Journal of Technology Law & Policy

Volume 20 | Issue 2 Article 4

December 2015

Corporate Compliance in the Digital Age

Sean Hipworth

CORPORATE COMPLIANCE IN THE COMPUTER AGE

Sean G. Hipworth[*]

I. INTRODUCTION

The high cost of a compliance failure, both in monetary (*e.g.*, fines) and non-monetary (*e.g.*, bad publicity) terms has companies taking a more proactive approach to managing risk than they have in the past. Too many companies have been slow to act[1] in the face of existing industry standards, emerging regulatory regimes, and increasing enforcement efforts by U.S. and foreign government agencies, but for many companies (or at least their in-house counsel), compliance is a top priority.[2] A recent poll of thousands of Chief Legal Officers or General Counsel by the

* J.D. 2015, University of Florida (cum laude) and passed the Florida Bar exam July 2015. In law school, he served the Association for Public Interest Law, the *Journal of Technology Law & Policy*, completed the International & Comparative Law Certificate Program, and focused primarily on business law issues. Currently, he is an Associate Attorney with Warner, Sechrest & Butts, P.A. in Gainesville, Florida.

1. Maxwell Murphy, *Some Firms Resist Beefing Up*, WALL ST. J., Mar. 3, 2015, at B8 (More than 300 companies, with a combined market value of more than $450 billion, utilize internal controls—to prevent financial errors and fraud—written more than two decades ago, while the most widely followed standards were updated more than a year and a half ago).

2. Ashby Jones, *Highlights From the Law Blog*, WALL ST. J., Feb. 9, 2015, at B7 ("In-House Lawyers Worry About Ethics, Data, Trolls").

Association of Corporate Counsel showed that ethics and compliance are "important" or "extremely important" to respondents, and not far behind were data breaches.[3]

However, despite the growing concern over these issues in the business community, many companies struggle to find a clear path through the thicket. Especially in finance, for example, confident and aggressive behavior is in many ways incentivized, creating an "ethical culture" is often the work of a cottage industry of outside consultants or other experts.[4] Directors may even feel unable or impotent to affect needed change without such outside help.[5] Even if in-house counsel is equipped to address all existing compliance issues, and outside experts provide adequate assistance, today's compliance program may not suffice tomorrow, and even a robust policy, if not followed, will not be a complete shield against liability.

Perhaps the reason companies may have trouble coming to terms with their compliance obligations is that they fail to account for a moving target. A compliance program that can account for every conceivable present threat is insufficient insofar as it fails to be predictive or flexible enough to account for emerging risks. Like any desktop computer, a compliance program, especially if not conscientiously maintained, will quickly become obsolete and result in legal exposure for the company.

The author's focus is on two general areas of compliance risk: bribery and data protection. The objective is to highlight risk factors and propose solutions. The risks or solutions may have both human and technological elements. Both will be discussed as they are often complementary and neither exist in a vacuum.

II. WHY COMPLY?

Directors of corporations have a duty to monitor operations to ensure they are in compliance with the law; a board of directors cannot make this assumption without being informed.[6] In the seminal *Caremark*, the question was whether the directors of a corporation had breached their duty to monitor operations by allowing violations of the law to occur

3. Association of Corporate Counsel, *ACC Chief Legal Officers 2015 Survey*, (2015), *available at* http://www.acc.com/vl/public/Surveys/loader.cfm?csModule=security/getfile&pageid=1389460&page=/legalresources/surveys/index.cfm&qstring=&title=ACC%20Chief%20Legal%20Officer%20(CLO)%202015%20Survey%20-%20Executive%20 Summary.

4. Emily Glazer & Christina Rexrode, *As Regulators Focus on Culture, Wall Street Struggles to Define It*, WALL ST. J. ONLINE (Feb. 1, 2015), at A1, *available at* http://www.wsj.com/articles/as-regulators-focus-on-culture-wall-street-struggles-to-define-it-1422838659.

5. *See* Joann S. Lublin, *'Board Doctors,' to Supervise the Supervisors*, WALL ST. J., Feb. 18, 2015, at B5.

6. *In Re* Caremark, 698 A.2d 959 (Del. Ch. 1996).

(which resulted in a $250 million settlement by the corporation).[7] In that case, the Delaware Court of Chancery departed from earlier jurisprudence holding that the duty to monitor only arose if "something occurs to put them on suspicion that something is wrong."[8] Forty years later, the Delaware Supreme Court clarified the limits of the duty to monitor by holding that a board breaches its *Caremark* duties only when it "utterly fail[s] to implement any reporting or information system or controls" or "having implemented such a system or controls, consciously fail[s] to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention."[9]

A plaintiff asserting that a board of directors had not met its fiduciary duties must prove that the directors *knew* they were not discharging those duties.[10] In order to show scienter, plaintiffs must plead "particularized facts . . . that [the directors] had 'actual or constructive knowledge' that their conduct was legally improper."[11] The question unanswered is how difficult it would be to satisfy this requirement.

This scienter standard (burden of proof) provides sufficient protection for directors behind the business judgment rule (a rule of evidence) the result of which is that the judgment of a properly functioning board of directors will not be second-guessed absent an abuse of discretion so long as there is some informed basis for that decision.[12] Directors who adhere to this standard should be protected from derivative suits by shareholders, but may still be liable under applicable government regulations, rules, or statutes.

While a director's fiduciary duties are not *per se* a compliance issue, any failure to adhere to applicable regulatory regimes would likely expose a corporation or its directors or officers to a shareholder's suit.

