TABLE OF CONTENTS

Articles »

Handling Harmful or Deficient Rule 30(b)(6) Deposition Testimony
By George Denegre and Carey L. Menasco
To what extent is it binding, and what can you do about it?

Omnicare Addresses Liability for Expressions of Opinion under Section 11
By Patricia A. Gorham and Samuel J. Casey
The decision creates an ambiguous and potentially shifting landscape.

P.F. Chang's Cyber Breach Raises CGL Coverage Concerns
By Michael Luongo
The Travelers lawsuit makes clear that consumer general liability policies alone may not provide coverage for cyber incidents.

Ethical Issues Implicated by Lawyers' Use of Third-Party Cloud Services
By Amelia Toy Rudolph
Proceed with caution when entering the cloud.

News & Developments »

New York Embraces "Likely to Succeed" Standard for Appeals
Exhaustion of appeal options is unnecessary.

Recent SEC Publications Address Cybersecurity
These publications provide tips to investors, and also may be useful for broker-dealers and investment advisors to consider in addressing cybersecurity issues at their firms.
Handling Harmful or Deficient Rule 30(b)(6) Deposition Testimony

By George Denegre and Carey L. Menasco – May 29, 2015

Anyone who has defended a deposition pursuant to Federal Rule of Civil Procedure 30(b)(6) has worried about harmful or deficient testimony that will come back to haunt the client. Of course, obtaining that harmful testimony is a primary goal of the lawyer sitting on the other side of the table. There is no question that such testimony is “binding on the corporation.” But what precisely does that mean? Does the adversary have a free pass either to exclude contrary evidence or to use the damaging testimony without challenge at trial? It depends. Often the extent to which a court will allow a party to introduce contrary evidence seems to correlate directly with the degree to which a 30(b)(6) witness was adequately prepared and, thus, is intertwined with sanctions. This article addresses the differing approaches taken by courts and suggests possible ways to remedy harmful 30(b)(6) testimony before trial or motion practice. These issues are of particular importance to law firms, accounting firms, and other institutional clients, given the proliferation of Rule 30(b)(6) practice in professional liability cases.

Basic Principles Governing Rule 30(b)(6) Depositions

Federal Rule of Civil Procedure 30(b)(6) allows a party to depose an entity through designated representatives. The general purpose of a Rule 30(b)(6) deposition is to permit the examining party to discover the corporation’s position through a witness designated by the corporation to testify on its behalf. Rosenruist-Gestao E. Servicos LDA v. Virgin Enters., Ltd., 511 F.3d 437, 441 n.2 (4th Cir. 2007). Once noticed, the entity must produce a deponent who is knowledgeable on the subject matters identified in the notice. 7 James Wm. Moore et al., Moore’s Federal Practice § 30.25 (3d ed. 2014) (citing Alexander v. FBI, 186 F.R.D. 137, 141 (D.D.C. 1998)). According to one oft-quoted standard, the corporation “must make a conscientious good-faith endeavor to designate the persons having knowledge of the matters sought by [the interrogator] and to prepare those persons in order that they can answer fully, completely, unequivocally, the questions posed by [the interrogator] as to the relevant subject matters.” Protective Nat’l Ins. Co. of Omaha v. Commonwealth Ins. Co., 137 F.R.D. 267, 278 (D. Neb. 1989) (quoting Mitsui & Co. v. Puerto Rico Water Res. Auth., 93 F.R.D. 62, 67 (D.P.R. 1981)). Many courts hold that this duty extends “not only to facts, but also to subjective beliefs and opinions.” Estate of Scott W. Thompson v. Kawasaki Heavy Indus., 291 F.R.D. 297, 303 (N.D. Iowa 2013) (quoting Brazos River Auth. v. GE Ionics, Inc., 469 F.3d 416, 433 (5th Cir. 2006)). The burden is “onerous,” and the corporate representative must be diligently prepared.

To What Extent Is 30(b)(6) Testimony Binding and Why?

There is a general agreement that the Rule 30(b)(6) deposition testimony is binding on the entity. See, e.g., A&E Prods. Grp., L.P. v. Mainetti USA, Inc., No. 01-10820, 2004 U.S. Dist. LEXIS 2904, at *19 (S.D.N.Y. Feb. 25, 2004); Resolution Trust Corp. v. Farmer, No. 92-3310, 1994 U.S. Dist. LEXIS 8755, at *5 (E.D. Pa. June 23, 1994) (“The purpose behind Rule 30(b)(6) is to create testimony that will bind the corporation.”) (citations omitted). But courts are not consistent about what precisely that means.

Some courts hold that “binding” means “really binding,” and they refuse to allow the introduction of contrary evidence at trial. See, e.g., lerardi v. Lorillard, Inc., No. 90-7049, 1991 U.S. Dist. LEXIS 11887, at *8 (E.D. Pa. Aug. 20, 1991). (“If the designee testifies that [the agency] does not know the answer to [the opposing party’s] questions, [the agency] will not be allowed effectively to change its answer by introducing evidence during trial.”); Great Am. Ins. Co. v. Summit Exterior Works, LLC., No. 3:10-cv-1669, 2012 U.S. Dist. LEXIS 17548, at *16–18 (D. Conn. Feb. 13, 2012); QBE Ins. Corp. v. Jorda Enters., 277 F.R.D. 676, 690 (S.D. Fla. 2012). These courts reason that treating the statements in a Rule 30(b)(6) deposition as admissions is most consistent with the purpose of the rule, which is to
“permit[ ] the examining party to discover the corporation’s position via a witness designated by the corporation to testify on its behalf.” Kawasaki, 291 F.R.D. at 303 (quoting Rosenruist-Gestao E. Servicos LDA, 511 F.3d at 440 n.2).

