29th Annual National Institute on White Collar Crime

The 29th Annual National Institute on White Collar Crime was held on March 4-6 in New Orleans. Criminal law experts, including representatives from the Department of Justice, weighed in on topics such as sentencing in white-collar crime cases, investigation and prosecution of international corruption, enforcement of securities and tax fraud, cybercrime, money laundering and asset forfeiture.

Please visit CJS YouTube (ABA/CriminalJustice) and Flickr (abacjs) pages for highlights of the conference.

Stakeholders Weigh In on Collateral Consequences at Summit

In celebration of the completion of the “National Inventory on the Collateral Consequences of Conviction,” the ABA Criminal Justice Section hosted the “National Summit on Collateral Consequences” on February 27, 2015 in Washington, D.C.. This one day Summit was held at the law offices of Jones Day near Capitol Hill, and featured expert presentations on a flagship Section issue.

The program featured an assortment of perspectives including: James Cole, former deputy U.S. Attorney General; U.S. District Judge Paul L. Friedman of the District of Columbia; Amy Solomon, senior advisor to the U.S. Department of Justice’s Assistant Attorney General; D.C. Superior Court Judge Michael L. Rankin; and ABA President William C. Hubbard.

Video highlights can be found on CJS “Collateral Consequences” playlist on YouTube.

MARK YOUR CALENDAR:

ABA/CJS Annual Meeting: July 30-Aug. 4, Chicago, IL


CJS 8th Annual Fall Institute: Oct. 22-25, Washington, DC

Inaugural Global White Collar Crime Institute: Nov. 19-20, Shanghai, China

The ABA Criminal Justice Section ...
Chair Felman Testifies Before U.S. Sentencing Commission

James E. Felman, Chair of the ABA Criminal Justice Section, testified on behalf of the Association, during a public hearing on the Proposed 2015 Amendments to the Federal Sentencing Guidelines before the U.S. Sentencing Commission on March 12 in Washington, D.C.

Felman presented the work of the ABA Criminal Justice Section Task Force on The Reform of Federal Sentencing for Economic Crimes, which issued its final report in November 2014.

To hear more about the Task Force’s proposed guidelines visit our YouTube playlist on Sentencing, or visit the Task Force website at www.americanbar.org/crimjust.

ABA Adopts CJS-Sponsored Resolutions

The ABA Criminal Justice Section successfully moved four resolutions for adoption as ABA Policy during the ABA House of Delegates meeting on February 9, 2015 in Houston, TX.

The resolutions include #107 A which urges governments to adopt a presumption against the use of restraints on juveniles in court; #107 B which urges accountability for those who unlawfully intimidate witnesses; #107 C which urges governments to enact sentencing laws that would eliminate life without the possibility of release or parole for youthful offenders both prospectively and retroactively; and #107 D which adopts the black letter of the ABA Standards for Criminal Justice: Prosecution Function and Defense Function. More information can be viewed at www.americanbar.org/groups/criminal_justice/policy.html

CJS Council Passes New Resolutions

At the 2015 Spring Council Meeting in St. Pete, FL on April 25, 2015, the CJS Council passed the following resolutions for approval at the ABA 2015 Annual Meeting in August 2015:

Pell Grants: This resolution urges Congress to restore Pell Grant eligibility for prisoners who qualify under existing need-based criteria.

Standards on Monitors: These Standards will give guidance on the role of Monitors appointed to oversee organizations as a result of judicial or regulatory ruling.

The Council also approved co-sponsorship of the Proposed Act on Juvenile Records (governing the confidentiality and expungement of juvenile delinquency records) and a resolution on overuse of psychotropic medication for children in state custody.
The Consent Once Removed Doctrine: An Emerging Nuance to the Fourth Amendment Warrant Requirement

By Jeffrey T. Wennar

The Fourth Amendment to the United States Constitution states, “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

A point of departure for any understanding of the Fourth Amendment was established in Coolidge v. New Hampshire when the Supreme Court held that “[t]he most basic constitutional role in this area is that ‘searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well defined exceptions.’”

Over the years, the Supreme Court has recognized certain exceptions to the warrant requirement of the Fourth Amendment: search incident to arrest, automobile search, plain view, inventory, consent, Terry, abandoned property, hot pursuit or exigent circumstances, community-caretaking, suitcase or container, and protective sweeps.