A. *Anti-Bribery Regimes*

The Foreign Corrupt Practices Act (FCPA)[13] was first enacted in 1977 and amended twice, in 1988 and 1998, and makes it illegal for companies or their employees to bribe foreign officials. It also contains transparency requirements for accounting. The legislation was partly in response to a U.S. Securities and Exchange Commission (SEC) investigation in which

---

7. *Id.*
8. Graham v. Allis-Chalmers Mfg. Co., 188 A.2d 125, 130 (Del. 1963).
9. Stone *ex rel.* AmSouth Bancorporation v. Ritter, 911 A.2d 362, 370 (Del. 2006).
10. *Id.*
11. Wood v. Baum, 953 A.2d 136, 141 (Del. 2009).
12. *In re* KKR Fin. Holdings LLC Shareholder Litig., 101 A.3d 980, 989-90 (Del. Ch. 2014).
13. 15 U.S.C. § 78dd-1.

> more than 400 corporations . . . admitted making questionable or illegal payments. The companies, most of them voluntarily, . . . reported paying out well in excess of $300 million in corporate funds to foreign government officials, politicians, and political parties. These corporations . . . included some of the largest and most widely held public companies in the United States; over 117 of them rank[ed] in the top Fortune 500 industries.[14]

Finding that bribery of foreign officials was detrimental to U.S. companies and that corporate bribery was unnecessary for economic success, Congress passed the FCPA.[15]

The Act provides that anyone acting on behalf of a public corporation may not pay, promise to pay, or authorize the payment of any money, gift, or anything of value to a foreign official in order to influence his decision-making in an official capacity.[16] In other words, illegal bribes are not limited to money payments, and include practices such as providing employment for the relative of a business partner (or potential business partner). The statute contains no *de minimis* threshold for the value of the gift or item received.

The statute contains an exception for "facilitating or expediting payment[s] to a foreign official, political party, or party official the purpose of which is to expedite or to secure the performance of a routine governmental action."[17] Whether a payment is prohibited or falls under the exception is fact-based and is by no means certain (*i.e.*, there is not a bright line rule to guide a company's practices). The statute broadly defines "foreign official" to include:

> any officer or employee of a foreign government or any department, agency, or instrumentality thereof, or of a public international organization, or any person acting in an official capacity for or on behalf of any such government or department, agency, or instrumentality, or for or on behalf of any such public international organization.[18]

Because of the broad language of the statute, any company doing business in foreign jurisdictions must be wary of how business opportunities are secured or risk facing an enforcement action by the U.S. Department of Justice (DOJ). Because the statute applies to anyone acting on behalf of a corporation, including employees or agents, a single rogue

---

14. H.R. REP. NO. 95-640, at 4 (1977).
15. *Id.* at 4-5.
16. 15 U.S.C. § 78-dd1(a).
17. *Id.* at § 78-dd1(b).
18. *Id.* at § 78-dd1(f)(1)(A).

actor may result in a compliance failure. Persons the company deals with (*e.g.*, doctors employed by a state-run hospital) may not be manifestly foreign officials but could fall under the purview of the FCPA.

Increasingly aggressive enforcement actions of the FCPA by both the SEC and the DOJ have many companies on heightened alert for violations. The nebulous statutory standard is made more uncertain by the fact that enforcement actions are commonly settled and not adjudicated on the merits.[19] Defendants are incentivized to "accept resolution vehicles notwithstanding the enforcement agencies' untested and dubious enforcement theories or the existence of valid and legitimate defenses."[20] Even if a company has committed no violation, news of a regulatory inquiry or enforcement action against it could adversely impact business, and companies will be eager to settle the matter.

The FCPA's definition of "foreign official" has not been the subject of expansive judicial interpretation.[21] Prosecutors of enforcement actions often consider employees of state-owned enterprises to be "foreign officials" without regard to rank, title, or classification under their local law because they are considered instrumentalities of a foreign government.[22]

Whether a money payment (or anything of value) has been given for the purpose of "obtaining or retaining business" can also be uncertain.[23] In 2001, officers of a Houston-based corporation were indicted for allegedly making improper payments to Haitian "foreign officials" in order to reduce customs duties and sales taxes owed to the Haitian government.[24] The trial court granted the defendants' motion to dismiss because, as a matter of law, the alleged payments were not made with the purpose of obtaining or retaining business and did not fall within the scope of the FCPA's anti-bribery provisions.[25] On appeal, the Fifth Circuit held that such payments could provide an unfair advantage and thus might violate the FCPA, reversing and remanding the case.[26]

The U.S. Sentencing Guidelines encourage corporations to "[report] the offense to appropriate governmental authorities, fully [cooperate] in the investigation, and clearly [demonstrate] recognition and affirmative acceptance of responsibility for its criminal conduct."[27] These same guidelines discourage companies from challenging enforcement actions

19. Mike Koehler, *The Façade of FCPA Enforcement*, 41 GEO. J. INT'L L., 907, 907 (2010).
20. *Id.*
21. *Id.* at 916.
22. *Id.*
23. *See* 18 U.S.C. §§ 78dd-1(a), 78dd-2(a), 78dd-3(a) (2006).
24. United States v. Kay, 359 F.3d 738, 740 (5th Cir. 2004).
25. *Id.* at 742.
26. *Id.* at 755-56.
27. U.S. Sentencing Guidelines Manual § 8C2.5(g) (2009).

in adversarial proceedings because they may be treated more severely, if punishment is merited, because the nature of challenging an enforcement is to resist "affirmative acceptance of responsibility."[28]

U.S. companies doing business abroad may also be subject to the jurisdiction of other anti-bribery regimes in addition to the FCPA. The Parliament of the United Kingdom passed the Bribery Act of 2010[29] as a complete overhaul of existing anti-corruption and anti-bribery laws. Much like the FCPA, it has similarly broad reach and proscribes a broad range of conduct. "A person" commits an offense if he "offers, promises or gives a financial or other advantage to another person" and "intends the advantage . . . to induce a person to perform improperly a relevant function or activity, or . . . to reward a person for the improper performance of such a function or activity," or if he "knows or believes that the acceptance of the advantage would itself constitute the improper performance of a relevant function or activity."[30] Violations occur "whether the advantage is offered, promised or given by [a person] directly or through a third party."[31] As under the FCPA, the nature of the gift need not be monetary or reach a *de minimis* threshold to violate the law.

