Ellen Hunt of AARP; Patrick Smith of DLA Piper; and Stephen Cohen of the Securities and Exchange Commission.

In another example, the Treasury Department's Financial Crimes Enforcement Network last year fined Thomas Haider, the former CCO for MoneyGram International, $1 million for failing to ensure that his company abided by the anti-money laundering provisions of the Bank Secrecy Act. The Financial Industry Regulatory Authority similarly fined a compliance officer last year for substantial anti-money laundering compliance failures. In that case, Harold Crawford, former global AML compliance officer for investment bank and securities firm Brown Brothers Harriman, was fined $25,000.

It's no wonder compliance officers are feeling the heat. As Ellen Hunt, director of ethics and compliance for AARP, quipped: "You can't put corporate culture in an orange jumpsuit."

A recent survey by Thomson Reuters echoed that concern. The report found that 59 percent of nearly 600 compliance professionals in financial services firms said they expect their personal liability to increase in 2015. That figure is up from 53 percent who gave the same response last year.

Preventing Personal Liability

Despite an increasing number of enforcement actions imposed on CCOs, the news isn't as dismal as it sounds. "People who perform their responsibilities diligently, in good faith, and in compliance with the law are our partners, and they're not responsible, typically, from a liability perspective," Cohen said during a keynote panel at Compliance Week 2015.

The idea that a compliance officer would face criminal liability for acting in good faith, even in the event of a compliance failure, is "almost inconceivable," Caldwell said. In reality, the CCOs who have faced a civil or criminal case ei-

ther directly participated in the misconduct, mislead regulators, intentionally ignored their compliance responsibilities, or all of the above.

During an investigation, Cohen said, the first thing the SEC will examine is how the CCO handled an issue as it arose. That means compliance officers should document every decision they make to demonstrate that they took adequate measures, in the event that enforcement agencies come knocking.

Patrick Smith, co-chair of the white-collar corporate crime and investigations practice at DLA Piper, advised that CCOs further document every decision they make during the investigation phase and the resolution phase, including any disciplinary measures. "The most effective thing you can do when there is a significant compliance lapse is to fire someone," he said.

In the MoneyGram case, for example, FinCEN particularly faulted Haider's failure to suspend or terminate any agents participating in illicit activity. "His inaction led to thousands of innocent individuals being duped out of millions of dollars through fraud schemes that funneled, and sometimes laundered, their illicit profits through MoneyGram's money transmission network," FinCEN said at the time.

"When the investigation breaks out, your entire track record and your responsibilities as a compliance officer are going to be looked at," Smith said. The question, he said, is, "Will you be deemed to have been willfully blind or constantly avoided the wrongdoing in your organization?"

Whistleblower CCOs

Panelists also talked about the role of CCOs as whistleblowers. Generally, the expectation is that compliance officers who receive internal reports of wrongdoing will investigate those reports in the ordinary course of business. "We're not looking to change that structure," Cohen said. The idea of giving whistleblower awards to CCOs is "hopefully that it opens compliance officers' eyes that there is another option—not the first option, but another option."

Compliance officers' eyes were certainly opened earlier this year, when one of their own received more than $1 million as a whistleblower award against his or her own company. The SEC has never identified the person, the company, or even exactly what he or she did there—the agency only disclosed that the winner was a "compliance or audit" executive.

The compliance officer in that case felt disclosure to the SEC was necessary, Cohen said, because management was aware of illicit activity and wasn't doing anything about it. "The chief compliance officer wasn't sitting around spotting wrongdoing and rushing to the SEC to try to make money," Cohen said.

A requirement to report to the very same people who already know about wrongdoing "doesn't make a lot of sense to me," Cohen said. "This compliance officer did what, quite frankly, I think they ought to have done: They looked for another path to rectify [the problem]."

Whistleblower awards are "an important lifeline," Hunt said. Although cleaning up misconduct internally is the best avenue to take, compliance officers know that "sometimes our colleagues lie to us," she said. "They don't tell us the truth, so you have to be diligent."

