March 2015

In This Issue
Message from the Chair
Compliance Officers and Personal Liability: Could this be the Riskiest Corporate Job?
Lessons to Be Learned from the Sony Breach
Why Culture Trumps Compliance
Editor's Corner
Committee Leadership Roster

Important Dates
2015 Business Law Section Spring Meeting
April 16-18, 2015
San Francisco, CA

Editorial Board
Alan Gutterman

Message from the Chair

Dear Corporate Compliance Committee members,

The Spring Meeting in San Francisco is fast approaching. The advance registration deadline is Friday, March 27. You may register here. On-site registration will be available, of course.

Our Committee has numerous events planned, and I encourage you to attend.

Thursday, April 16, 10:30-12:30 am PT - CLE Program: "Avoiding Hiring and Firing and Wage and Hour Problems: A Program of the Corporate Counsel Triage Series." We are co-sponsoring this program by the Middle Market and Small Business Committee

Thursday, April 16, 2:30-4:30 pm PT - CLE Program: "International Trade Compliance for the Business Lawyer." I will chair the panel, and we will have in-house counsel from Bank of America and Cigna, as well as outside counsel from Crowell & Moring LLP, to provide a great primer on international trade law (sanctions, export controls, anti-boycott, etc.) and a particular focus on how these issues arise in transactions and how to manage them.

Thursday, April 16, 4:30-5:30 pm PT - Corporate Compliance Committee Business Meeting. There will be a conference bridge line for those who are unable to join in person.

Friday, April 17, 10:30 am - 12:30 pm PT - CLE Program: "Illegal Touchdown! (Un-)ethical Behaviors, Compliance, Risk Management and Dispute Resolution in the Modern World of Sport." We are co-sponsoring this program by the Business and Corporate Litigation Committee.

Saturday, April 18, 8:00-10:00 am PT - CLE Program: "A Tale of Two Cities: Legal Ethics and Business Ethics." We are co-sponsoring this ethics CLE by the Business Law Education Committee.

I hope you are able to join us in San Francisco in a few weeks to participate in these and the many other events on offer. The Section staff has put together a great meeting for us.

Thank you for your continued support of the Committee.

Best regards,
Brian T. Sumner
Chair

Compliance Officers and Personal Liability: Could this be the Riskiest Corporate Job?
By Ted Banks

In December 2014, a 57-page complaint filed by the U.S. Attorney in Manhattan sought to impose personal liability on the former compliance officer for MoneyGram International, Thomas Haider. It alleges that he willfully or recklessly failed to stop money laundering activities. The complaint seeks a fine of $1 million and would bar Haider from working in financial services. The case is unusual because, in 2012, the government negotiated a deferred prosecution agreement with MoneyGram. Actions against compliance officers are relatively rare, although prosecutions against the “responsible corporate officer” for illegal activity of a corporation are clearly part of a prosecutor’s enforcement toolbox. See, e.g., United States v. Park, 421 U.S. 658 (1975).

Regardless if the case represents a new trend in government enforcement, it does contain important lessons for all compliance officers:

- Compliance officers who actively participate in schemes to violate the law face liability. This often includes cover-up activities by the compliance officers. This is no surprise in any area.
- If you are a compliance officer, you have an obligation to ensure that your company is following the compliance program. A "paper program" does not provide any protection at all. Compliance officers cannot passively allow the compliance program to be ignored. For example, in United States v. Caputo, 456 F. Supp. 2d 970 (N.D. Ill. 2006), the evidence showed a scheme to evade regulations by the CEO. The compliance officer was chosen because the CEO knew that he could dominate him, and wouldn’t need to worry about being pushed to actually follow the law.
- The government may be learning that one of the most powerful deterrent tools is prosecution of individuals. The people who commit the violation must be convinced that they will personally pay the price for violations for which they are responsible. Violators should be subject to fines, jail, loss of industry employment, and public shaming. If corporations just pay a fine and make promises to be good, the individuals who were behind the violation have little incentive not to do it again.

What does this all say to compliance officers? If you are responsible for a compliance program, make sure it is working. The program design must be effective, and not just look good on paper to the uninitiated. If the program design is good, it must be implemented by the company, and not frustrated by inadequate resources or management evasion.