The European Union Convention against Corruption Involving Officials similarly prohibits both "passive" (receiving) and "active" (giving) corruption by means of "advantages of any kind whatsoever."[32] This broad language could conceivably cover anything of value (even *de minimis* value) given under a variety of circumstances, whether intended to induce favorable business decisions or not.

While Chinese culture has a long-held tradition of gift-giving, the Chinese government has more recently been increasing its efforts to combat corruption. The Anti Unfair Corruption Law of the People's Republic of China (PRC) applies generally to "managers," which is nearly as broad in its scope as the definition of "person" under the respective U.S. or U.K. anti-bribery regimes.[33] Violations may result in fines or criminal sanctions.[34]

More recently, the Criminal Law of the PRC was amended to impose

---

28. Koehler, *supra* note 19, at 927.

29. Bribery Act 2010, *available at* http://www.legislation.gov.uk/ukpga/2010/23/contents.

30. *Id.* § 1(1)-(3).

31. *Id.* § 1(5).

32. European Union Convention against Corruption Involving Officials (1997), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:41997A0625%2801%29:EN:HTML.

33. Anti-Unfair Competition Law of the People's Republic of China (中华人民共和国反不正当竞争法) (promulgated by the Third Session of the Standing Committee of the Eighth National People's Congress, Sept. 2, 1993, effective Dec. 1, 1993) art. 2.

34. *Id.* arts. 22-27.

criminal liability upon state functionaries soliciting or receiving bribes of a value of at least 5000 yuan, and provides for escalating penalties (including death) depending on increasing value and whether "circumstances are especially serious."[35]

Two things these regimes have in common are broad language and application. Only in the country with arguably the strongest tradition of gift-giving between business partners (China) is there a clear guideline or *de minimis* value a payment or "advantage" must reach to constitute illegal action, meaning gift-giving in other countries can be an especially dangerous business practice. Also, multinational or global enterprises engaged in proscribed practices may face liability in multiple jurisdictions for the same conduct.

The preceding regulations are only a few of those applicable to commerce, and only those imposed by a few of the largest jurisdictions, in market terms. Brazil,[36] Canada,[37] Japan,[38] and several African nations,[39] for example, have laws or measures that may impact any corporation doing business there.

B. *Anti-Bribery Failures*

Official bribery is broadly defined and can occur without any money changing hands. It is difficult to say how widespread such practices are, but high-profile instances have been made public.

Since 2011, the U.S. unit of Japanese electronics company Olympus Corp. has been under investigation by the DOJ for possible violations of anti-kickback laws.[40] In 2013, J.P. Morgan Chase & Co. disclosed that it was the subject of an investigation by the DOJ, focusing on the FCPA and the company's hiring practices in China.[41] One revelation in that probe was that Gao Jue, the son of China's commerce minister, was hired

---

35. Criminal Law of the People's Republic of China, Chapter VIII, arts. 383-86.

36. Clean Company Act 2014 (Law No. 12,846), *available in Portuguese at* http://www.cov.com/files/upload/E-Alert_Attachment_Brazilian_Clean_Companies_Act_Original.pdf.

37. Corruption of Foreign Public Officials Act (1998), *available at* http://laws-lois.justice.gc.ca/PDF/C-45.2.pdf.

38. Unfair Competition Prevention Act (last amended 1999), *available at* http://www.wipo.int/edocs/lexdocs/laws/en/jp/ jp040en.pdf; Penal Code (Act No. 45 of 1907), *available at* http://www.cas.go.jp/jp/seisaku/hourei/data/PC.pdf; National Public Service Ethics Act (Act No. 129 of 1999), *available at* http://www.cas.go.jp/jp/seisaku/hourei/data/npsea.pdf.

39. *See* Business Action Against Corruption (Africa), http://www.baacafrica.org/w/initiatives.php (last visited Apr. 25, 2015).

40. Takashi Mochizuki, *U.S. Inquiry Is Focused On Olympus*, WALL ST. J., Feb. 9, 2015, at B3.

41. Aruna Viswanatha & Emily Flitter, *Exclusive: U.S. Expands China Hiring Probe to Morgan Stanley*, REUTERS, Nov. 26, 2013, http://www.reuters.com/article/2013/11/26/us-china-jpmorgan-morganstanley-idUSBRE9AP19T20131126 (last visited Apr. 25, 2015).

and retained despite his poor performance.[42] Hong Kong authorities have also been investigating the hiring practices of other western banks.[43]

French engineering company Alstom SA's settlement over an FCPA enforcement action by the DOJ in 2014 was so large ($772 million) that it could not pay without hurting its ability to continue doing business, requiring court approval to delay the payment.[44] Avon Products, Inc. reached a settlement in 2014 for a $135 million payment, in addition to $350 million spent on investigations in China and elsewhere.[45] Wal-Mart Stores, Inc. "has spent more than half a billion dollars on its own probe into possible bribery in Mexico and other countries."[46]