Most courts that follow this reasoning have allowed the introduction of contrary evidence if the party introduces evidence sufficiently explaining the reason for the change; the nature of the required explanation varies significantly. For example, in Kawasaki, the district court held that the deposition testimony of the defendant’s 30(b)(6) witness was binding on the defendant and “that some extraordinary explanation must be required before [the defendant] is allowed to retreat from binding admissions in the testimony of its Rule 30(b)(6) designee.” 291 F.R.D. at 309. See also Rainey v. Am. Forest & Paper Ass’n, Inc., 26 F. Supp. 2d 82, 94 (D.D.C. 1998) (must establish that information was not known or inaccessible); Hyde v. Stanley Tools, 107 F. Supp. 2d 992, 993 (E.D. La. 2000) (inconsistent affidavit may be accepted if accompanied by reasonable explanation).

The majority view is that “[t]he testimony of a Rule 30(b)(6) representative, although admissible against the party that designates the representative, is not a judicial admission absolutely binding on that party.” State Farm Mut. Auto. Ins. Co. v. New Horizon, Inc., 250 F.R.D. 2013, 212 (E.D. Pa. 2008) (quoting 8A Charles Alan Wright et al., Federal Practice and Procedure § 2103 (Supp. 2007)); A.I. Credit Corp. v. Legion Ins. Co., 265 F.3d 630, 637 (7th Cir. 2001); R&B Appliance Parts, Inc. v. Amana Co., 258 F.3d 783, 786 (8th Cir. 2001). It is evidence that, like any other deposition testimony, can be contradicted and used for impeachment purposes. A.I. Credit Corp., 265 F.3d at 637. Under this view, harmful or deficient Rule 30(b)(6) deposition testimony can be used for impeachment, but the opposing party may seek to introduce evidence that contradicts or is inconsistent with the deposition testimony.

Nevertheless, as a practical matter, it is hard to take much comfort from the proposition that courts in some jurisdictions will permit the introduction of evidence that contradicts or is inconsistent with the 30(b)(6) testimony. This should seem intuitive. The 30(b)(6) witness is the voice of the corporation, and his or her face will be shown to the jury on a big video screen. It is not easy to undo the testimony of that chosen representative. See, e.g., Kawasaki, 291 F.R.D. at 309 (rejecting defendant’s argument that video deposition of its 30(b)(6) witness could not be played in plaintiff’s case-in-chief).

Is It Necessary to “Fix” Harmful 30(b)(6) Testimony? How?
As noted, the majority of courts allow a party to introduce evidence that contradicts or is inconsistent with 30(b)(6) testimony. Therefore, depending on how bad the “sound bite” given, it may not be necessary to take affirmative steps to fix that testimony. But it may not be possible to know in advance the court’s view on this issue, and, if the point is important enough, it may be worth trying.

Rule 30(e) permits a deponent to designate changes “in form or substance” to the transcript of his or her deposition. Some parties have tried to correct Rule 30(b)(6) deposition answers under Rule 30(e) by showing substantive changes on the errata sheets that are used to reflect changes to deposition transcripts. See, e.g., Porter v. West Side Rest., LLC, No. 13-1112, 2014 U.S. Dist. LEXIS 57126 (D. Kan. Apr. 24, 2014); Green v. Wing Enter., Inc., No. 1:14-1913, 2015 U.S. Dist. LEXIS 13654 (D. Md. Feb. 5, 2015). This approach is unlikely to be of much help because courts are very resistant to permitting substantive changes to testimony through this method. Id. In addition, the opposing party may still use the original answers provided in the 30(b)(6) deposition and impeach the witness at trial with inconsistencies. See, e.g., In re Weatherford Int’l Secs. Litig., No. 11-cv-1646, 2013 U.S. Dist. LEXIS 120321 (S.D.N.Y. Aug. 23, 2013). That said, this option is worth considering and may be useful under certain conditions.

Federal Rule of Civil Procedure 26(e)(2) imposes a duty on a party to amend certain types of discovery responses. While deposition testimony is not included in the list of discovery devices encompassed by the rule, some courts have extended it to correcting 30(b)(6) testimony. Diamond Triumph Auto Glass, Inc. v. Safelite Glass Corp., 441 F. Supp.
2d 695, 723 n.17 (M.D. Pa. 2006). This is a reasonable position because Rule 30(b)(6) depositions are intended to define the entity’s positions, unlike depositions of individuals. Thus, another possible solution would be to package the documents or information that establish the correct answer and serve them on opposing counsel as part of a supplemental discovery response. Counsel should take care to identify the specific testimony that is being supplemented and corrected.

While it would be unorthodox in a case in which a witness was generally prepared, it may be worth offering additional corporate testimony on the subjects that were inadequately dealt with the first time. But opposing counsel probably will not be open to having the witness’s “sound bites” undone. And this suggestion raises issues of costs and legal expense as well as the exposure of having additional 30(b)(6) testimony.

While these suggestions may not fully solve the problem of harmful testimony, they may give the party some credibility with the court when the time comes to decide how the testimony is going to be treated. Many of the rulings in this area are fact driven, and the court may well be influenced by counsel's efforts to set the record straight immediately—especially if the witness was generally prepared to testify.