You have to seek that balance between your loyalty to the company and doing what's right, Hunt added. "Sometimes you're going to have to die on that sword." ■

CCO PERSONAL LIABILITY CASES

Below is a summary of enforcement actions brought by various enforcement agencies against chief compliance officers for alleged compliance lapses in oversight.

Agency: U.K. Serious Fraud Office

Case Summary: On May 12, 2015, the U.K. Serious Fraud Office charged Jean-Daniel Lainé, former senior vice president of ethics and compliance of Alstom International Limited, with violating Section 1 of the Prevention of Corruption Act, as well as two offenses of conspiracy to corrupt in violation of Section 1 of the Criminal Law Act. The alleged offenses took place between 2006 and 2007 and concern the supply of trains to the Budapest Metro. The matter has been sent for trial at Southwark Crown Court.

Agency: Securities and Exchange Commission

Case Summary: On April 20, 2015, the SEC charged Bartholomew Battista, the former chief compliance officer of asset manager BlackRock Advisors and fined him $60,000 for failing to report a "material compliance failure" to the firm's board of directors. Blackrock agreed to a related $12 million penalty. According to the SEC, Blackrock and Battista failed to disclose that Daniel Rice, a top-performing portfolio manager, was managing energy-focused funds and separately managed accounts at BlackRock when he founded Rice Energy, a family-owned and operated oil-and-natural gas company. Rice Energy later formed a joint venture with a coal company that eventually became the largest holding in the BlackRock Energy & Resources Portfolio.

Agency: Financial Crimes Enforcement Network

Case Summary: On Dec. 18, 2014, FinCEN fined Thomas Haider, the former CCO for MoneyGram International $1 million for failing to ensure that his company abided by the anti-money laundering provisions of the Bank Secrecy Act. Concurrently, the U.S. Attorney's Office for the Southern District of New York filed a complaint in U.S. District Court that seeks to enforce the penalty and bar Haider from future employment in the financial industry.

Agency: Financial Industry Regulatory Authority

Case Summary: On Feb. 5, 2014, FINRA fined Harold Crawford, former global AML compliance officer for investment bank and securities firm Brown Brothers Harriman (BBH), $25,000 for substantial anti-money laundering compliance failures, including its failure to have an adequate anti-money laundering program in place to monitor and detect suspicious penny stock transactions. BBH agreed to a related $8 million fine.

Source: Compliance Week.

In London, Compliance Officers in the Crosshairs

Compliance officers who find themselves subject to prosecutorial scrutiny should seek independent legal advice as soon as possible

By Howard Stock

The corruption and conspiracy charges brought by Britain's Serious Fraud Office against Alstom SA could have serious implications for compliance officers.

On May 12, the prosecutor—the SFO is keen to distinguish itself from mere regulator—charged Jean-Daniel Lainé, former senior vice president of ethics and compliance at Alstom, with corruption and conspiracy to corrupt, according to court documents. The charges involve numerous Alstom subsidiaries, but Lainé has been charged for his alleged role in bribes paid to the Budapesti Kozlekedesi Vallalat (BKV) to win a contract between BKV and Alstom Transport SA to supply trains for Budapest's metro system. Lainé appeared at Westminster Magistrates Court on May 12, and the case is expected to go to trial early in 2017.

Former director Graham Hill, who once oversaw compliance at Alstom, faces similar charges regarding India's Dehli Metro. Bruno Kaelin, another compliance officer, was named as a co-conspirator but has not been formally charged. Hill's case is due to go to trial next May.

Compliance officers rarely find themselves in the dock in cases of fraud; indeed, the SFO has never prosecuted a compliance officer before. Lainé, whose compliance program was certified by independent agency ETHIC Intelligence in 2009 and was renewed for two more years in 2011, is the sixth individual charged in the hydra-headed story of Alstom corruption. Lainé retired from the company in 2013 after 40 years.