Perhaps the most recent and scandalous example of official bribery involved Petróleo Brasileiro S.A. (Petrobras). In 2014, an investigation of money launderers operating out of gas stations eventually reached top levels of Petrobras, a semi-public Brazilian multinational, and threatened to derail the political career of President Dilma Rousseff.[47] Brazilian authorities alleged that some construction companies paid bribes to secure $23 billion in contracts.[48] In less than a year, prosecutors "charged 39 people with corruption, money-laundering and organized crime . . . includ[ing] two top Petrobras officials and 27 construction industry executives from large Brazilian firms."[49]

While the investigation of Petrobras was not initiated by U.S. authorities and does not involve an FCPA enforcement action, the scandal has undoubtedly had a chilling effect on Brazil's economy and in turn the willingness of U.S. multinationals to do business there. The scandal is particularly damaging due to Petrobras' importance to Brazil's economy, employing millions of people and having a substantial influence on the country's GDP.[50]

C. *Data Protection Directives and Requirements*

There are many ways a company may come into possession of data it is required by law to protect. Businesses are generally required to make reasonable efforts to protect sensitive personal information. The

---

42. Ned Levin et al., *Emails Track J.P. Morgan Hire in China*, WALL ST. J., Feb. 7-8, 2015, at A1.

43. *Id.*

44. Rachel Louise Ensign & Ted Mann, *Alstom Gets Break on a Fine*, WALL ST. J., Feb. 2, 2015, at B5.

45. *Id.*

46. *Id.*

47. Marla Dickerson & Rogerio Jelmayer, *Brazil Oil Giant Spawns Colossal Mess*, WALL ST. J., Feb. 2, 2015, at A9.

48. *Id.*

49. *Id.*

50. *Id.*

reasonableness of their protective efforts will depend on the type of data the company stores or acquires. The National Institute of Standards and Technology (U.S. Department of Commerce) published a Guide to Protecting the Confidentiality of Personally Identifiable Information in 2010.[51] The recommendations of that document "are intended primarily for U.S. Federal Government agencies and those who conduct business on behalf of the agencies, but other organizations may find portions of the publication useful."[52]

Several memoranda from the Office of Management and Business (OBM) define "personally identifiable information" as that which can be used to distinguish or trace a person's identity.[53] This data could include, for example, a person's name, address, social security number, telephone number, email address, driver's license number, or a combination of two or more of these pieces of data.[54] Entities doing business in a sector governed by the Health Insurance Portability and Accountability Act (HIPAA)[55] are required to safeguard medical records that could be used to identify an individual.[56]

In the Internet age, consumer data, which may include personally identifiable information, is easily gathered and quite valuable as an asset.[57] Treating these assets as the company's property without due care to safeguard consumers is, however, perilous.

Entities operating within the jurisdiction of the European Union are bound by even more stringent privacy laws (including the newly established "right to be forgotten"[58]), which are the subject of intense ongoing debate and a point of contention for many multinational U.S. Firms concerned about disparate standards.[59]

This is by no means an exhaustive survey of regulations. The United States has dozens of sector-specific privacy or data security laws, and many states have their own safeguards, any of which should be a concern

---

51. The National Institute of Standards and Technology, *Guide to Protecting the Confidentiality of Personally Identifiable Information* (2010), *available at* http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf.

52. *Id.* at ES-1.

53. *Id.* at C-1.

54. *Id.*

55. 45 C.F.R. § 160.103 (a "health plan," "a healthcare clearinghouse," or "a health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter").

56. *Id.* at C-2.

57. *See, e.g.*, Kate O'Keefe, *Real Prize in Caesars Fight: Data on Players*, WALL ST. J., Mar. 20, 2015, at B1.

58. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), 2014.

59. *See* Tom Fairless & Stephen Fidler, *Europe Aims to Impose Data Rules*, WALL ST. J., Feb. 25, 2015, at B1.

for general counsel serving in respective jurisdictions.

D. *Notable Data Breaches*

As more companies move away from paper filing and embrace paperless, electronic storage, data breaches become a more common occurrence. In 2013, the department store, Target, suffered a data breach that compromised the credit card and debit card data of as many as 40 million customers.[60] The company eventually proposed to pay $10 million to settle a class-action lawsuit in addition to its damaged public image.[61]

During 2014, Home Depot payment terminals had been compromised over a 5-month period after being infected with custom-built malware.[62] "Home Depot estimated the investigation, credit monitoring service, call center staffing and other steps would cost $62 million, offset by $27 million it expects to be reimbursed by its insurance."[63]

In late 2014, Sony Pictures Entertainment was the victim of a widely publicized cyberattack which "laid bare not just weaknesses in corporate Internet security but major shortcomings in how the government and companies work together to respond to attacks."[64] The company's public response to the hack was ham-handed, to say the least, and, entirely apart from scrutiny of its data security, resulted in embarrassing disclosures for the company and its executives.[65]

In early 2015, health insurer Anthem, Inc. was a victim of a massive

---

60. Greg Wallace et al., *Target: 40 Million Credit Cards Compromised*, CNN MONEY, Dec. 18, 2013, http://money.cnn.com/2013/12/18/news/companies/target-credit-card/ (last visited Apr. 26, 2015).

61. Sarah Halzack, *Target Data Breach Victims Could get up to $10,000 each from Court Settlement*, WASH. POST, Mar. 19, 2015, http://www.washingtonpost.com/news/business/wp/2015/03/19/target-data-breach-victims-could-get-up-10000-each-from-court-settlement/ (last visited Apr. 25, 2015).