A search conducted pursuant to a valid consent is a well-recognized exception to the Fourth Amendment. In a challenge to a warrantless search by consent, the trial court must base its ruling on the “totality of the circumstances” whether the consent was knowingly and voluntarily given. The government is not required to show the defendant was informed of the ability to refuse consent. The consent must be more than simply giving in to law enforcement. A third party with actual or apparent authority may provide a valid consent to search. Law enforcement officers are not required to disclose their true identities nor their true purpose in order to receive consent. The scope of the consent is what a reasonable person would have understood from the exchange between the consenter and officer. The Court has cautioned where the consent occurs after an illegal entry, the consent will be found invalid.

The Supreme Court has rejected additional exceptions to the Fourth Amendment warrant requirement for searches of homes. However, a doctrine known as “consent once removed” has been evolving for over thirty years originating in the 7th Circuit, finding traction in both federal and state courts. “The concept of consent once removed is, ultimately, a variation of the ‘traditional’ consent doctrine.” This article examines those federal circuits that have addressed this doctrine. The reader is advised to research their particular jurisdiction to ascertain that jurisdiction’s decisions regarding this doctrine.

In 2009, the Supreme Court was presented with a §1983 action against officers alleging Fourth Amendment violations for entering a residence without a warrant. Callahan was to sell methamphetamine an informant for the Central Utah Narcotics Task Force. The informant went to Callahan’s residence to make the purchase. The informant entered the residence, confirmed that the methamphetamine was there, “then told [Callahan] that he needed to obtain money to make the purchase and left.” After meeting with police, the informant returned to Callahan’s residence and was let into the home by Callahan’s daughter. The informant completed the transaction and gave a pre-determined signal to police who then entered the residence arresting Callahan.

The Court restated the 10th Circuit’s definition, “[t]he ‘consent-once-removed’ doctrine applies when an undercover officer enters a house at the express invitation of someone with authority to consent, establishes probable cause to arrest or search, and then immediately summons other officers for assistance.”

The Supreme Court noted that the Circuit Court’s majority opinion applied the doctrine to undercover officers, not to informants. Although the Supreme Court made an in-depth examination of the consent once removed doctrine as applied by lower courts, the Court did not adopt the doctrine as a new exception to the Fourth Amendment warrant requirement.

In Pearson v. Callahan, the person entering the residence was an informant. Federal Circuit Courts have addressed the secondary entry by law enforcement officers after receiving consent from either an undercover officer or from an informant.
In *United States v. Akinsanya,*32 the defendant was arrested in his apartment after selling heroin to an informant. The Circuit Court affirmatively applied the doctrine to the actions of the police predicated by the actions of the informant. The 6th Circuit was presented with an informant who had set up a drug transaction in Yoon’s apartment.33 Upon being notified the marijuana was in the apartment, officers entered the apartment to effect the arrest. The 6th Circuit, relying on a 7th Circuit decision,34 expanded the 6th Circuit’s previous decision applying the doctrine to law enforcement officers only,35 making the doctrine applicable to confidential informants as well as law enforcement officers.

The doctrine is not without limitations. In *United States v. Dia,*36 the 7th Circuit found that once undercover officers exited the suspect’s hotel room the officers had the opportunity to, and should have, obtained a search warrant.37

In a §1983 action, the 6th Circuit reviewed the entry of animal service officers into a home without a warrant.38 In that case undercover animal service officers were invited into the home on the pretense of purchasing a puppy.39 The undercover officer stepped outside for a moment and the officers then knocked on the door.40 When O’Neill opened the door he was confronted by uniform officers demanding a breeder’s license which O’Neill did not possess.41 Citing and analogizing *Maryland v. Macon,*32 the Court found that the O’Neills had “opened a portion of their home to the public when they invited those who responded to their newspaper ad to come and look at puppies.”42 The Court emphasized that they were not extending the doctrine to re-entry.43 The Court went on to distinguish the 7th Circuit cases,44 stating they “do not stand for the general proposition that achieving ‘one consensual entry’ permits ‘law enforcement agents [to] thereafter enter and exit a home at will.”45 Ultimately, the 6th Circuit declined to apply the doctrine stating “[a]pplying the consent once removed doctrine to the LMAS officer’s second entry, where no arrest was intended, would go well beyond the confines of this limited doctrine . . .”46

The consent once removed doctrine has a limited purpose with specific restrictions that law enforcement must adhere to when utilizing the doctrine. As long as the law enforcement officer is able to establish and articulate probable cause for the arrest or search – after first being invited by someone with authority into the premises and then immediately summoning additional officers for assistance – the officer is acting within the parameters established by several courts. It is imperative that attorneys advising officers be familiar with the specific law regarding this doctrine in their jurisdiction.