**To What Extent Can the Other Side Use 30(b)(6) Testimony?**

So what should the party who obtains favorable testimony do? If the testimony opens the door for a motion for summary judgment, then the most obvious path is to use it in support of the motion and rely on the cases cited above for the proposition that the harmful testimony cannot be contradicted. See, e.g., *Hyde*, 107 F. Supp. 2d at 993 (corporation could not defeat summary judgment with affidavit that contradicted the deposition testimony of its corporate representative); *Rainey*, 26 F. Supp. 2d at 95 (“[T]he Kurtz affidavit's quantitative assertion works a substantial revision of defendant’s legal and factual positions. This eleventh hour alteration is inconsistent with Rule 30(b)(6).”). Similarly, if the matter is moving to trial, the receiving party should consider filing a motion in limine to exclude any evidence that contradicts the Rule 30(b)(6) testimony. See, e.g., *Reilly v. Natwest Mkts. Grp. Inc.*, 181 F.3d 253, 269 (2d Cir. 1999) (affirming order precluding five witnesses from testifying); *Leardi*, 1991 U.S. Dist. LEXIS 11887, at *8 (holding that party cannot introduce evidence during the trial contradicting previous statements by Rule 30(b)(6) designee); *Rockett v. Stifel, Nicolaus & Co., Inc.*, No. 7:12-cv-144, 2014 U.S. Dist. LEXIS 153989 (M.D. Ga. Oct. 30, 2014) (reserving ruling until time of trial).

In response, the opposing party should underscore the majority view that 30(b)(6) testimony is not an admission and offer contradictory or inconsistent evidence. It should also offer a reasonable explanation as to why the testimony was not offered earlier, such as that the correct information was not available at the time of the deposition, or otherwise place the harmful testimony in a favorable context. *Hyde*, 107 F. Supp. 2d at 993. On the latter point, the opposing party should emphasize the preparedness of the witness and perhaps point to the volume of information covered at the deposition. Absolute perfection is not required, and the court may be more forgiving of a memory lapse or “slip-up” in the context of a productive deposition. *Id.* (honest mistake may suffice).

**Issues Related to the Unprepared Witness**

The discussion above assumes that a prepared witness gave harmful testimony. What happens when a corporate entity presents a 30(b)(6) witness who is unprepared or unable to answer the questions posed? Cases in this area often involve sanctions that exclude or restrict the use of evidence contradicting testimony given by an unprepared 30(b)(6) witness. But they do not necessarily give a free pass to the party receiving the deficient testimony.

Producing an unprepared witness is tantamount to a failure to appear for the deposition. *United States v. Taylor*, 166 F.R.D. 356, 363 (M.D.N.C. 1996). In circumstances where a 30(b)(6) witness was unable to answer questions on noticed topics, the designating party must substitute an appropriate deponent when it becomes apparent that the previous deponent is unable to respond to certain relevant areas of inquiry. 7 James Wm. Moore et al., *Moore's
Federal Practice § 30.25 (3d ed. 2014). If the party does not provide another witness voluntarily, a court will likely compel it to do so, if requested to do so, and will often award sanctions. State Farm, 250 F.R.D. at 215–16.

Failure to provide a prepared substitute witness, especially after a request by the other party, can result in the award of draconian sanctions. For example, in Jo Ann Howard & Associates, PC v. Cassity, No. 4:09-cv-1252, 2014 U.S. Dist. LEXIS 163793, at *10 (E.D. Mo. Nov. 14, 2014), the district court noted the “severity of the witness’s unpreparedness” where the witness could not answer even general questions about the topics listed in the deposition notice and claimed to not be speaking on behalf of the party. The district court assessed heavy sanctions against the defendant, prohibiting it from introducing evidence on the topics the witness could not answer and instructing the jury to assume any testimony the witness would have provided would have been adverse to the defendant.

If the party does not offer a substitute witness, one strategy would be to use the lack of responsive answers at trial or to support a motion for summary judgment. But several courts have taken issue with this strategy. In Gutierrez v. AT&T Broadband, LLC, 382 F.3d 725, 733 (7th Cir. 2004), the Seventh Circuit criticized the plaintiff’s strategic choice to wait to raise the issue until after the close of discovery:

[Although we in no way condone the defendants' choice to provide . . . a largely unresponsive witness, as their Rule 30(b)(6) deposition representative, we also note that the plaintiffs made a tactical decision not to insist that the defendants produce better witnesses after [the witness] proved inadequate. Such a request very likely would have been viewed favorably had it been made prior to the close of discovery, with possible sanctions levied against the defendants for failing to provide an appropriate deponent in the first instance. Yet, the plaintiffs raised their dissatisfaction with [the witness] after the close of discovery, in the midst of summary-judgment briefing, and with prior knowledge that better witnesses . . . existed. The district judge was not required to belatedly punish the defendants by striking [the better witness’s] affidavit or reopening discovery in such circumstances.

Other courts have reached similar conclusions in various other contexts. See, e.g., United States ex rel. Roach Concrete, Inc. v. Veteran Pac. JV, No. 10-C-826, 2013 U.S. Dist. LEXIS 57334 (E.D. Wis. Apr. 22, 2013); Ozburn-Hessey Logistics, LLC v. 721 Logistics, LLC, 40 F. Supp. 3d 437 (E.D. Pa. 2014); Diamond Triumph, 441 F. Supp. 2d at 723 n.18.

The court in Aldridge v. Lake County Sheriff's Office, No. 11-C-3041, 2012 U.S. Dist. LEXIS 102514 (N.D. Ill. July 24, 2012), took the opposite approach. In that case, the plaintiff sought to exclude testimony at trial based on the 30(b)(6) witness’s inability to address designated topics at his deposition. After finding that the 30(b)(6) testimony was grossly deficient, the court observed that neither party moved to extend the discovery deadline to allow the defense to produce another, more prepared, witness on any of the topics. But, far from finding a lack of diligence on the part of the plaintiff, the court still punished the defendant. The court limited the defendant to the answers it gave at the 30(b)(6) deposition: “Regardless of whether defendant failed to prepare its witness, or whether there was a genuine lack of knowledge, defendant will not be able to take a position at trial on those issues where one of its Rule 30(b)(6) designees did not provide testimony.” In the court’s words, “defendant [was] stuck with the record it [had] created.”