62. Robin Sidel, *Home Depot's 56 Million Card Breach Bigger Than Target's*, WALL ST. J. (Sept. 18, 2014), *available at* http://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571.

63. *Id.*

64. Devlin Barrett & Danny Yadron, *Sony, U.S. Agencies Fumbled After Cyberattack*, WALL ST. J., Feb. 22, 2015, at B1.

65. *See, e.g.*, Michael Cieply & Brooks Barnes, *Sony Hack Reveals Email Crossfire Over Angelina Jolie and Steve Jobs Movie*, N.Y. TIMES (Dec. 10, 2014), http://www.nytimes.com/2014/12/11/business/media/emails-from-hacking-reveal-sonys-dirty-laundry.html (last visited Apr. 26, 2015); *Sony Film Executives Apologize for Racially Tinged Emails about Obama*, N.Y. TIMES (Dec. 11, 2014), *available at* http://www.nytimes.com/2014/ 12/12/business/media/scott-rudin-and-amy-pascal-of-sony-apologize-for-racially-tinged-comme nts-on-obama.html (last visited Apr. 26, 2015); Daniel Miller, *Future of Sony's Amy Pascal Questioned After Hacked Email Revelations*, L.A. TIMES (Dec. 11, 2014), http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-sony-amy-pascal-apologizes-20 141212-story.html (last visited Apr. 26, 2015).

breach.[66] The company admitted that "8.8 million to 18.8 million people who were not its customers could be victims in the attack."[67] It was later revealed that the company had "stored the Social Security numbers of 80 million customers without encrypting them," in part due to the difficulty in accessing encrypted information.[68] Under HIPAA, covered entities are required to "address" encryption in their business operations but are not required to encrypt data if they determine doing so would impose an unreasonable burden.[69] However, the Health and Human Services' Office for Civil Rights, which enforces HIPAA regulations

> has imposed penalties or reached settlements in 24 data-breach cases in recent years, including . . . Humana Inc. agree[ing] to pay $1.7 million after an unencrypted laptop was stolen from one of its facilities . . . [and] QCA Health Plan Inc. agree[ing] to pay $250,000 to settle potential HIPAA violations after an unencrypted laptop containing information on 148 individuals was stolen.[70]

Many more data breaches have occurred, but these are a few of the more high-profile incidents that have been made public.

III. SOLUTIONS

I have provided a small sample of the regulatory regimes of corporate compliance as well as a small sample of corporate compliance failures. This section will suggest how technological tools can be used to complement and promote the human element of an ethical business culture.

A. *What Scope Should a Compliance Program Have?*

Any sophisticated compliance program will necessarily integrate other technologies used by the company. If employees in a small company communicate primarily through email, then the company's compliance program may only need to include a basic policy on emails. Conversely, a large institutional investment firm conducting thousands of

---

66. Caroline Humer, *Anthem Says at Least 8.8 Million Non-Customers Could be Victims in Data Hack*, REUTERS (Feb. 24, 2015), http://www.reuters.com/article/2015/02/24/us-anthem-cybersecurity-idUSKBN0LS2CS20150224 (last visited Apr. 25, 2015).

67. *Id.*

68. Danny Yadron & Melinda Beck, *Anthem's Records Weren't Encrypted*, WALL ST. J. (Feb. 5, 2015), http://www.wsj.com/articles/investigators-eye-china-in-anthem-hack-1423167560 (last visited Apr. 26, 2015).

69. *Id.*

70. *Id.*

transactions each day should have a system in place that can keep pace with and monitor such complex interactions if it wishes to keep abreast of emerging risks (*i.e.*, the scope and sophistication of a firm's compliance program should be proportional to the scope and sophistication of its technological capabilities and tailored to its specific business). This should be fairly obvious but is worth mentioning because many companies fail to account for their firm-specific risks, and even outside "experts" may not adequately understand the nature of the business in order to offer competent advice. Any firm's unique risk set makes up its "Risk Profile."

A company's Risk Profile can change over time. A compliance strategy should be regularly updated to account for changes in market conditions, company strategy, capital structure, or overseas expansion, for example.

B. *Managing Risk During Recruiting and Hiring*

The corporate machinery only works through its officers, directors, and employees. If not for their actions, the corporation could not grow or transact business.[71] Any compliance program is similarly impotent unless the employees are made aware of it, convinced of its utility, and faithfully adhere to its tenets and policies. Any compliance failure can ultimately be traced to choices made by the same people the company must entrust with running its compliance program. It follows that being selective in hiring is important to a compliance program's success.

Technology can and should be utilized as a gatekeeping device at the threshold of employment. Employee criminal background checks are a fairly routine part of the hiring process. Convictions for crimes involving dishonesty, fraud, or crimes involving computers are a red flag, especially if a firm does business abroad or handles private information. However, a criminal history should not automatically preclude an applicant from a job opportunity unless the nature of the crime has some bearing on the work to be done or the performance to be expected, or the employer could fall afoul of applicable labor laws.[72]

People put more personal information online now than ever given the prevalence of Facebook and Twitter, to name two popular platforms. Seeking more information about applicants, some companies have requested they turn over their usernames and passwords for their online

71. *See* White v. State, 160 So. 2d 496, 501 (Ala. Ct. App. 1964) ("A corporation, being persona ficta, an artificial being, exists, in legal theory, only through the acts of its alter ego or its agents, servants, employees, officers or directors which can be attributed to it.").