**Endnotes**

11. Dombrowski
27. Id. at 227.
28. Id. at 228.
29. *Callahan v. Millard Cty.,* 494 F.3d 891, 895–999 (10th Cir. 2007).
31. Id. at 244.
34. *United States v. Paul,* 808 F.2d 645 (7th Cir. 1986).
37. Id. at 458.
39. Id.
40. Id.
41. Id. at 727.
44. Id. at 731.
45. *Akinsanya,* supra note 33; *Diaz,* supra note 37.
47. Id. at 732.

**Check the ABA Criminal Justice Section Website**

[www.americanbar.org/crimjust](http://www.americanbar.org/crimjust)

for

**Latest News & Updates**

**Calendar of Events**

**New Resources**

**Project Information**

**Committee Activities**

---

**Criminal Justice Section Newsletter**

**Page 4**

**Spring 2015**
HANDLING DATA BREACHES
By Jason Gonzalez, Kathryn A.F. Martinez and John Roman

Nearly every day there is a new announcement of a data breach somewhere in the United States. There are certainly “high value” targets, like banks and healthcare companies, but even small organizations and non-profits are not immune. Failure to properly handle data breaches can lead to disastrous results, ranging from lost reputation and public relations nightmares, to government enforcement actions and nationwide civil litigation. Breaches take every form imaginable — a lost laptop, a hacker, a well-meaning employee releasing confidential information. The potential impact is no different: liability and loss.

What can lawyers do to help their clients address these risks? Here are a few ideas:

Know the Information Security Basics

Our first recommendation is simple: make sure the client understands what data it collects and why. More often than one might think, businesses collect and save sensitive information when they really don’t need to.
Try to sit down with the client and map out what data is collected, why it is collected, and where it resides (either electronically or in hard copy). If any sensitive data is collected but not truly needed, get rid of it.

Second, help the client develop appropriate information security policies and procedures. What is “appropriate,” of course, will depend on the client’s business, its risk profile, and its size and resources. There are many excellent consultants that can assist with this process, and many guides (such as the NIST Security Framework or ISO27001) that help identify best practices that may fit the client’s needs. As discussed below, the adequacy of a client’s security practices likely will come under intense scrutiny in the event of a breach. Try to ensure that the client has good policies and follows them.

Third, try to ensure the client’s employees are properly trained on information security. At the risk of stating the obvious, most data breaches stem, in one way or another, from the actions of an employee. Whether it’s lost laptops and mobile devices, weak passwords, clicking on malicious email attachments, or falling prey to “phishing” scams, the human element is perhaps the most important security variable. Thoughtful and engaging training can help reduce (but unfortunately probably not eliminate) this risk. And don’t just do training once – do “refresher” trainings at least once a year.

A few corollaries to keep in mind:

1. Security is not restricted to information technology. When evaluating information security, think beyond just the IT department. Among many other things, a client should assess its human resource procedures such as employee onboarding and off boarding, on and offsite data storage, data disposal / shredding practices, and international travel policies (as international travel can lead to warrantless “border searches” of laptops and mobile devices).

2. Establish, in advance, a comprehensive data breach response plan. It is can be difficult and surprisingly time consuming to assemble the proper internal and external team to handle a data breach. Spend the time in advance to identify the right team members, establish clear areas of responsibility and process steps, and work through any engagement letter and/or retention issues with outside vendors such as computer forensics and public relations firms. This will enable you and your client to get a running start when a data breach hits and time is of the essence.

3. Provide frequent employee reminders on e-mail usage. Yes, we mentioned employee training earlier. But email usage deserves special mention, as email is a common attack vector for hackers, and even sophisticated users can be remarkably susceptible to the temptation to click on mysterious attachments. Frequent reminders of the dangers of doing so should be provided, as well as advisements about particular “phishing” or social engineering techniques that are prevalent at the time.

4. Conduct periodic risk assessments and security posture assessments. Business models and operational processes change, and can alter a client’s risk levels and potential liabilities. A third party data security expert who specializes in data breach prevention can provide an objective, unbiased annual review of your organization’s overall security.