If you cannot design or implement an effective program, it is not enough to stay in the job as compliance officer just to "fight the good fight." If the company won't comply, and you know about it, it is time to leave. And for a lawyer, that may mean a "noisy withdrawal."

Ted Banks is a partner in the firm of Scharf Banks Marmor LLC in Chicago. He has been involved in corporate compliance for more than 35 years, and is the editor the Corporate Legal Compliance Handbook, published by Wolters-Kluwer. He teaches compliance law at the Loyola University School of Law, and serves as a compliance monitor for the Federal Trade Commission and the Competition Bureau of Canada. tbanks@scharfbanks.com

---

Lessons to Be Learned from the Sony Breach

By Kirk J. Nahra

Many data breaches generate significant media attention, but we have never seen the kind of impact from an information security breach that we have from the continuing fallout from the breach involving Sony. We’ve had national security implications, large-scale international negotiation and sanctions issues, enormous commercial fallout, and widespread personal embarrassment from business activities, all along with the "normal" fallout involving personal data of
various kinds. And this situation has not yet ended, and may continue almost indefinitely as data continues to spill out from the hackers (whoever they turn out to be).

So, what are the major lessons from this situation?

All companies have data security risks

Sony isn't a financial services company. It isn't a health care company. And, therefore, it isn't required to meet specific and detailed regulatory requirements for data security involving personal data (yes, I know there are exceptions such as the Massachusetts state law, but work with me on this one). At a minimum, we don't think of Sony as a company that uses large volumes of personal data about its consumers or that faces specific regulatory requirements for data security.

But the fact of the matter is—as this breach shows—that virtually every employer has volumes of data about employees, and, because of the "big data" phenomenon, more and more companies also have detailed facts about clients, consumers, business partners and other individuals. Every company has this information. And all of them are subject to breaches, from a growing variety of causes. The conclusion is that every company that, at a minimum, has employees and/or customers must care about data security, at least from a compliance perspective.

Read more...

Why Culture Trumps Compliance

By Stephen M. Paskoff

On July 30, 2014, the Wall Street Journal reported the following on a recent meeting of the New York Fed: "Thomas Baxter, Executive Vice President and General Counsel of the New York Fed, stressed at the outset of his remarks that he was only speaking for himself, but he pointedly critiqued company culture, saying that if a firm's values don't support the rules used to guide employee behavior, the organization 'is headed for troubled territory.'"

Mr. Baxter is right on the money. His statement applies not only to banking but also to other types of businesses. NAVEX Global recently released a survey reporting that most compliance officers have shifted to transforming culture as opposed to simply - and it is relatively simple - educating employees on applicable regulations. This is a welcome development. Unfortunately, it's happening a little too late for organizations like General Motors and the Veterans Administration.

In 2002, I met with the number two aide to one of the nation's top general counsels. We were discussing how his organization would comply with the newly-enacted Sarbanes Oxley Act, which introduced major changes to the regulation of financial practices and corporate governance requirements. What he told me that day proved to be a common organizational approach. He said his organization planned to communicate basic standards and document leader and employee receipt. The company's leaders had concluded getting material out broadly, not whether it had impact, was all that needed to be done.

I thought his employer and others following the same course had made a grievous mistake. And, history has made it clear that they did. Time after time, organizations with supposedly robust compliance mechanisms have proven their systems to be as effective as paper shuffling. They've become prey to gross violations that all of their policies, actions, and public commitments promised would never happen.

Compliance initiatives based solely on systems, processes, memos, and other activities - which are largely ignored - tell people what to do; but it's organizational culture that determines what people actually do. Culture is derived by what people see being done by those they respect and, frankly, may
fear. It's based on how individuals are rewarded or punished when they meet or breach key values. This varies from organization to organization: I know one company that fires anyone who lies on an expense report, no matter how high up the chain they are; another allows employees to cut corners on business deals and deceive clients as long as they meet their financial goals. The reality is people violate rules all the time and either don't believe they'll be caught or get into trouble if they are.

Thus, culture represents the way organizational values are actually lived, not the words by which they are expressed. And, a healthy organizational culture won't take root by forcing employees to sign documents they've barely read and that are ignored by individuals who control their workplace opportunities and futures. Defining clear principles on paper is a first step, but that's all it is.