Based on the rationale of Gutierrez and other similar cases, the best practice when tendered an unprepared witness is to demand a substitute witness and, if that request is denied, move to compel. After taking these steps, the party receiving deficient testimony should be well positioned to use the nonresponsive testimony to its advantage during motion practice or at trial.

Conclusion
The holding in any particular case often turns on how diligently the witness prepared for the deposition. The most
serious sanctions or restrictions often flow from a lack of diligence on the part of the party producing the representative. Because there is no way for a party to know in advance what rules the court will apply to a request to exclude testimony, the best advice is to prepare—and then prepare some more.

**Keywords:** litigation, professional services liability, Federal Rules of Civil Procedure, 30(b)(6), corporate deposition, corporate representative

George Denegre and Carey L. Menasco are shareholders of Liskow & Lewis, PLC, in New Orleans, Louisiana.
Omnicare Addresses Liability for Expressions of Opinion under Section 11
By Patricia A. Gorham and Samuel J. Casey – May 29, 2015

The Supreme Court, in *Omnicare, Inc. v. Laborers District Council Construction Industry Pension Fund*, 135 S. Ct. 1318 (Mar. 24, 2015), recently addressed the scope of potential liability for expressions of opinions under section 11 of the Securities Act of 1933 and, in doing so, cast a considerable cloud of uncertainty over the advisability of including unnecessary opinion statements in registration filings going forward. While the Court adopted a narrow view of when an opinion statement violates section 11’s proscription against *misrepresentations* of material facts, the *Omnicare* decision developed a more expansive view of when statements of opinion may constitute *omissions* of material facts. The *Omnicare* decision, in focusing on the reasonable understanding of the investor, rather than the subjective belief of the issuer, creates an ambiguous and potentially shifting landscape through which issuers must navigate when filing registration statements with the Securities and Exchange Commission. This uncertainty will require increased restraint when making opinion statements and heightened attention to any proffered bases for such opinions.

The Factual and Legal Background

Section 11 imposes strict liability on sellers of securities if any part of the registration statement contains a material misstatement or omission of fact. 15 U.S.C. §77k(a). Prior to *Omnicare*, the Supreme Court had not yet interpreted the extent to which section 11’s strict liability regime extends to the contents of opinion statements.

Omnicare is a provider of pharmacy-related services for nursing homes. Purchasers of its securities asserted section 11 liability against Omnicare based on two alleged material misstatements or omissions: The first related to the company’s belief that its contractual arrangements were in compliance with federal and state laws, and the second involved the company’s professed belief that its contracts with pharmaceutical manufacturers were “legally and economically valid arrangements that bring value to the healthcare system and the patients that we serve.” Although the registration statement contained several caveats, these statements of belief were challenged based on allegations in unrelated lawsuits that Omnicare’s contracts with third-party medical service companies were illegal kickback schemes. The section 11 plaintiffs’ allegations centered on a warning from one of the company’s attorneys indicating that one of the contracts “carrie[d] a heightened risk” of liability; thus, the plaintiffs concluded that the company did not possess reasonable grounds to believe that its expressed opinions were truthful and complete.

The *Omnicare* district court initially dismissed the section 11 claim for failure to allege “subjective falsity”—that Omnicare did not actually hold the opinions expressed in the registration statement—which it deemed a necessary element of a section 11 claim. This decision was reversed on appeal in a groundbreaking decision by the Sixth Circuit that equated statements of opinion with statements of fact and held Omnicare strictly liable for any materially false statement. The Sixth Circuit decision explicitly eliminated the need to look to the issuer’s subjective belief and held that any statement, “[n]o matter the framing,” will incur liability for the issuer if proven both material and false. The Supreme Court granted certiorari to address

> [w]hether, for purposes of a claim under Section 11 of the Securities Act of 1993, a plaintiff may plead that a statement of opinion was “untrue” merely by alleging that the opinion itself was objectively wrong, as the Sixth Circuit has concluded, or must the plaintiff also allege that the statement was subjectively false—requiring allegations that the speaker’s actual opinion was different from the one expressed—as the Second, Third, and Ninth Circuits have held.
Omnicare’s position on appeal to the Supreme Court was that a statement of opinion is actionable only when the belief was not genuinely held by the issuer. The plaintiffs, likely anticipating a retreat from the Sixth Circuit’s expansive holding, put forth three situations in which an expression of opinion should be actionable under section 11: (1) where the opinion was not genuinely held, (2) where the opinion was misleading as to the subject matter of an opinion (for example, where the opinion assumes an underlying fact that is not true), and (3) where the opinion statement implies that the issuer had a reasonable basis for the opinion.

The Supreme Court’s Decision
The Supreme Court promptly dismissed the Sixth Circuit’s notion that section 11 liability can be established where a statement of opinion turns out to be “objectively false”—a position the Court held “wrongly conflate[d] facts and opinions.” In rejecting the “opinion as fact” construction adopted by the Sixth Circuit, the Supreme Court delineated two exceptions to the rule that opinion statements do not subject an issuer to section 11 liability. First, the Court reiterated the uncontested notion that there may be section 11 liability for a statement of opinion when the issuer does not actually hold the professed belief. Second, the majority, citing Justice Scalia’s concurrence in Virginia Bankshares, Inc. v. Sandberg, 501 U.S. 1083, 1109–10 (1991), held that opinion statements sometimes include inferences about supporting facts, and where those supporting facts are untrue (and material), section 11 liability may accrue.