Jason Gonzalez (CIPP/US) is a partner at Nixon Peabody LLP and the firm’s Privacy and Data Protection practice group leader. Kathryn A.F. Martinez is an associate at Nixon Peabody LLP and John Roman (CISSP) is the firm’s Director of IT Operations.
posture. Also, make sure that the client routinely patches its software systems, uses encryption as appropriate, and segments its network so that sensitive data is not kept on public-facing systems.

5. **Manage vendors.** Some of the most prominent and harmful breaches in recent history resulted from a vendor’s lax security. Clear oversight, allocation of risk and responsibility, and auditing rights can help a client ensure that its vendors are using best practices to secure and protect data. Help the client negotiate: Who is responsible for the expenses associated with a data breach? Is there an indemnification provision that allows for reimbursement for legal counsel? Is there a liability or damages limitation in the event of a breach? A little planning and foresight can go a long way.

6. **Consider cyberinsurance.** Cyberinsurance can cover the cost of a forensic analysis, costs associated with credit monitoring for affected individuals, legal costs, and other expenses associated with a data breach. Consider advising your client to contact a broker that specializes in such insurance to see if it is appropriate (and cost-effective) for its business.

### Handling the Breach

Even if a client follows excellent security practices, there is no guarantee that a breach can be avoided. Once a breach is suspected, you and the client will have to work quickly and decisively to address it. Below is a short checklist of actions to consider. Keep in mind that they might not all be appropriate in every situation, nor necessarily followed in any particular order.

1. **Don’t Panic.** Do not assume that the incident is necessarily a data breach. Conduct an initial review of the available information to make a preliminary determination of whether data security was compromised, including a determination (if possible) of whether data was, in fact, disclosed. A particularly important consideration here is whether the data at issue was encrypted – if it was, there is a chance that even if a security compromise occurred, it may not constitute a true reportable data breach. Also attempt to determine if the security breach is still ongoing and its potential scope. All of these determinations may help focus your initial investigative approach, although it is entirely possible (and perhaps necessary) that these preliminary determinations will be superseded as new information is obtained.

2. **Deploy the data breach response plan.** Hopefully, your client will be prepared with a data breach response plan, and can deploy it immediately. In the first few hours, this often involves activating a phone or contact tree that alerts all the team members of the potential issue. Skilled computer forensic consultants should be among the first to be notified. If there is no response plan in place, key steps include: (a) designating a primary contact to ensure consistent and efficient communications; (b) retaining computer forensic consultants and (perhaps) public relations persons ASAP; and (c) formulating a preliminary investigation and analysis plan, including what systems should be analyzed first.

3. **Investigate. Preserve. Document.** Thoroughly investigate all potentially affected systems, keeping in mind that your investigative decisions (and thoroughness) may be scrutinized later. If the breach is active, take action to prevent further data loss by securing and blocking unauthorized access to systems/data and preserve evidence for investigation. Meet with key personnel and document facts (if criminal activity is suspected, coordinate these interviews with law enforcement). When possible, preserve evidence (backups, images, hardware, etc.) for forensic examination. Be sure to document all mitigation efforts for later analysis. Advise staff to keep breach details in confidence until notified otherwise. If criminal activity is suspected, notify law enforcement and follow any applicable federal, state, or local notification requirements.

4. **Comply with Breach Notification Laws.** After identifying the data owners affected, review your notice obligations – which will vary between jurisdictions – and what resources will be offered to those affected (e.g., customer service hotline, credit monitoring, identity theft protection). Draft a breach notification to be sent to all affected individuals, which may also need to be submitted to state attorneys general, depending on the extent of the breach and the number of people affected in any particular state.

5. **Reflect on Lessons Learned.** After the breach has been addressed, assess the cause of the breach, as well as the response. Solicit feedback from the responders and any affected entities and review breach response activities including feedback from involved parties to determine response effectiveness.
Be Ready for the Aftermath

Unfortunately, “handling” a data breach does not always end with remediation of the actual security breach and the notification (if necessary) of the affected parties. Data breaches are increasingly the subject of government enforcement actions, as well as private civil litigation. Perhaps the most active government enforcement agency in this area is the Federal Trade Commission which, as of February 2014, has brought more than fifty civil actions against businesses for alleged data security failures. State attorneys general also bring numerous enforcement actions based on security violations, and even the SEC and FINRA have gotten into the game. While their specific statutory mandates vary, generally speaking, these agencies focus on how well the breached entity implemented security protections, investigated and addressed the breach, and notified the affected parties. Thus, if the client effectively followed procedures consisted with those outlined above, chances are the regulators may treat it more charitably. Key to successfully navigating a governmental investigation in this area is keeping in mind, from the beginning, the importance of preserving the relevant evidence, complying with statutory mandates, and being able to advocate (and support with documentation) that the client acted reasonably and appropriately when addressing the problem.