Alstom SA pleaded guilty in the United States in December, agreeing to pay a record $772 million to resolve investigations into a bribery scheme prosecutors said was "astounding in its breadth." The settlement followed a five-year investigation into transport projects in India, Poland, and Tunisia. The interesting thing about Lainé's alleged involvement, however, may not be so much what he may or may not have done, but rather what he did not do: operate a compliance program that prevented the fraud from happening in the first place, or blowing the whistle once it had occurred.

In a May 20 speech at the Global Anti-Corruption and Compliance in Mining Conference, Ben Morgan, joint head of bribery and corruption at the SFO, reminded the audience that despite their best efforts, "corruption-free mining is not a reality." Still, he said, compliance officers would "have a chance, if you want to, to positively influence what happens if something goes wrong."

No Cozy Deals

Morgan may have delivered his comments to the mining sector, but they are just as valid for other industries as well. The implication of his words is clear: contact the SFO with corruption concerns you have before it discovers those problems itself.

"If you don't tell us, or you do and you don't engage with us properly, prosecution is a likely outcome," Morgan warned. The tone of his comments strongly suggested that confessing may put the individual in a better light, but that transparency will not be an absolute defense. "No cozy deals," he said. "So don't be under any illusion."

The impression of cooperation would not be sufficient, Morgan said, emphasizing the adversarial nature of the SFO. The only hope is in "actually helping us, behind [being] fully frank and honest with us," he said, remarking ruefully "as little by little some companies now are."

> "We are reliant on compliance officers and internal audit to act as an important line of defense to support effective regulation at firms and to show backbone even when challenged by their colleagues."
>
> Georgina Philippou, Acting Director of Enforcement, FCA

Don't expect that spirit of cooperation to be a two-way street, either. Aside from demanding an immediate mea culpa should any wrongdoing emerge, the SFO eschews providing any actual guidance. "As our director has memorably said in the past, we are not in the business of telling people how not to rob banks," Morgan said. "We are in the business of catching those that do and holding them to account." Cold comfort for compliance officers for whom failure to act fast enough will plainly be seen by the SFO as a suspicious act of obstruction.

A member of Lainé's legal defense team at Wilmer Hale, Christopher David, declined to discuss specific details of the Alstom case, but he did have general advice for compliance officers. He calls the SFO's current attitude and approach to compliance officers misguided and perhaps indicates a lack of awareness as to the role and function of a compliance officer within a multinational company.

"On a day-to-day basis, the SFO should be viewing the corporate compliance officer as the 'good guy' within a company who is trying to prevent illegal conduct," David says. "The SFO could and should support compliance officers by providing as much guidance as possible," as regulators are doing in the United States.

"Both the [Justice Department] and [Securities and Exchange Commission] are criminal prosecutors, yet Ben Morgan specifically said that he was not going to tell companies how to be compliant as the SFO is the 'prosecutor,' " David says. "This is an odd distinction when surely it is

in everyone's interest that criminal offenses are not committed in the first place."

While the SFO has not completed any cases against compliance officers yet, this isn't the first time that British regulators have taken compliance officers to task for breach of duty. In fact, this year has been a trying time for compliance officers.

In March, the Financial Conduct Authority settled with Stephen Bell, Financial Group's former compliance director, to the tune of £33,800 over the failure of his compliance program to prevent breaches of service by its financial advisers. In May, the FCA fined the former compliance officer at the Bank of Beirut £19,600 for his part in the bank's "repeatedly providing the regulator with misleading information after it was required to address concerns regarding its financial crime systems and controls."

Show Backbone

Georgina Philippou, the FCA's acting director of enforcement and market oversight, said of the case (which also fined the bank £2.1 million and its auditor Michael Allin £9,900), "We are reliant on compliance officers and internal audit to act as an important line of defense to support effective regulation at firms and to show backbone even when challenged by their colleagues."

CCOs are most exposed within sectors regulated by the FCA, David says, and from a criminal exposure point of view, compliance officers are particularly vulnerable in circumstances where they are required to give direct approval of the payment of commission to third parties.