In considering whether Omnicare’s opinion statements could trigger section 11 liability, the Court identified two types of statements that can exist within opinion statements. First, the Court found that every opinion statement necessarily implies the factual statement that the issuer actually holds the stated opinion. Second, some opinion statements contain “embedded” statements of fact and these embedded statements can, if misleading, violate section 11. As an example of an explicit embedded factual statement, the Court suggested that the statement “I believe our TVs have the highest resolution available because we use a patented technology to which our competitors do not have access” includes the embedded factual statement that the speaker uses a patented technology. However, because the statements at issue in Omnicare had already been determined to be “pure statements of opinion,” the Court dismissed the notion that either of the statements at issue contained any affirmative misstatements of material fact, whether explicit or embedded.

Turning next to the issue of whether Omnicare’s affirmative statements of opinion could implicate section 11 liability as omissions, the Court plowed new jurisprudential ground. Ignoring Justice Thomas’s admonition to avoid addressing issues not raised by the parties below, the Court framed the issue thusly: “We therefore must consider when, if ever, the omission of a legal fact can make a statement of opinion like Omnicare’s, even if literally accurate, misleading to an ordinary investor.” The Court then described two possible instances in which even an accurate statement of opinion could lead to omission liability. First, the issuer will be liable if the issuer does not actually hold the stated belief. Second, a reasonable investor may be misled where the expression of opinion “omits material facts about the issuer’s inquiry into or knowledge concerning a statement of opinion, and if those facts conflict with what a reasonable investor would take from the statement itself.”

The Court’s declaration that even a genuinely held opinion could nevertheless subject an issuer to liability in certain circumstances has the potential to expand liability significantly. While the Court’s holding may appear broad, a careful reading of the full opinion leads to the conclusion that omission liability is best seen as accreting to opinion statements when irrationally made. For example, where an opinion is made in the face of known, persuasive contrary evidence or is made with no inquiry into the facts where such an inquiry would be expected, those opinion statements could lead to liability. The Court noted that even an issuer that stated that it believed its conduct was lawful could be liable if the issuer never consulted an attorney or knew the government was taking an opposing view. Going so far as to state that if the decision “chills misleading opinions, that is all to the good,” the Omnicare decision forces issuers to provide some context behind the formation of the opinion.
The Court noted that claims of omission liability under section 11 for opinion statements require more than mere conclusory allegations and must include specific allegations of (1) an omitted fact (2) that would have been material to a reasonable investor (3) that rendered the opinion misleading because the excluded fact shows the lack of basis for the opinion. The majority neatly summarized the issuer's duty when making opinion statements as “only [needing to] divulge an opinion’s basis, or else make clear the real tentativeness of its belief.” Conversely, a plaintiff, under Omnicare, must do more than merely assert that the opinion at issue was incorrect or that the issuer failed to reveal the basis for the opinion; rather, the plaintiff must plead specific facts about the issuer's lack of inquiry or possession of contrary facts that would make the opinion statement misleading (and the omitted fact material).

Justice Scalia, concurring in part and concurring in the judgment, derided the majority opinion for “invit[ing] roundabout attacks on expressions of opinion” by drastically expanding the situations in which an opinion is held to infer statements regarding “collateral facts” and thus increasing potential liability. In Justice Scalia’s view, an opinion statement inherently disclaims the expression of facts, whereas the majority opinion flips that notion on its head and reads an opinion as expressing, in certain circumstances, an undisclosed basis in fact. A better approach, Justice Scalia advocated, would be to focus on whether the issuer had a reasonable basis for expressing the opinion, rather than inquiring into what a reasonable listener would deem a necessary basis for expressing the opinion.

The Takeaway
The Omnicare decision was not a clear-cut victory for either the plaintiffs' or defendants' bar. While the majority failed to accede to Omnicare's position that only opinions that were not actually held can lead to liability, it also declined to adopt the Sixth Circuit's much more expansive view of when opinion statements can be misleading. Despite the limiting language used by the Court, the Omnicare decision will nevertheless likely have far-reaching effects on opinions expressed in registration statements going forward and undoubtedly will generate considerable discussion in cases to come. Notably, the decision fails to elucidate a bright-line standard for when opinion statements implicitly include a factual statement, and its focus on what a reasonable investor would expect further devolves the inquiry into amorphousness. Thus, where opinions are expressed in registration statements, issuers should be careful to outline the basis for those opinions. Because section 11 liability is strict, the issuer should give close and careful scrutiny to the necessity and substance of any opinions included in registration statements going forward.

Keywords: litigation, professional services liability, Securities Act, section 11, securities, opinion statements

Patricia A. Gorham is a partner and Samuel J. Casey is an associate of Sutherland Asbill & Brennan in Atlanta, Georgia.
P.F. Chang's Cyber Breach Raises CGL Coverage Concerns
By Michael Luongo – May 29, 2015

Technological advancements in recent decades have enabled businesses to rapidly expand their operations, reduce costs, improve reliability, and enhance their customers' experience. A corollary of this proliferation of technology is that businesses regularly collect and store detailed personal information about their customers, including home addresses, credit and debit card numbers, and bank account information. While businesses use this information to better serve their clientele, hackers and other bad actors see a treasure trove of valuable data that can be exploited for financial gain. Not surprisingly, hackers are increasingly targeting retailers, such as Target and Home Depot, in an attempt to steal customer information. Nicole Perlroth, "Target Struck in the Cat-and-Mouse Game of Credit Theft," N.Y. Times, Dec. 19, 2013; Mitch Lipka, "56 Million Accounts at Risk in Home Depot Hack," CBS Moneywatch, Sept. 18, 2014. Attacks are becoming so commonplace, that many experts warn that it is not a question of if a company’s security systems will be compromised, but when. Kate Vinton, "How Companies Can Rebuild Trust after a Security Breach," Forbes, July 1, 2014.