Civil litigation is another significant potential consequence of data breaches. Putative class actions have been brought around the country following data breaches and, while several different causes of action typically are alleged, the primary theories of liability often include that the defendants failed to maintain proper security procedures, in violation of statutory and/or common law duties; that the defendants’ representations (including in privacy policies) as to data security were false or misleading; and that the defendants’ alleged delay in notifying plaintiffs of the breach caused harm. As far as claimed damages, typical allegations include that plaintiffs suffered an increased risk of future harm, incurred expenses to address that increased risk (such as credit monitoring services and the like), and suffered anxiety and emotional distress. Some plaintiffs also have alleged that the defendants’ data breach caused the plaintiffs’ personal information to “lose value.”

Defendants have vigorously challenged such suits, focusing particularly on whether plaintiffs have suffered an “injury in fact” sufficient to support standing. While Courts in some early cases found that plaintiffs’ claims of risk of future harm were sufficient, the Supreme Court’s ruling in Clapper v. Amnesty Int’l, 133 S.Ct. 1138 (2013) is generally viewed as making such claims more difficult to sustain. In Clapper, the respondents challenged the Foreign Intelligence Surveillance Act of 1978, which permitted surveillance of individuals who were not “United States persons” and who were believed to be located outside the U.S. Id. at 1142. They argued that they had standing because their jobs made it likely that they would engage in sensitive communications with such surveillance targets and that, therefore, there was “an objectively reasonable likelihood” that they too would be subject to allegedly improper surveillance. The Supreme Court rejected this argument, concluding that “respondents’ theory of future injury is too speculative to satisfy the well-established requirement that threatened injury must be ‘certainly impending.’” Id.

Many defendants have successfully relied upon Clapper to argue that plaintiffs’ alleged risks of future harm were not sufficient to confer standing. Recent cases out of the Northern and Southern Districts of California, however, have found allegations of risk of future harm stemming from data breaches sufficient, at least to survive motions to dismiss. These two lines of cases are difficult to satisfactorily reconcile, as the factual allegations regarding the risk of future harm in these various cases can be viewed as quite similar, and do not necessarily seem to call for different outcomes. It may be that, as a result of these arguably diverging applications of Clapper’s standing analysis, enterprising plaintiffs’ attorneys may be tempted to “forum shop” to have cases heard in California to take advantage of the favorable law potentially developing there.

Lawyers advising clients regarding post-data breach litigation therefore should consider the following:

- Preserve the evidence. There is no easier way for a client to get in hot water with law enforcement or civil plaintiffs than by failing to preserve evidence. Data preserved in connection with the breach investigation itself should continue to be preserved in anticipation of later civil litigation.

- Conduct your data breach investigation with an eye towards being able to explain, later on, what steps you took, why you took them, and why the timeline you followed was appropriate. It’s highly likely that others, including the government and plaintiffs’ attorneys, will second-guess your decisions and timeline later.
Preserve the privilege. Be sure that it’s clear that the internal data breach investigation is done at your direction, and for the purpose of advising the client. Make sure this is reflected in an engagement letter, that any external consultants are hired by you, rather than the client, and that those that participate in the investigation know that it is to be kept appropriately confidential. This will increase the chances (but not guarantee) that the details of the investigation will be protected by the attorney-client privilege and/or work product protections.

Prior to any litigation, review your client’s privacy policies and terms of use to ensure that the representations they make regarding data security are accurate and defensible, as plaintiffs have alleged detrimental reliance on such statements. Also consider including warranty disclaimers regarding security, as some courts have looked to such disclaimers when evaluating plaintiffs’ claims that a data breach amounted to a breach of warranty.