"This could create a situation where the business hides key facts from the compliance officer and, notwithstanding the need to have a robust compliance program, the compliance officer therefore inadvertently becomes complicit in the making of corrupt payments," David says. "There should be a clear distinction between the compliance function and the business, particularly in relation to the approval of payments to third parties."

Compliance officers who find themselves subject to prosecutorial scrutiny should seek independent legal advice as soon as possible and not give any on-the-record interviews until personal legal advice has been obtained, David says—including to internal or company-appointed investigators. "This is not always practically possible, but given the current regulatory climate, should be kept in mind," he says.

To prevent an issue from arising in the first place, compliance officers, particularly those in highly regulated sectors, should make sure they understand all the products and services that their institution offers. This is an area of particular focus for regulators in the United States; the Justice Department has said it looks at a compliance officer's technical background and ability when reviewing a business compliance program, "and where the U.S. goes, U.K. regulators and enforcement agencies often follow," David says.

Given the SFO's mission, it is primarily focused on specific areas of alleged misconduct, and less so on the bigger picture. As such, compliance officers at companies under investigation by the SFO should strive to educate and assist the SFO in understanding the wider context from an early stage. The goal is to help the SFO understand the extent of the company's liability, as opposed to it being a case of rogue employees that the company could not have stopped.

"This is particularly important in the United Kingdom given our higher standards of corporate liability," David says. For compliance officers, trying to resolve a potential issue internally is not a safe option. ■

SFO TAKES ACTION

Below is an excerpt from the U.K.'s Serious Fraud Office regarding the charges the agency brought against Alstom's former director of compliance.

Further charges have been brought as part of the SFO's ongoing investigation of Alstom Network U.K.

In addition to the charges that were announced as part of phase three in April this year, the SFO has charged Jean-Daniel Lainé and he appeared this morning, together with Michael John Anderson, 54, and representatives of Alstom Network U.K., at Westminster Magistrates' Court. The matter has been sent for trial at Southwark Crown Court.

Mr. Lainé, 68, is a French national who attended court to answer two charges of corruption contrary to section 1 of the Prevention of Corruption Act 1906, as well as two offences of conspiracy to corrupt contrary to section 1 of the Criminal Law Act 1977. The alleged offences are said to have taken place between 1 January 2006 and 18 October 2007 and concern the supply of trains to the Budapest Metro.

Prior to retirement, Mr. Lainé was senior vice president ethics & compliance, and a director of Alstom International. He is the sixth individual to be charged by the Serious Fraud Office in its investigation of Alstom.

In April, Alstom Network U.K., formerly called Alstom International, a U.K. subsidiary of Alstom, was charged with a further two offences of corruption contrary to section 1 of the Prevention of Corruption Act 1906, as well as two offences of conspiracy to corrupt contrary to section 1 of the Criminal Law Act 1977.

Michael John Anderson, 54, of Kenilworth in Warwickshire, who was working as a business development director for Alstom Transport SA in France, has been charged with the same offences.

The alleged offences are said to have taken place between 1 January 2006 and 18 October 2007 and concern the supply of trains to the Budapest Metro.

The first hearing in this case will take place at Westminster Magistrates' Court on 12 May 2015.

Source: Serious Fraud Office.

THE COST OF COMPLIANCE

Executive Summary from *Cost of Compliance Survey 2015* by Thomson Reuters

Thomson Reuters has undertaken its annual survey into the cost of compliance and the challenges firms expect to face in the year ahead. Nearly 600 compliance professionals from financial services firms across the world took part in the survey. The report builds on annual surveys of similar respondents conducted over the last six years and where relevant highlights year-on-year trends and developments.

The survey has become a voice for practitioners. Great insight into the practical reality and challenges of compliance functions around the world can be gained from the open concerns and views that participants have shared, and for this Thomson Reuters extends its thanks, and an assurance that these views remain confidential.