72. *See* Press Release, U.S. Equal Employment Opportunity Commission, EEOC Files Suit Against Two Employers for Use of Criminal Background Checks (June 11, 2013), *at* http://www.eeoc.gov/eeoc/newsroom/release/6-11-13.cfm.

profiles.[73] It seems natural for an employer to wonder if a potential employee has "anything to hide," but as is the case with any background check, a hiring manager must take care not to be biased against an applicant due to information he or she is not entitled to have or consider during the hiring process (*e.g.*, race, marital status, or religious affiliation). Many privacy advocates (and job applicants) have decried asking for the keys to information of such a personal nature.[74] Several states have banned the practice.[75]

That is not to say that investigating an applicant beyond the materials he submits for consideration is inadvisable. Looking into a person's social network can unearth potential conflicts of interest or relationships that might be considered suspicious.

A company hiring foreign nationals should consult the Specially Designated Nationals List maintained by the Office of Foreign Assets Control:

> As part of its enforcement efforts, OFAC publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific. Collectively, such individuals and companies are called "Specially Designated Nationals" or "SDNs." Their assets are blocked and U.S. persons are generally prohibited from dealing with them.[76]

Doing business with persons on the list is *per se* a violation of federal law, but there may be mitigating circumstances if the only reference to the person on the list is a "weak AKA," (a relatively broad or generic alias)[77] the person involved in processing the search had no reason to

---

73. Shannon McFarland, *Job Seekers Getting Asked for Facebook Passwords*, USA TODAY (Mar. 21, 2012), http://usatoday30.usatoday.com/tech/news/story/2012-03-20/job-applicants-facebook/53665606/1 (last visited Apr. 26, 2015).

74. *See, e.g.*, Anita Ramasastry, *Can Employers Legally Ask You for Your Facebook Password When You Apply for a Job?*, VERDICT: JUSTIA.COM (Mar. 27, 2012), https://verdict.justia.com/2012/03/27/can-employers-legally-ask-you-for-your-facebook-password-when-you-apply-for-a-job (last visited Apr. 25, 2015).

75. Jonathan Dame, *Will Employers Still Ask for Facebook Passwords in 2014?*, USA TODAY (Jan. 10, 2014), http://www.usatoday.com/story/money/business/2014/01/10/facebook-passwords-employers/4327739/ (last visited Apr. 25, 2015).

76. Specially Designated Nationals List, U.S. Dept. Treas., http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx.

77. Recent OFAC Actions - SDN Alias Screening Expectations, U.S. Dept. Treas., http://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/weak_strong_alias.aspx.

> A "weak AKA" is a term for a relatively broad or generic alias that may generate

know the individual was on the list, and the person maintains "a rigorous risk-based compliance program."[78]

Personality tests for applicants can be administered quickly and cheaply online rather than in-person testing, and have become increasingly common.[79] The objective of any such testing program should be to identify and weed out potential bad actors with a penchant for fraud or other misconduct that might violate an ethical compliance program.

C. *Orientation for New Employees and Promoting a Culture of Compliance*

Once brought into the fold, employees need to be oriented with the company's ethics or compliance program. The initial training should be substantial and commensurate with the Risk Profile of the firm. The compliance policy itself should not merely be a static "paper" policy. It should be introduced and then reinforced.

Initial orientation should by no means be the only exposure employees have to compliance training. An employee who does not feel like he is a part of an ethical culture is less likely to feel compelled or obligated to behave ethically. Dan Ariely is the James B. Duke Professor of Psychology and Behavioral Economics at Duke University and a founding member of the Center for Advanced Hindsight.[80] His research suggests that subtle reminders to behave (asked to recall the Ten Commandments, or being reminded of a university's honor code, for example) reduced occurrences of dishonesty when test subjects were asked to self-report their performances on a simple test, whereas people without any reminder would consistently inflate their scores.[81] On the other hand, witnessing someone else cheat, benefit, and avoid any adverse consequence resulted in more dishonest behavior.[82]

> a large volume of false hits. Weak AKAs include nicknames, noms-de-guerre, and unusually common acronyms. OFAC includes these AKAs because, based on information available to it, the sanctions targets refer to themselves, or are referred to, by these names. As a result, these AKAs may be useful for identification purposes, particularly in confirming a possible "hit" or "match" triggered by other identifier information. Realizing, however, the large number of false hits that these names may generate, OFAC qualitatively distinguishes them from other AKAs by designating them as weak.

Id.

78. *Id.*

79. *See* Kimberli R. Black, *Personality Screening in Employment*, 32 AM. BUS. L.J. 69, 69 (1994) (citing a survey showing that 46% of employers use some type of personality testing).

80. Dan Ariely, Blog, http://danariely.com/ (last visited Apr. 25, 2015).

81. *See* Dan Ariely, Tag: Cheating, http://danariely.com/tag/ cheating/ (last visited Apr. 25, 2015).

82. Dan Ariely, Blog, "Taxes and Cheating," http://danariely.com/ 2012/04/10/taxes-and-

This ethical dynamic is the reason "tone at the top" is such a popular phrase in corporate compliance.[83] In the United States, if the modern age of corporate regulation began with the Securities Act of 1933 and the Securities Exchange Act of 1934, then the post-modern era can arguably be traced to the Enron scandal. That firm's meteoric rise and fall is described in a case study by Malcom S. Slater:

> Until its collapse in the fourth quarter of 2001, Enron Corporation was the world's dominant energy trader, accounting for about one-quarter of all energy trading in the United States. By pioneering the development of large-scale energy trading, Enron was able to transform itself from an "old economy" gas pipeline operator to a "new economy" financial intermediary and market maker. In the process, Enron's revenues grew from $3.5 billion in 1991 to a reported $10.8 billion 10 years later. During the last five years of the millennium, Enron delivered a 507% total return for its shareholders, and for many years it was a regular and prominent member of published lists of America's most admired and innovative companies. At the beginning of 2001, Enron's market capitalization was $62.5 billion. One year later Enron's stock was worth only pennies to its unfortunate shareholders, and the company held (at the time) the dubious distinction of being the largest bankruptcy in American economic history.[84]