Take a hard look at the type of data breach alleged. Even courts viewed as “plaintiff friendly” may be more willing to find no injury (and thus no standing) if the alleged breach resulted from a lost laptop or other “incidental” theft, as opposed to a targeted, advanced-persistent-threat type hack that indicates a true intent to steal and misuse data.\(^3\)

Endnotes

1 Statement of FTC Chairwoman Edith Ramirez to U.S. Senate Judiciary Committee, Hearing on Privacy in the Digital Age; Preventing Data Breaches and Combating Cybercrime, February 4, 2014. The FTC proceeds generally under Section 5 of the FTC Act, which prohibits “unfair or deceptive acts or practices in or affecting commerce.” 15 U.S.C. § 45. The FTC typically alleges that the defendant entity, by failing to use adequate security practices, engaged in “unfair” business practices. The FTC also frequently brings enforcement actions based on an entity’s alleged misrepresentations in its privacy policy, including regarding the quality of the data security practices the entity implements.

2 The approach of SEC and FINRA has been to focus not only on cyber-security breaches, but also on the processes and controls regulated entities should follow to prevent breaches from occurring in the first place. They have disciplined firms for, among other things, not properly training staff on protection of customer information, having lax password policies, and failing to properly use encryption, antivirus software, and firewalls.

3 See, e.g., Reilly v. Ceridion Corp., 664 F.3d 38, 42 (3rd Cir.2011) (no standing where harm depended on third parties reading, copying, and understanding their personal information, intending to use such information to commit future criminal acts, and being able to make unauthorized transactions in plaintiffs’ names in the future); In re Barnes & Noble Pin Pad Litig., No. 12–cv–8617, 2013 WL 4759588, at *3 (N.D.Ill. Sept. 3, 2013) (“[m]erely alleging an increased risk of identity theft or fraud is insufficient to establish standing.”); Hammond v. The Bank of New York Mellon Corp., No. 08 Civ. 6060, 2010 WL 2643307, at *2 (S.D.N.Y. June 25, 2010) (“Plaintiffs here do not have Article III standing (i.e., there is no “case or controversy”) because they claim to have suffered little more than an increased risk of future harm from the loss (whether by accident or theft) of their personal information.”); Allison v. Aetna, Inc., No. 09–2560, 2010 WL 3719243, at *5 (E.D.Pa. Mar. 9, 2010) (no standing where the plaintiffs “alleged injury of an increased risk of identity theft is far too speculative.”); Amburgy v. Express Scripts, Inc., 671 F.Supp.2d 1046, 1052 (E.D.Mo.2009) (“[P]laintiff surmises that, as a result of the security breach, he faces an increased risk of identity theft at an unknown point in the future. On the facts as alleged in the Complaint, it cannot be said that the alleged injury to plaintiff is imminent.”); Hammond v. Heartland Payment Sys., Inc., 2009 WL 704139, at *1 (D.N.J. Mar. 16, 2009) (suau sponte dismissing case because plaintiff’s allegations of increased risk of identity theft and fraud “amount to nothing more than mere speculation.”); Randolph v. ING Life Ins. and Annuity Co., 486 F.Supp.2d 1, 8 (D.D.C.2007) (“Plaintiff’s allegations therefore amount to mere speculation that at some unspecified point in the indefinite future they will be the victims of identity theft.”); Key v. DSW, Inc., 454 F.Supp.2d 684, 689 (S.D.Ohio 2006) (“In the identity theft context, courts have embraced the general rule that an alleged increase in risk of future injury is not an ‘actual or imminent’ injury.”); Bell v. Axciom Corp., No. 06CV00485–WRW, 2006 WL 2850042, at *2 (E.D.Ark. Oct. 3, 2006) (rejecting plaintiff’s allegation of increased risk of identity theft and stating, “[b]ecause Plaintiff has not alleged that she has suffered any concrete damages, she does not have standing under the case-or-controversy requirement.”). The US Supreme Court’s recent grant of certiorari in Spokeo, Inc. v. Robbins (No. 13-1339) may also be significant in this area, as the Court is asked to decide whether plaintiffs alleging only violations of statutory rights, as opposed to actual financial or personal injury, have Article III standing. If the Court decides that standing exists for such “statutory injury” claims, data breach plaintiffs may well allege that the breach violated certain statutory rights, conferring standing without any need to allege any particularized financial or personal injury.


Pappas, Continued from Page 10

recognizes that the risk of corruption is an important consideration in such assessment. This in turn may prove to be an impetus in litigation centered on allegations of ineffective ICFR due to undetected corrupt activity.

Given that under the Sarbanes-Oxley Act, ultimate responsibility for an effective internal controls environment is in the hands of officers of the company — and indeed can form the basis of personal liability — it would be prudent for public companies and their counsel to focus on the state of their internal controls “windows” and the risk of breakage due to corruption.