When a company suffers a cyber attack, it not only has to contend with the immediate threat to its internal network and intellectual property but also must deal with legal fallout from consumers whose private information has been compromised. Ordinarily, companies turn to their commercial general liability carriers to defend and indemnify them when they face legal action. However, many insurance carriers are reluctant to extend coverage in cybersecurity breach lawsuits, thereby leaving companies to fend for themselves. Whether carriers are required to cover businesses for data breach lawsuits under commercial general liability policies has become a hotly litigated legal issue. One such coverage lawsuit was recently filed by Travelers Indemnity Company in federal court against one of its insureds, the P.F. Chang’s restaurant chain, which may serve as a test case for future cyber liability claims.

The lawsuit originated last summer when P.F. Chang’s announced that it was the victim of a cyber attack targeting its patrons’ credit card and debit card accounts. Nicole Perlroth, “P.F. Chang’s Investigating Possible Data Breach,” N.Y. Times, June 10, 2014. P.F. Chang’s was alerted to the security breach by the Secret Service and launched an investigation into the breach with federal authorities and a team of third-party forensic experts. The investigation uncovered a massive data breach that spanned a period of nine months from September 18, 2013, to June 11, 2014, and that gave hackers access to credit and debit card information from over 7 million P.F. Chang’s customers. Security experts later discovered thousands of newly stolen credit and debit cards data for sale on the same black market outlets known for selling millions of cards stolen in the Target stores data breach. The website enables thieves to download the cards’ magnetic stripe information, which can be copied onto counterfeit credit cards.

Shortly after news of the security breach became public, the affected customers filed three class action lawsuits against P.F. Chang’s, alleging that the company failed to safeguard its customers’ personal financial data, including credit and debit card information. Two of the lawsuits were filed in the United States District Court for the Northern District of Illinois: Lewert v. P.F. Chang’s China Bistro, Inc., No. 1:14-cv-04787 (N.D. Ill. filed June 25, 2014), and Kosner v. P.F. Chang’s, No. 1:14-cv-04923 (N.D. Ill. filed June 30, 2014). These complaints were later consolidated. The third lawsuit, Lovell v. P.F. Chang’s China Bistro, Inc., No. 2:14-cv-01152 (W.D. Wash. filed July 30, 2014), was filed in the United States District Court for the Western District of Washington.

According to the Illinois class actions, P.F. Chang’s failed to abide by industry standards in security, enabling hackers to steal financial data from within the company’s systems. The complaints further alleged that the company avoided implementing improved measures, in an effort to save money by cutting corners, and that such heightened security could have prevented or mitigated the scope of the security breach. The plaintiffs maintained that the hackers continued to use the information they obtained as a result of P.F. Chang’s inadequate security measures to cause
financial harm to consumers across the United States. These lax policies allegedly violated state consumer financial protection laws.

The Washington class action similarly alleged that P.F. Chang’s security failures enabled hackers to steal financial data from within P.F. Chang’s systems and to make subsequent unauthorized purchases on the customers’ credit cards. The plaintiffs additionally claim that P.F. Chang’s failed to disclose the extent of the security breach or to notify its customers in a timely manner.

P.F. Chang’s gave notice of the claims to Travelers in order to obtain coverage for the class action lawsuits. Travelers had insured P.F. Chang’s under a commercial general liability policy. However, rather than defend P.F. Chang’s in the class actions, Travelers responded by filing a federal lawsuit of its own against the restaurant chain, Travelers Indemnity Co. of Connecticut v. P.F. Chang’s China Bistro, Inc., No. 3:14-cv-01458-VLB (D. Conn. filed Oct. 2, 2014), seeking a declaratory judgment that it has no duty to defend or indemnify P.F. Chang’s in the underlying class actions. Travelers advances several theories in support of its decision not to defend or indemnify P.F. Chang’s under its commercial general liability insurance policies in cases involving data breaches.

Initially, Travelers argues that the class action lawsuits were outside the scope of coverage. Travelers notes that its policies apply only to “bodily injury” and “property damage” that is caused by an “occurrence.” The policies define an “occurrence” as an accident, “bodily injury” as physical or mental injury to a person, and “property damage” as physical injury to tangible property or loss of use of tangible property but not loss of or damage to electronic media or records. Because these definitions do not expressly cover electronic damage, Travelers contends that there is no duty to defend. Similarly, Travelers maintains that the underlying class actions do not trigger coverage for an “advertising injury,” as defined in the policy. Last, Travelers posits that even if the class actions fell within the scope of coverage, there would still be no duty to defend because the policies included an exclusion for violations of consumer financial protection laws. P.F. Chang’s has contested the action, and the lawsuit is currently pending.

As cyber attacks on businesses continue to rise, businesses must develop a risk management protocol that approaches the issue from several angles in order to limit liability. First, businesses must ensure adequate protection for cyber crimes. The Travelers lawsuit makes clear that consumer general liability policies alone may not provide coverage for cyber incidents. Where coverage is in doubt, companies should purchase cyber liability insurance policies that provide express coverage for technology-related risks. Clear wording is essential, and there must be no doubt that actual cyber exposure is covered. The justification for purchasing cyber insurance is that data breaches are expensive and often trigger various state notification laws, require reaching out to affected customers, and mandate expensive repair of the compromised system. Therefore, a strong policy, which should encompass potential first-party and third-party claims, is essential.