One of the main problems leading to Enron's collapse was its corporate culture. Risky behavior was incentivized, sound accounting methods were discarded, and the company's stock price was the primary, if not sole, focus of many business decisions.[85] This corporate culture, or attitude, directly emanated from the company's CEO, Kenneth Lay, by all accounts an aggressive and risk-taking personality himself.[86]

In retrospect, if "tone at the top" has a real influence on a corporation's ethical culture, the downfall of Enron was predictable. If compliance training only occurs at the beginning of a term of employment, a company risks not having an effective program. Rather, compliance training should

---

cheating/ (Apr. 10, 2014) (last visited Apr. 26, 2015) ("Seeing someone cheat for their own benefit and then get away with it clearly has an impact on our moral behavior—loosening it to a substantial degree.").

83. Francesca Gino et al., *Contagion and Differentiation in Unethical Behavior*, 20 PSYCHOL. SCI. 393, 397 (2008) ("The results of the two experiments show that people react to the unethical behavior of others, and that their reaction depends on the social norms implied by the observed dishonesty and also on the saliency of dishonesty.").

84. Malcom S. Salter, *Innovation Corrupted: The Rise and Fall of Enron*, 1 (Harvard Bus. Sch. Case 905-048, Dec. 2004) (Rev. Oct. 2005).

85. *Id.*

86. *Id.*

be recurring and reminders that the company is fostering an ethical culture should be frequent. The board of directors should also attend regular compliance training. Any existent compliance risks should be brought to the employees' attention and they should be briefed on new or emerging compliance risks. Most importantly, management needs to be committed to fostering a culture of compliance and leading by example.

Even if an ethical culture is fostered, compliance decisions should not be left up to individual employees. Discretion should be limited, clear reporting channels should be identified, and anonymous complaints should be allowed, if not encouraged.

Technology can assist at all stages of compliance promotion and enforcement. Training (or periodic re-training) can be conducted online using training (or more creative) videos rather than in-person sessions.[87] Regular emails (*e.g.*, newsletters) can highlight both bad (creating risk) and good (minimizing risk) behavior within the company and reinforce the company's ethical culture.

D. *Monitoring Business Relationships*

The employees in a multinational enterprise with the highest risk profile are those involved in sales and forming new business relationships. Because the FCPA and other regulations broadly define who can be the recipient or payer of an official bribe, it may not be obvious or apparent that a potential business partner poses a compliance risk.

Any potential new business partner (*e.g.*, supplier, distributor, manufacturer, retailer) must be vetted and a risk-assessment should be performed. A compliance program should be concerned with who is involved with the potential partner and whether there is any affiliation (direct or indirect) with a foreign government.[88] A comprehensive analysis of risk may not be possible if the people in charge of a compliance program are not familiar with the business culture of the market to be entered.[89] Employees responsible for dealing with these people should be absolutely clear that the FCPA and other regulations broadly cover gifts of all kinds, including entertainment and travel

87. *See, e.g.*, Dan Heath & Chip Heath, *How to Make Corporate Training Rock*, Fast Company (Dec. 1, 2009), *at* http://www.fastcompany.com/1460648/how-make-corporate-training-rock (last visited Apr. 26, 2015).

88. *See* Stephen Clayton, *Top Ten Basics of Foreign Corrupt Practices Act Compliance for the Small Legal Department*, Association of Corporate Counsel (June 1, 2012), *at* http://www.acc.com/legalresources/publications/topten/SLD-FCPA-Compliance.cfm (last visited Apr. 25, 2015).

89. *See* Kimberly S. Johnson, *Career Builder: a Stint Abroad*, WALL ST. J., Feb. 10, 2015, at B7 ("Years spent in the trenches abroad can help an executive navigate cultural mores, regulations, and supply-chain disruptions").

accommodations, and should actively resist any proposed graft.

Third parties should also receive compliance training commensurate with the corporation's policies if due diligence suggests their practices may constitute a violation.[90] A potential business partner not willing to accommodate a comprehensive compliance program should raise a red flag and discourage a corporation from pursuing that business opportunity.[91] While others within the company may rue the lost opportunity, those in charge of compliance must frame the issue to management as a transaction (or transactions) that could end up as a substantial fine, or even criminal sanctions, if a violation occurs.

E. *Using Information Technology to Manage Data Streams*

Many essential business functions are not performed by people, but by computers. Developments in information technology have facilitated unprecedented levels of cross-border access, communication, and enterprise. While technology can be a boon to business, it can also facilitate wrongdoing.[92] The same technologies that increase a company's productivity and bottom line can be exploited, resulting in crushing liability.

While privacy activists and employees may be troubled by what they perceive as a slippery slope (or an already outrageous overreach into employees' lives), a company should monitor the activities of its employees. The extent to which employees should be monitored is determined by what information they may have access to.

Many corporate employees may receive a device (cell phone) for business use. If they also have a personal cell phone, they would have to carry two devices. Many companies have so-called bring your own device policies to avoid that problem, but such a policy, while placating employees who may prefer their iPhone to a company-issued Blackberry, introduces difficult security challenges for those in charge of protecting company data.[93] Blurring the line between business and personal use of a cell phone or tablet could result in carelessness, malware infection, and

---

90. Clayton, *supra* note 88.

91. *See* Amanda McGraw, *How to Identify the 14 Red Flags of Ethical Misconduct & Mitigate Them with Your Compliance Training Program* (Sept. 18, 2014), https://www.tnwinc.com/9832/red-flags-ethical-misconduct-compliance-training-program-part-1/ (last visited Apr. 25, 2015).