Endnotes


2 PwC Securities Litigation Study, April 2014.

3 The Committee of Sponsoring Organizations has the following members: Institute of Management Accountants, American Accounting Association, American Institute of Certified Public Accountants, Institute of Internal Auditors, and Financial Executives International.
The New Internal Control Framework: Perspectives for Litigation Counsel

By Jimmy Pappas

While prosecution of accounting fraud is often understood to involve financial accounting misstatement, the Securities and Exchange Commission (SEC) is increasingly advancing the theory of fraud to include issues around internal controls over financial reporting (ICFR).

The purpose of these internal controls is to provide reasonable assurance regarding the preparation of financial statements for external purposes, in accordance with generally accepted accounting principles. An effective ICFR includes controls that ensure that both the amounts on the face of the financial statements — and the related disclosures in the footnotes — are materially correct.

Increased emphasis on internal controls by the SEC could potentially broaden exposure to liability for corporate officers who sign certifications, as required under Sections 302 and 404 of the Sarbanes-Oxley Act. Per Scott W. Friestad, associate director in the SEC’s Enforcement Division, “Corporate executives have an obligation to take the Sarbanes-Oxley disclosure and certification requirements very seriously.”

Broken windows, liable officers

The SEC seems poised to continue to focus on internal controls — even absent restatements of public-company financials — as part of its so-called “broken windows” strategy, under the theory that focusing on infractions before they become larger violations will benefit investors and the financial markets.

Indeed, litigation attorneys are increasingly being called to defend corporate executives against allegations of failing to maintain effective ICFR. According to data analyzed by PwC,® allegations of deficiencies in ICFR are included in the majority of accounting-related litigation cases — reaching 70% in 2013, compared to 60% in 2012. Properly addressing questions regarding the design and operation of ICFR, therefore, can be crucial to the resolution of litigation involving ICFR.

The COSO Framework: A reference point for internal controls

In 1985, the National Commission on Fraudulent Financial Reporting, a private-sector initiative also known as the Treadway Commission, was formed to study the financial reporting system in the United States. The Commission issued a report recommending that its Committee of Sponsoring Organizations (COSO)1 work to integrate the various internal control concepts and definitions, and to develop a common reference point. The result of this effort, in 1992, was COSO’s Internal Control—Integrated Framework (the “1992 Framework”). The 1992 Framework became widely accepted as a means for designing, implementing, and assessing the effectiveness of internal controls. It outlined five broad components of an effectively designed internal control system — Control Environment; Risk Assessment; Control Activities; Information and Communication; and Monitoring Activities. Most publicly traded companies in the United States chose to use the 1992 Framework to comply with Section 404(a) of the Sarbanes-Oxley Act, as allowed by SEC rules.

While these five basic components were useful as broad guidelines, the onus was largely on individual companies to turn them into actionable internal controls on the ground. An evolving business environment, however, which over the last two decades has become increasingly complex, global, and technology-driven — not to mention subject to greater stakeholder scrutiny around internal control transparency and accountability — required a less opaque bridge between these five components and a company’s approach to building an effective internal control environment.

The 2013 Framework: A road map for assessing ICFR-related litigation

In response, COSO issued an updated internal control framework (the “2013 Framework”), which became effective on December 15, 2014. Conceptually the two frameworks are similar in that they include the same five broad components of an effectively designed internal control system. But the 2013 Framework adopts a more explicit approach — it lays out 17 principles, across these 5 components, which had been only implicitly addressed in the 1992 Framework — as illustrated in the diagram below:

Jimmy S. Pappas is a Managing Director with PwC.

This article appears in conjunction with PwC’s sponsorship of the CJS and that neither the CJS nor the ABA recommends or endorses the product or services of PwC.
The additional granularity of the 2013 Framework gives companies and their counsel a road map for evaluating the strengths and weaknesses of ICFR-related litigation claims. It also offers clear parameters within which counsel must make the case that the five components of an effective internal control system are present and functioning.

The fraud risk assessment: A wide-ranging tool

Of special interest to litigation counsel is Principle 8, which for the first time explicitly calls on companies to conduct a fraud risk assessment in ensuring that ICFR is not undermined by fraud. Importantly, the fraud risk assessment includes consideration of not only fraudulent reporting (e.g., reporting of fictitious revenue) and misappropriation of assets (e.g., unauthorized and willful disposal of assets), but also of corruption — an area previously more closely aligned with legal compliance control objectives than with financial reporting control objectives. And, since many companies operate in environments where corruption is more prevalent than in the United States, the need for a robust fraud risk assessment under the 2013 Framework is further accentuated.