To instill ethical behavior, organizations must provide incentives and encourage everyone to not only act properly but also to report violations. And, they need to recognize and, perhaps, reward people when they do. That's the strategy banks, auto manufacturers, healthcare institutions, government agencies, etc., should follow if they're serious about making ethical choices, welcoming values, and having daily meaning. It's much bigger than just handing out compliance-worthy statements and having employees check the box.

Stephen M. Paskoff, Esq., is the founder, president and CEO of ELI®, a training company that teaches professional workplace conduct, helping clients translate their values into behaviors, increase employee contribution, build respectful and inclusive cultures, and reduce legal and ethical risk. In addition, Mr. Paskoff is the former Co-Chair of the ABA's Compliance Training and Communication Subcommittee, which explores best practices in training methodology as well as overall strategies for implementing learning and communication plans to maintain corporate compliance.

Editor's Corner

By Alan S. Gutterman

Welcome to our first Committee Newsletter of 2015. I am the Newsletter Editor and I'm writing to seek your contributions for future issues, which we plan to publish on a quarterly basis. We invite you to submit relatively short pieces, perhaps 300 to 500 words, on topics of interest to our members. In addition, we are open to longer articles if you are so inclined. If you have something you'd like to share, please contact me at my e-mail address below. Many thanks in advance and we hope you enjoy the information we've provided in this issue.

Alan S. Gutterman is the Publications Chair of the Corporate Compliance Committee and can be reached at agutterman@alangutterman.com. He is the Director of the Growth-Oriented Entrepreneurship Project (www.growthentrepreneurship.org) and the Business Counselor Institute (www.businesscounselorinstitute.org) and is also Of Counsel to Qian & Company, a California Professional Law Corporation headquartered in San Francisco. Readers interested in compliance-related materials developed and distributed by Mr. Gutterman should contact him at the address above.

Committee Leadership Roster

Chair: Brian T. Sumner (brian.sumner@alcoa.com)

Subcommittees

Compliance Program Organization & Implementation
Chairs: Timothy M. Moore (tmoore@shb.com), Ann Straw (ALStraw@vcnainc.com)

Vice-Chairs: Dave Ackerman (dacker6@pride.hofstra.edu)

Compliance Training & Communications

Chairs: Theodore L. Banks (tbanks@scharfbanks.com), Stephen M. Paskoff (Paskoff@eliinc.com)

Vice-Chairs Michael L. Schuman (mschuman@schiffhardin.com), Ricardo Aponte (raparsi@gmail.com; Ricardo@iss-pr.com)

Information Governance

Chairs: Michael J. Green (michael.green@gcinc.com), Peter F. McLaughlin (peter.mclaughlin@dlapiper.com), Kirk Nahra (knahra@wileyrein.com)

Vice-Chairs: Eleni Koulourioti (eleni.koulourioti@db.com)

Internal Investigations

Chairs: James M. Lord (jlord@sideman.com)

Vice-Chairs: Timothy M. Moore (tmoore@shb.com)

Publications

Chair: Alan S. Gutterman (agutterman@alangutterman.com)

Vice-Chairs: Michael L. Schuman (mschuman@schiffhardin.com)

Risk Management

Chairs: Margaret Cassidy (m.cassidy@cassidylawpllc.com), Tovah Nadassky (tovah.nadassky@hotmail.com)

Task Forces

Administrative Directors

- *Content: Peter F. McLaughlin (peter.mclaughlin@dlapiper.com)
- Diversity: Ricardo Aponte (raparsi@gmail.com; Ricardo@iss-pr.com)
- International Coordinating: Eleni Koulourioti (eleni.koulourioti@db.com)
- *Programs: Brian T. Sumner (brian.sumner@alcoa.com)
- *Publications and Business Law Today: Alan S. Gutterman (agutterman@alangutterman.com)
- *Technology: Dave Ackerman (dacker6@pride.hofstra.edu)
Lessons to Be Learned from the Sony Breach

By Kirk J. Nahra*

Many data breaches generate significant media attention, but we have never seen the kind of impact from an information security breach that we have from the continuing fallout from the breach involving Sony. We’ve had national security implications, large-scale international negotiation and sanctions issues, enormous commercial fallout, and widespread personal embarrassment from business activities, all along with the “normal” fallout involving personal data of various kinds. And this situation has not yet ended, and may continue almost indefinitely as data continues to spill out from the hackers (whoever they turn out to be).