92. *See* Marc Goodman, Op-Ed., *How Technology Makes Us Vulnerable*, CNN.COM (July 29, 2012), http://www.cnn.com/2012/07/29/opinion/goodman-ted-crime/ (last visited Apr. 25, 2015) ("The criminal underground is highly innovative and often acts as an early adopter of emerging technologies.").

93. *See* Gene Marks, *Do You Really Need a BYOD Policy?*, FORBES.COM (Feb. 25, 2013), http://www.forbes.com/sites/quickerbettertech/2013/02/25/do-we-really-need-a-byod-policy/ (last visited Apr. 24, 2015).

the company's (or customers') data being compromised.

Any personal device used to transact company business should be monitored (*e.g.*, through a firewall filter). Incoming and outgoing communications may be benign, but if they are not, a company may be found liable if it should have known the communications were facilitating an illicit payment or data breach. Communications should be screened for common code words used to conceal bribes.[94] These filters can be set up to be automated, minimizing the human eyes that may view any single communication and mitigating privacy concerns.

Segregating personal and business functions on a personal device is technically difficult, and there is no product currently on the market that would allow a company to partition[95] the device and segregate its respective functions. However, technology does exist that would alter the way a phone functions. A British company, Bibitel, offers a "skin" that goes over an existing SIM card, permitting cheaper international phone calls.[96] If employees want to use their own devices, this may offer a compromise, keeping the functionality of a device that a user enjoys while offering a degree of customization over how communications are sent and received and through which, if any, filters those communications may pass.

Encryption of personal data of customers or others makes the data safer but also makes it more difficult to access and use. As discussed above, HIPAA, for example, does not *require* encryption, but failure to encrypt data may result in liability.

Tokenization offers a third-party solution to data protection. The personal information that a company collects should be limited to what the company actually needs. For example, if a person's driver's license number is gathered in order to verify his identity but is not needed for any other purpose, then that information should not be retained since keeping it only adds risk. Of course, some personal data must be retained. A merchant may retain the credit card numbers of customers who make frequent purchases as a convenience, for example. Rather than keep a database of customers' names along with credit cards, the credit card numbers can be masked using "tokenization."[97]

---

94. *See* James Rough, *Red Flag Account Descriptions Used to Conceal Bribes*, Arizona Chapter of Certified Fraud Examiners, http://www.navigant.com/insights/library/disputes-and-investigations/2013/red-flag-account-descriptions-used-to-conceal-bribes/ (last visited Apr. 26, 2015).

95. *See* Margaret Rouse, "Partition," TechTarget, http://searchstorage.techtarget.com/definition/partition (last visited Apr. 25, 2015) ("In personal computers, a partition is a logical division of a hard disk created so that you can have different operating systems on the same hard disk or to create the appearance of having separate hard drives for file management, multiple users, or other purposes.").

96. Bibitel, Sim Skin, *at* http://www.bibitel.com/.

97. Bruce Upbin, *Tokenization and the Collapse of the Credit Card Payment Model*, Forbes

The process substitutes identifying information for a "token" (a unique, identifying number, or piece of data, that by itself does not identify anyone) that the company retains in a database. For example, if a transaction using a person's credit card needs to be processed, the corporation can submit the token to a third party service that stores personal information and retrieve the required data in exchange.[98] Because the token does not directly relate to the customer's data, if a hacker or wrongdoer obtains the token, no personal information is compromised, and the data of the token itself has no intrinsic value.[99]

Despite best efforts to prevent them, a company may have a duty to acknowledge its failures and notify those whose information was compromised by a security breach. Any delay or inefficiency in this process can have an adverse effect on business or public perception.[100] To quickly respond to a data breach, a company needs to have a plan in place with the technical ability to diagnose the extent of a breach and execute the remedial plan.

IV. CONCLUSION

Corporate compliance is here to stay, and if regulations and fines are forthcoming, so will be the money spent by firms to limit their liability. Corporate counsel, if it does not have the ear of the CEO or upper management, should grab hold. Management may not be actively concerned about compliance but they need to be convinced of its utility and necessity.

Both technological and human solutions are necessary because each is dependent on the other. Having a compliance program tailored to each individual business is the ideal way to mitigate risk. Risk management begins before employees are hired and may not end until long after an employee is terminated or leaves the company. By creating efficiencies and synergies in the compliance program that are complementary and not counterproductive to business operations, corporate counsel or a compliance officer can justify the costs of any compliance program by vividly describing the costs of non-compliance. The movement embracing corporate social responsibility and increasing enforcement

---

(Feb. 15, 2013), http://www.forbes.com/sites/bruceupbin/2013/02/15/tokenization-and-the-collapse-of-the-credit-card-payment-model/ (last visited Apr. 25, 2015).

98. *Id.*

99. *Id.*

100. *See, e.g.*, Catey Hill, *Home Depot's Data Breach is Worse than Target's, So Where's the Outrage?*, MARKET WATCH (Sept. 25, 2014), http://www.marketwatch.com/story/yawn-who-cares-about-home-depots-data-breach-2014-09-24 (last visited Apr. 25, 2015) ("Target took a while (about a week) after learning of the potential breach to address consumers, while Home Depot acted more quickly (within about a day of when it learned about it).").

actions will exist for the foreseeable future. Companies that fail in their duties will not.