In addition, companies must make cybersecurity a priority by enhancing security procedures and developing internal policies regarding employee use of technology. For starters, companies should require the use of lock codes on all mobile devices, prohibit storage of work data on personal devices that are not encrypted, have a system in place to erase files remotely on lost or stolen devices, and restrict what programs employees install on company devices. Companies should further train employees regarding the risks of cyber threats and employ software or third-party support to protect against security breaches. By taking a proactive approach to cybersecurity, companies can best minimize the threat to their customers’ personal data and also ensure that they remain protected in the event of a breach.

Companies must assume that their computer networks have some level of vulnerability. For that reason, they must solidify their efforts to mitigate that risk. This process, in part, should exclude over-reliance on traditional insurance as
a panacea. Companies should have no gaps in their insurance coverage and certainly not with respect to cyber liability.

**Keywords:** litigation, professional services liability, cybersecurity, insurance, class actions, hackers, cyber liability

Michael Luongo is an associate at Goldberg Segalla, LLP, in Philadelphia, Pennsylvania.
Ethical Issues Implicated by Lawyers' Use of Third-Party Cloud Services
By Amelia Toy Rudolph – February 23, 2015

Law firms increasingly turn to “cloud services” for processing and storing confidential client information because of their greater flexibility and efficiency. Use of “the cloud,” however, outsources the administration, physical control, and maintenance of sensitive data to a third-party vendor, which raises IT security and data privacy risks.

Recent amendments to the ABA Model Rules of Professional Conduct (Model Rules) indicate less leeway for lawyers who inadvertently violate their ethical obligations through the use of technology, including such ubiquitous services as cloud computing. While the cloud does not enjoy a single accepted definition, it generally encompasses a variety of products and services that provide on-demand access to remote computing services over the Internet. Cloud services can include: (1) productivity applications such as Google Docs; (2) online document and practice management software such as Rocket; (3) remote data storage, file sharing, and retrieval services such as Dropbox, Carbonite, or iCloud; and (4) web-hosted email services such as Gmail and Hotmail.

Not only can lawyers affirmatively contract with cloud service providers, but they also can access the cloud without realizing it—for example, when using their smartphones, laptops, tablets, or web conferencing services. Whether intentional or inadvertent, the use of cloud services raises a host of ethical issues for lawyers, with accompanying obligations and duties. This article reviews the ABA Model Rules relating to the use of technology, in particular the rules regarding competence, confidentiality, and outsourcing of nonlegal services, and suggests considerations for you as a lawyer to keep in mind when taking advantage of, or otherwise encountering, cloud services.

The ABA's Ethical Rules Bearing on Technology
The ABA Commission on Ethics 20/20 was formed “to develop guidance for lawyers regarding their ethical obligations to protect [clients' confidential] information when using technology and to update the Model Rules of Professional Conduct to reflect the realities of a digital age.” ABA Comm’n on Ethics 20/20, Report to the House of Delegates: Resolution and Report on Technology and Confidentiality (May 2012). In May 2012, the Commission submitted reports to the ABA House of Delegates regarding lawyers’ use of technology and confidentiality and regarding the ethical implications of outsourcing work on client matters to lawyers and nonlawyers outside the firm. Id.; ABA Comm’n on Ethics 20/20, Report to the House of Delegates: Resolution and Report on Outsourcing (May 2012).

Each state bar retains discretion as to whether and to what extent to adopt the Model Rules and recent amendments. A lawyer’s ethical obligations in a particular situation therefore depend on which state’s rules of professional conduct apply, not to mention other applicable federal, state, and international statutes, regulations, and rules regarding data privacy and security.

Rule 1.1 of the Model Rules was unchanged by the recent amendments. It states:

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

Comment 8 to Model Rule 1.1 was amended, however, to reinforce the importance of understanding relevant technology in order to provide competent representation to clients:
To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

_Id._ (emphasis added). While this comment would appear to expand the scope of a lawyer’s duty of competence, the Commission on Ethics 20/20 report to the House of Delegates proposing the amendment states otherwise:

The proposed amendment, which appears in a Comment, does not impose any new obligations on lawyers. Rather, the amendment is intended to serve as a reminder to lawyers that they should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer’s general duty to remain competent.

_ABA Resolution 105A: Technology and Confidentiality_ (May 2012). As recent news reports of data breaches highlight, one risk associated with relevant technology is that confidentiality of data can be compromised. _Rule 1.6 of the Model Rules_ was amended to highlight a lawyer’s responsibility in this regard. Model Rule 1.6(a) states, “A lawyer shall not reveal information relating to the representation of a client” unless certain exceptions apply. Model Rule 1.6 applies to both privileged and nonprivileged but confidential client information. The ABA added a new provision, Model Rule 1.6(c):

A lawyer shall make _reasonable efforts_ to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

_Id._ (emphasis added). Although this duty was already described in several existing comments to Model Rule 1.6, the rule was amended to state this obligation explicitly in the black-letter rule, given the pervasive use of technology to store and transmit confidential client information. A new comment to Model Rule 1.6, _Comment 18_, provides further guidance on what is required for a lawyer to act competently to preserve confidentiality and makes clear that this amendment was not intended to create a strict liability standard for lawyers any time a client’s confidentiality is breached:

Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer’s supervision. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer’s efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer’s ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client’s information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules.
Id. (citations omitted). Another Model Rule affected by technology-related amendments is Model Rule 5.3.