So, what are the major lessons from this situation?

**All companies have data security risks**

Sony isn’t a financial services company. It isn’t a health care company. And, therefore, it isn’t required to meet specific and detailed regulatory requirements for data security involving personal data (yes, I know there are exceptions such as the Massachusetts state law, but work with me on this one). At a minimum, we don’t think of Sony as a company that uses large volumes of personal data about its consumers or that faces specific regulatory requirements for data security.

But the fact of the matter is—as this breach shows—that virtually every employer has volumes of data about employees, and, because of the “big data” phenomenon, more and more companies also have detailed facts about clients, consumers, business partners and other individuals. Every company has this information. And all of them are subject to breaches, from a growing variety of causes. The conclusion is that every company that, at a minimum, has employees and/or customers must care about data security, at least from a compliance perspective.

This isn’t news—the Federal Trade Commission (FTC) has taken the position for more than a decade that every company with employees or customers has specific data security requirements.¹ It’s just that many companies don’t listen if there isn’t a specific law, often until it is too late.

Even for those companies that don’t recognize their risks and obligations for personal data, the Sony breach drives home that there is much more to worry about than protecting personal data. The laws focus on personal data—Congress and the FTC don’t (generally) care if companies don’t protect their own commercial information. But the Sony breach makes clear that this commercial data is (1) valuable; (2) at risk; and (3) can subject the company to enormous problems, even if “compliance” isn’t one of them. For those companies where the threat of an FTC enforcement action isn’t enough, the risks related to corporate data—something every company has—should drive this emphasis home even more.

**There’s “data security” and “cyber security”**

One reason that the Sony breach caught so much public attention is because of the national security and diplomatic implications of the breach. These risks—which have little to do with personal data—demonstrate why there is a separate debate building in Congress and elsewhere about “cybersecurity.” The data security regime is well established, and continues to expand, but those
requirements focus on specific kinds of personal data and the risks to individuals in connection with breaches involving that data.

Cybersecurity, meanwhile, focuses more on the interconnections between companies and systems, and the potential concerns to the country and on a broader basis from cybersecurity attacks. The key provisions of federal law and policy for cybersecurity deal with “critical infrastructure,” a broad category of companies that are included by virtue of the role they play in our country. Some of these industries—like health care and financial services—are included in both data security regulatory regimes and cybersecurity. Others (e.g., chemical and power companies) are only (or primarily) affected by cybersecurity. And while cybersecurity focuses on the national security impact of potential cyber-attacks, the Sony attack should push companies on a much broader level to apply strong and effective cybersecurity controls, even where not required by law.²

Many information security risks aren’t “legal” or compliance related

While Sony may face regulatory action and (already) faces lawsuits from former employees, much of the negative attention for Sony and negative business implications have nothing to do with personal data. All of Sony’s proprietary information is at risk. One movie was affected in significant ways, and many others may be affected going forward. Senior executives faced personal and business complications from release of business communications. None of these “injuries” is what either data security laws or cybersecurity principles are designed to address. Yet, these are an important reminder of how important it is to protect technology infrastructures, even without facing any regulatory or enforcement pressure.

The compliance risks also matter

Most of the attention to security breaches in recent years has involved personal data—credit cards, Social Security numbers, or medical information that can cause specific financial or other harms to individuals. While there is no reason to think that this attack on Sony was driven by this personal data, the personal information clearly is affected, and a large number of employees (and perhaps consumers) face potential harms as a result of the attack. Already, Sony faces a lawsuit from former employees. Other suits may follow. We can expect various investigations, some of which may focus on personal data. While it is not clear that Sony violated current information security standards, there have been various reports that Sony ignored earlier evaluations of their information security framework. This situation is a reminder of the importance of constant vigilance on information security, and the critical need to fix problems that have been identified. A failure to fix problems both exposes the company to actual risk of a breach, but also makes the impact from these follow-on legal claims much riskier.