The report findings are intended to help regulated financial services firms with planning, resourcing, and direction. Given the sharpening regulatory focus on global systemically important financial institutions (G-SIFIs), Thomson Reuters specifically asked G-SIFIs to identify themselves to enable comparison between themselves and other, smaller, firms.

The findings once again highlight the pressures facing compliance functions, and for 2015 serve as a red flag indicator that resources, outside of G-SIFIs are in danger of being stretched too thinly. The main findings are:

» Ever-increasing change: Compliance officers are clearly experiencing regulatory fatigue and overload in the face of snowballing regulations. Seventy percent of firms are expecting regulators to publish even more regulatory information in the next year, with 28 percent expecting significantly more.

» More than a third of firms spend at least a whole day every week tracking and analyzing regulatory change. Global regulatory change is creating the biggest challenge due to inconsistency, overlap, and short time frames. Understanding regulators' expectations and requirements and being able to interpret and apply them is as great a challenge as keeping abreast of the changes.

» Three-quarters of firms are expecting the focus on managing regulatory risk to rise in 2015. This is predominantly due to the greater regulatory focus on conduct risk.

» Personal liability: 59 percent of respondents (53 percent in 2014) expect the personal liability of compliance officers to increase in 2015, with 15 percent expecting a significant increase. Twenty-one percent of G-SIFIs expect a significant increase in personal liability.

» Resource challenges: from recruitment challenges in finding and retaining suitably skilled staff to increasing pressure on budgets. Two-thirds of firms are expecting skilled staff to cost more in 2015.

» Regulatory matters are consuming disproportionate amounts of board time, from correcting non-compliance and preventing further sanctions to implementing structural changes to meet new rules.

» Interaction and alignment between control functions continues to show a lack of coordination. Nearly half of compliance functions are spending less than an hour each week with internal audit.

» G-SIFIs, in comparison with the full population of respondents, have the greatest expectations about budget and resources available for tracking and analyzing regulatory change, updating policies, and liaising with regulators. ■

THOMSON REUTERS™

THOMSON REUTERS
ACCELUS™

THE RISING COST OF COMPLIANCE

70% OF FIRMS

are expecting regulators to publish even more regulatory information in the next year with **28%** expecting significantly more

MORE THAN 1/3 OF FIRMS

spend at least a whole day every week tracking and analyzing regulatory change.

41% of G-SIFIs

are spending more than a day creating and amending reports for the board

59%

of respondents expect the **PERSONAL LIABILITY** of compliance professionals to increase in 2015

2 OUT OF 3

of firms are expecting skilled staff to cost more in 2015

THREE-QUARTERS

of firms are expecting the focus on managing regulatory risk to rise in 2015

NEARLY HALF

of compliance functions are spending

LESS THAN AN HOUR

each week with internal audit

THOMSON REUTERS™

When CCOs Are Held Liable

Below is a timeline of some major CCO missteps between 2012-2015, which resulted in severe financial losses and reputational damage.

By Aarti Maharaj

MAY 8, 2013

FINRA Fines Compliance Officer $25,000

Miami-based Atlas One Financial Group was fined $350,000. Napoleon Arturo Aponte, former chief compliance officer and anti-money laundering compliance officer, was slapped with a $25,000 joint fine and severally with the firm, and suspended for three months in a principal capacity, says FINRA. According to reports, Aponte failed to identify and monitor suspicious account activity and disregarded to adequately investigate numerous AML "red flags," by filing a suspicious activity report (SAR).

Aponte
(Source: LinkedIn)

DECEMBER 20, 2012

Peter Madoff, former chief compliance officer, sentenced to 10 years in prison

Peter Madoff, former chief compliance officer and senior managing director of Bernard L. Madoff Investment Securities (BLMIS), was sentenced to 10 years in prison for crimes stemming from a two-count Superseding Information to which he pled guilty that charged him with, among other things, conspiracy to commit securities fraud, tax fraud, mail fraud, ERISA fraud, and falsifying records of an investment adviser. The overt acts in the conspiracy count also included, among other things, making false statements to investors about BLMIS's compliance program and the nature and scope of its investment advisory business. Madoff pled guilty in June 2012. He was sentenced in Manhattan federal court by U.S. District Judge Laura Taylor Swain.