Corruption can have financial reporting implications

A corrupt act, such as the bribing of a foreign official to secure a lucrative contract, can have financial reporting implications that go beyond merely capturing any resulting liability the company may have incurred in the form of probable regulatory fines. Users of financial statements would also be interested in knowing, though appropriate disclosures in the footnotes to the financial statements, the extent to which a company’s reported revenue was materially increased through bribes. Because such revenue is not representative of a company’s ability to fairly compete in the market, investors will largely discount it.

This underscores the significance of Principle 8’s requirement that corruption be taken into consideration when performing the fraud risk assessment. Failing to timely detect and accurately reflect in the financial statements the impact of corrupt activity can be indicative of ineffective ICFR.

While white collar attorneys are already focused on advising or defending clients with respect to the growing number of anticorruption statutes — including the Foreign Corrupt Practices Act (FCPA), UK Bribery Act, and several dozen other similar laws now on the books in countries around the world — they should also be prepared to address possible regulatory and non-regulatory litigation centered on allegations of ineffective ICFR due to undetected corrupt activity.

Conclusion

Effective ICFR provides reasonable assurance regarding the preparation of financial statements for external purposes. The principles-based approach of the 2013 Framework provides a better road map for counsel to link the five components of an effective internal control environment to the control realities of an entity whose ICFR is subject to litigation — but it also imposes parameters, albeit broad, beyond which it will become difficult to assert the presence of an effective ICFR. Furthermore, the 2013 Framework emphasizes the importance of undertaking a robust fraud risk assessment in implementing an effective ICFR, and
Fourth International White Collar Crime Institute

October 12-13, 2015

Law Offices of Berwin Leighton Paisner (Adelaide House)
London, UK

Topics will include:
- Corporate Espionage
- Cybercrimes
- International Money Laundering and Sanctions
- Cross-border Evidentiary Concerns
- Whistleblowers
- Deferred Prosecution Agreements
- International Internal Investigations

Global White Collar Crime Institute

November 19-20, 2015

The Ritz-Carlton Shanghai, Pudong
Shanghai, China

Topics will include:
- General Counsels’ Roundtable
- Enforcers’ Roundtable
- Year in Review: Lessons Learned from Recent White Collar Prosecutions in China and the United States
- Anti-Corruption: Trends & Enforcement
- Cyber Crime and Virtual Currencies
- Internal Investigations
The National Attorneys General Training & Research Institute (NAGTRI) of the National Association of Attorneys General (NAAG) will host a seminar “Be, Bug or Turn”: The Use of Undercover Investigators, Wiretaps and Confidential Informants in Corruption Investigations” June 10-12, 2015 in Philadelphia. This training will explore best practices in the investigation and prosecution of a corruption case, with particular focus on the ethical and practical considerations relating to the use of undercover investigators, confidential informants and wiretaps. For more information visit: www.naag.org/nagtri/nagtri-courses/national/anti-corruption-be-bug-or-turn.php

NACDL’s 58th Annual Meeting & Seminar, “High Altitude Trial Skills from the Masters of Advocacy” will be held at the Westin Denver Downtown Hotel in Denver, CO July 23-26, 2015. NACDL presents this innovative program devoted to the art, science, and development of trial skills, with hands-on interactive lectures by the most highly-regarded defense lawyers from around the country. The faculty will implement live demonstrations throughout their presentations to impart new tactics and effective trial skills that can be used and applied in any kind of case by defense advocates at all experience levels. For more information visit: www.nacdl.org/annual/

The National Association of Attorneys General will also host its Summer Meeting in San Diego, June 16-18. The NAAG Summer Meeting is popular with the state and territorial attorneys general and its agenda covers substantive, prevailing legal topics. The always-popular U.S. Supreme Court Perspectives luncheon, with the latest assessment of cases, and the William H. Sorrell Lecture Series on Tobacco Policy and Enforcement, will bring prominent speakers to the meeting podium. For more information visit: www.naag.org/meetings-trainings/annual-meetings/summer-meeting.php

National District Attorneys Association (NDAA) will host its Summit on Prosecution Integrity will be held July 19-21, 2015 at the Intercontinental Hotel in Chicago. This summit will feature educational sessions and strategy sessions for using best practices to address issues critical to prosecutors’ efforts in every state. For information visit: www.ndaa.org