Think about all the places your data is

Unlike most breaches, which tend to impact specific data or particular components of a company’s operations, the Sony breach is striking by its vastness. From media reports, there seems to be no part of the Sony information technology structure that was not affected. In that sense, this is not a typical case. But it should drive home for all companies the need to think about what data you have and where you keep it. Data obviously falls into many categories, including (at least) proprietary information, internal communications, customer data, and employee data. Each of these categories (and any others) has their own reasons for data being collected and stored, and often fits into company systems in different ways. Companies need to pay close attention to a variety of issues that impact how a potential
breach can affect a company—by restricting access to various categories of data, by effective retention policies that restrict how long data is kept (note that the lawsuit that has been filed by employees is in fact by former employees), and in how many places data is stored and retained. It is always important to review traditionally sensitive pieces of information (such as employee Social Security numbers or customers’ credit card numbers), and minimize as much as possible the places in a company where these data elements are kept. In my experience, I always find that companies, for example, have Social Security numbers about employees in a large number of places where there is no reason for the numbers to be there. Review your data carefully, and take steps now to restrict how a breach could affect you.

Learn from the mistakes of others

Every security breach connects to some root cause. It might be hackers, malware, insider problems, lost equipment, or otherwise. The true cause of the Sony attack is not yet clear, and may not ever be. But, every breach provides an opportunity for other companies to learn from the problems and/or failings of others. When you see reports of a security breach problem, think about what happened, and how that issue could arise at your company. Reading about lots of stolen laptops? Then make sure that your company’s employees know how to protect their laptops, are taught to reduce the information on them, and evaluate the now-typical approach of encrypting all laptops that contain sensitive data. Did your company face a loss of data because of malware sent through a fraudulent e-mail? Then train your employees better on these issues and implement better controls on these emails and the resulting harm. These breaches are a roadmap to how you best can protect your own company, and provide a partial framework for the ongoing need to re-evaluate security controls on an ongoing basis.

Don’t forget the insider risk

While the major focus of attention on the Sony breach has involved the alleged role of North Korea, there are lingering reports that the breach was caused by a disgruntled group of former employees. Whether this is true or not (or there is some other cause), this breach should serve as an important reminder of one of the most common sources of security breaches—action by insiders. Many of these “insider” breaches involve behavioral flaws—sloppy activity, a failure to recognize spoofing or other problem e-mails, loss of equipment, etc., which are mainly addressed through better training and smarter controls. In addition, we are seeing frequent and widespread problems where insiders with appropriate access to data are misusing that access for improper and often illegal purposes. We are seeing this problem arise from “lower level” employees (customer service reps, for example), who need access to perform their jobs but then misuse it. We are seeing more sophisticated breaches resulting from technical employees who have broad access to a wide range of data. These breaches can involve personal attacks on individuals, identity theft, health care fraud, and a wide range of other harms perpetrated by insiders. This is a real problem that exists in virtually every industry. Your company must have a plan for addressing these insider threats. This plan must involve (1) better controls on access; (2) education and training on appropriate use of information; (3) an effective employee sanction policy (employees must know that they will be sanctioned for these improper activities) and a real means of policing how employees are accessing data, through audit trails and the like. This problem exists and it creates realistic threats for all companies.

Conclusions
Each year, we have a range of security breaches that capture public attention. Last year, it was the Target breach. At the end of the year and carrying over into the beginning of 2015, the Sony breach is our focus. It is not always clear that this attention translates to action for companies who face these risks on an ongoing basis. It is clear that risks from outsiders are growing. It is also clear that there are a broad range of “other” threats that exist in most companies and that can be addressed to reduce risk. Whether driven by compliance concerns or a more general sense of risk management, companies in all industries need to take these threats seriously, and must engage in thoughtful, creative, and aggressive means of developing an effective approach to information security. These threats are not going away, and your risks will grow until you take smart steps to reduce them.

1 For a discussion of how every company is affected by data security requirements, please see Nahra, “Privacy and Data Security is for Everyone: Common Matters That All Companies Should Address,” Bloomberg BNA’s Corporate Law & Accountability Report (July 18, 2014), available athttp://www.wileyrein.com/publications.cfm?sp=articles&id=9895.  

* Kirk J. Nahra is a partner with Wiley Rein LLP in Washington, D.C., where he specializes in counseling and litigation on privacy, data security, cybersecurity and data breach issues. He represents companies across all industry segments, both across the country and internationally. He can be reached at 202.719.7335 or knahra@wileyrein.com, and follow him on Twitter @kirkjnahrawork.