Madoff
(Source: Bloomberg)

FEBRUARY 5, 2014

Former AML Compliance Officer Fined $25,000

Crawford

The Financial Industry Regulatory Authority (FINRA) fined New York-based Brown Brothers Harriman & Co. (BBH) $8 million for substantial anti-money laundering compliance failures including, among other related violations, its failure to have an adequate anti-money laundering program in place to monitor and detect suspicious penny stock transactions. BBH did not have an adequate supervisory system to prevent the distribution of unregistered securities. BBH's former Global Anti- Money Laundering Compliance Officer Harold Crawford was also fined $25,000 and suspended for one month.

In concluding these settlements, BBH and Crawford neither admitted nor denied the charges, but consented to the entry of FINRA's findings.

Franzen

NOVEMBER 13, 2014

Compliance officer and chief auditor on administrative leave, pending termination.

According to North Dakota University System (NDUS), Chief Auditor Timothy Carlson allegedly lied about his work history when applying for the job, and Chief Compliance Officer Kirsten Franzen allegedly failed to establish a compliance program since being hired last year. A scathing letter issued to Franzen by Chief of Staff Murray Sagsveen lists a number of other reasons for her leave, including:

- Failure to set fraud awareness training.
- Failure to establish trust with colleagues and clients.
- Refusal to implement preventative compliance measures.

MAY 12, 2015

SFO Brings Corruption Charges Against Former Alstom Compliance Executive

The U.K. Serious Fraud Office (SFO) brought further charges as part of its ongoing investigation of Alstom Network U.K., this time against a former compliance executive of Alstom. In addition to the charges announced, the SFO has charged Jean-Daniel Lainé at Westminster Magistrates' Court. Lainé is facing four corruption charges in violation of Section 1 of the Prevention of Corruption Act, as well as two offences of conspiracy to corrupt in violation of Section 1 of the Criminal Law Act.

Lainé

DECEMBER 18, 2014

Former MoneyGram CCO fined $1 million

Haider

Former Chief Compliance Officer for MoneyGram International Thomas Haider has been fined $1 million for failing to ensure that his company abided by the anti-money laundering provisions of the Bank Secrecy Act.

The announcement was made on by the Treasury Department's Financial Crimes Enforcement Network. Concurrently, the U.S. Attorney's Office for the Southern District of New York filed a complaint in U.S. District Court that seeks to enforce the penalty and bar Haider from future employment in the financial industry.

From 2003 to 2008, Haider was the CCO for MoneyGram, where he oversaw its fraud department and anti-money laundering compliance department.

Escalation Processes to Avoid CCO Liability

By Jose Tabuena
Compliance Week Columnist

Compliance officers and their staff have become more concerned lately about exposure to personal liability, since recent regulatory actions have shown them to be at risk.

The argument for that liability is this: Compliance is expected to know the regulations and how they apply to the business model, and so a CCO should recognize violations more readily. Compliance officers typically know more than the business-line folks whom they advise regarding the regulatory requirements for the company's operations. As compliance often communicates periodically with government agencies, a retrospective failure to inform regulators of problems in a timely manner might suggest they are ill-informed or withholding information.

As described in recent columns, applying the Three Lines of Defense Model creates clear oversight responsibilities, defined so that functions and departments understand the boundaries of their responsibilities and how their roles fit into the organization's overall risk and control structure. This clarity is especially helpful to the compliance function (and internal audit, to the extent they are combined with compliance or perform second-line support), because it delineates the ownership and management of key risk areas, including regulatory violations. The model can help reinforce that foremost, the business line owns the risks inherent in its operations and is accountable for maintaining effective internal controls to safeguard the company.

Compliance Officer Liability

Recent actions against compliance officers have made clear the increasing scrutiny. What's disconcerting is that the compliance department or its individuals may be perceived as having misunderstood regulatory requirements, or as having not implemented adequate controls. Personal liability can potentially arise not just for actively aiding and abetting a violation, but also for omissions and compliance failures.

For example, the Financial Industry Regulatory Authority fined the former compliance officer of Brown Brothers Harriman $25,000 for "substantial anti-money laundering compliance failures," which included not having processes in place to monitor and detect suspicious transactions. Likewise, the Financial Crimes Enforcement Network recently hit the former chief compliance officer of MoneyGram with a $1 million civil penalty for failing to ensure that the company abided by the anti-money laundering provisions of the Bank Secrecy Act.

While these actions have been confined to the financial services sector, they portend professional and personal exposure for those undertaking a high-level compliance position. These concerns about gatekeeper responsibilities for compliance professionals shadow the concerns in-house counsel have about being in the cross-hairs following the Sarbanes-Oxley Act and subsequent regulations.

SEC Guidance on Supervisory Liability

The Securities and Exchange Commission has provided guidance on when compliance and legal professionals are considered to be acting as "supervisors" subject to liability for failing to supervise. This guidance, issued in the context of broker-dealer responsibilities, is consistent with the approach of the Three Lines of Defense model—namely, that the senior management in the first line of defense has ultimate responsibility for compliance.

The SEC staff guidance clarified that compliance personnel will not be held liable solely for being ineffective at detecting and preventing violations of law. Specifically, the determination of whether or not a person is a supervisor is based on whether that person has the requisite degree of responsibility or authority to affect the conduct of those whose activities are at issue (actively aiding in violation or recklessly ignoring the compliance matter). The SEC provides a list of questions to ask when considering whether a person is a supervisor, including:

- Has the person clearly been given, or otherwise assumed, supervisory authority or responsibility for particular business activities or situations?
- Do the firm's policies and procedures, or other documents identify the person as responsible for supervising, or for overseeing, one or more business persons or activities?
- Did the person have the power to affect another's conduct? Did the person, for example, have the ability to hire, reward, or punish that person?
- Did the person otherwise have authority and responsibility such that he or she could have prevented the violation from continuing, even if he or she did not have the power to fire, demote, or reduce the pay of the person in question?

Moreover, the guidance provides that compliance personnel can perform certain activities without being considered a supervisor, such as setting up a compliance program and providing advice to business line personnel. Compliance personnel do not become supervisors merely by participating in or providing advice to management or a senior executive committee. Nor, however, can a supervisor also be a mere bystander to events and ignore wrongdoing or red flags of irregularity.

Escalation Policies and Other Defenses

The SEC and the Three Lines of Defense model offer a framework that can protect compliance staff as well as the organization. Compliance and other second-line functions should keep in mind that when enough high-level people know something, the concern becomes a firm issue rather than one of personal exposure. Perhaps even worse

> Compliance will want to take an active role in monitoring whether matters raised are tracked to completion, including documentation of any appropriate discipline.

than the CEO and board first learning of a problem in the front pages, is the CCO realizing that the issue should have been disclosed to senior leadership, but was not.

One of the best protections for the compliance department is to have clear escalation policies. When misconduct occurs, state and document which supervisor is responsible for handling the matter. Boards and committees on which the CCO serves should specify in formal charters that the compliance role is advisory. Serious concerns that involve potential legal violations should be escalated to designated senior management.

The content of an escalation policy should be developed with the board and senior management based on what they need to know and when. Here are examples of issues that should be escalated:

- When the CEO, board member, or senior executive is named in an allegation.
- Anything with potential to cause reputational harm.
- Any significant financial or accounting issue; these must be defined (and generally escalated to the chair of the audit committee).
- Remedial action committed to, but not executed, by an executive or board director.

Protection of Legal Privileges

Escalation policies should be developed in conjunction with internal investigation protocols and processes for company personnel to assert the appropriate attorney-client privilege and work-product protections. The good news, as made clear in the Barko decision in federal appeals court last year, is that legal privilege can apply widely during internal investigations. The important element is to have robust processes to demonstrate that the legal advice is being sought such that the privilege applies.

Substance over form is what matters. The D.C. Circuit in Barko assigned little importance to who conducted witness interviews and what was specifically said to those interviewed about the purpose of the investigation. Nor did the D.C. Circuit regard the involvement of outside counsel as essential. What mattered was that lawyers, in this case in-house lawyers, were overseeing a fact-gathering process intended to help provide the company with legal advice. And what matters is having experienced staff and clear processes for conducting investigations and raising the privilege under the proper circumstances.

Of course the best protection for compliance and the company is to ensure that escalated issues are addressed quickly and appropriately. Compliance will want to be active in monitoring whether matters raised are tracked to completion, including documentation of any appropriate discipline.

Currently the liability risk for CCOs outside the financial industry is relatively low; for those who do their job and raise issues appropriately, however, the risk is even lower. ■

Jose Tabuena provides a unique perspective on internal auditing issues bringing Big 4 firm experience and having held a variety of audit-related roles, including compliance auditor, risk manager, corporate counsel, and chief compliance officer. He has conducted sensitive internal investigations and assessed the performance of internal audit and ethics and compliance functions in highly regulated industries. Tabuena has held major compliance management roles at Kaiser Permanente, Texas Health Resources, Orion Health, and Concentra | Humana. Tabuena is certified as a fraud examiner, in healthcare compliance, and he is an OCEG Fellow. Tabuena can be reached at jtabuena@complianceweek.com.

RECENT COLUMNS BY JOSE TABUENA

Below are some recent columns by Compliance Week Columnist Jose Tabuena. To read more from Tabuena, please go to www.complianceweek.com and select "Columnists" from the Compliance Week toolbar.

Applying the Three Lines of Defense Model
CW's Jose Tabuena continues his look at the Three Lines of Defense model by examining how a company can parcel out all its oversight functions across the three lines. Can compliance report to the risk-management function? (Yes.) Can internal audit and compliance be combined? (Only if you avoid several pitfalls that undermine independence.)
Published online 01/21/15

Effective Governance and the Three Lines of Defense
CCOs, internal auditors, fraud investigators—these days, they all may work at one firm jointly to assist in managing risk. The trick to effective governance, however, is to assign all those professionals to their proper places in the Three Lines of Defense model. Jose Tabuena explores the logic behind that model.
Published online 12/16/14

Information Governance: Creating Order in a World of Chaos
The massive accumulation of information can overwhelm companies, creating compliance risks. To meet the challenge of information governance, companies are mapping out existing systems where data resides and may be managed. Columnist Jose Tabuena looks at how companies are dealing with data overload.
Published online 11/11/14

Can Compliance and Audit Ever Tame Data Technology?
The rapid pace of change in new data technologies have fundamentally changed business operations and the work environment. Along with these advances come new and often unexpected compliance challenges. Columnist Jose Tabuena discusses the technological competence internal auditors will need to keep up.
Published online 10/15/14

REUTERS/ Denis Balibouse

RISK MANAGEMENT SOLUTIONS

CONFIDENTLY ANTICIPATE RISK AND MAKE BETTER BUSINESS DECISIONS

Thomson Reuters illuminates the path ahead, empowering you to help your business successfully navigate the evolving risk and regulatory landscape. We connect you to the intelligence and insight you need, when you need it, so you can make risk-aware choices addressing both challenges and opportunities.
Our solutions help you to:

- Understand risk and identify opportunity
- Take actions informed by industry-leading intelligence
- Connect risk and regulatory insights with strategy
- Implement best practices that drive value

By connecting trusted information, intuitive technology and insightful people, our solutions help you to confidently anticipate and act on risk.

LEARN MORE
RISK.THOMSONREUTERS.COM

THOMSON REUTERS™