Responsibilities Regarding Nonlawyer Assistance. While the black-letter rule was unchanged, the comments to the rule were significantly revised to clarify the professional obligations of a lawyer outsourcing legal and nonlegal work within and outside the firm. In particular, a new Comment 3 to Model Rule 5.3 identifies the distinct concerns that arise when nonlegal services are performed outside the firm that involve technology:

A lawyer may use nonlawyers outside the firm to assist the lawyer in rendering legal services to the client. Examples include the retention of an investigative or paraprofessional service, hiring a document management company to create and maintain a database for complex litigation, sending client documents to a third party for printing or scanning, and using an Internet-based service to store client information. When using such services outside the firm, a lawyer must make reasonable efforts to ensure that the services are provided in a manner that is compatible with the lawyer’s professional obligations. The extent of this obligation will depend upon the circumstances, including the education, experience and reputation of the nonlawyer; the nature of the services involved; the terms of any arrangements concerning the protection of client information; and the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality. When retaining or directing a nonlawyer outside the firm, a lawyer should communicate directions appropriate under the circumstances to give reasonable assurance that the nonlawyer’s conduct is compatible with the professional obligations of the lawyer.

Id. (citations omitted).

Application of the ABA Ethical Rules to Cloud Services

As soon as a lawyer gives a third party access to his or her clients’ information—whether a copy service, an offsite storage facility, or a cloud service provider—that lawyer risks the loss of confidentiality. As discussed above, Model Rule 1.1 requires lawyers to obtain the requisite level of knowledge and understanding of the technology they use to understand and manage the risks triggered by the use of that technology. This includes taking reasonable precautions to ensure that the technology they use is adequate and consistent with their professional obligations. The following are potential risks that you, as a lawyer, should take into account when dealing with cloud services.

To paraphrase the adage, security begins at home. Your own access to the cloud should be secure, whether wired or wireless. Not only should the cloud service facility be secure, but your point of access should also be secure, as well as your means of transmission to and from the cloud. If you use portable devices such as smartphones, laptops, or tablets, those devices should be internally secured so that the data stored on them remains protected in case of loss or theft. Many law firms have implemented BYOD (bring your own device) policies, and you should ascertain whether your firm has such a policy and, if so, comply with it.

If you are using the cloud to transmit or store client information, you have two main categories of risks to consider: first, risks associated with the cloud service provider itself and any unauthorized third parties attempting to access your client data through that provider, and second, risks associated with your own ability to access client data from your provider as needed. To assess these risks, Comment 3 to Rule 5.3, discussed above, would recommend that you read the service agreement from the cloud service provider to understand the extent to which these risks are implicated by the service you have chosen. It may also be advisable, if not required (see, e.g., Office of the Comptroller of the Currency, OCC Bull. No. 2013-29, Risk Management Guidance (Oct. 30, 2013)), to document the due diligence you perform regarding your chosen cloud service provider, in case your judgment is second-guessed later. This due diligence is not a one-time event, but should be undertaken at regular intervals to ensure that your understanding of the cloud service remains up-to-date.
Your obligations regarding use of the cloud for client data can be heightened if circumstances indicate greater sensitivity of the data—for example, if your clients are subject to the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, or the Fair Credit Reporting Act; if your client’s information is controlled for export; or if you are handling very sensitive litigation or working on a confidential proposed transaction. In such circumstances, Model Rule 1.1 may require client consent to the use of cloud services. Your client engagement letters may also require you to notify the client of use of cloud services.

10 Important Considerations in Use of Cloud Services
These are 10 issues to consider when evaluating your cloud service provider:

(1) Is the provider reputable, experienced, and well-established? Does the provider have experience in protecting confidential and sensitive information? Is the provider likely to remain in business for the foreseeable future?

(2) What security measures and protocols does the provider have in place to prevent reasonably foreseeable confidentiality breaches, either by its own employees or by unauthorized third parties? For example, does the provider have firewalls, encryption, robust passwords, intrusion detection systems, employee background checks, and other similar protocols? Does the provider conduct periodic audits to monitor the effectiveness of its protocols? Does the provider regularly update these protocols to be consistent with current best practices, as they evolve to match the ingenuity of hackers?

(3) Is the provider relying on any third parties to maintain or support its servers? If so, who are those third parties, and what is their competence and experience in handling confidential or sensitive information?

(4) Where are the provider’s servers located? You will need to know which laws govern those servers and, in particular, whether any international or foreign privacy laws might apply to your client data stored on such servers. For the same reason, if the provider is relying on third parties to support its service, you will need to know where those third parties are located.

(5) Is the provider obligated to notify you promptly in the event of a confidentiality breach, and how does the service agreement define “promptly”? You have obligations of your own in the event of a data breach affecting one or more of your clients, which can vary from state to state; will your provider notify you in enough time for you to comply with your obligations?

(6) What does the service agreement provide with regard to ownership and licensing of data stored with your provider? The service agreement may be unclear or inappropriate regarding who owns or has the right to use the data stored with the provider. In this regard, remember that Model Rule 1.15 requires that client property be identified as property of the client. If you direct the provider to produce or provide access to client information stored with the provider, can the provider refuse to comply with that direction pending resolution of a dispute over billing or other matters? What is your right of access to client information stored with the provider pending such a dispute?

(7) What are the provider’s obligations in responding to subpoenas or other government or civil process? Is the provider obligated to notify you if it is served with process requiring production of your client’s information, and, if so, is that notice required to be provided in sufficient time to permit you to intervene and object to the subpoena? Is the provider empowered to resist production if appropriate and permissible?
(8) What happens to your stored data when the relationship between your firm and the provider ends? What is the provider’s obligation to return custody of the data to you and to purge and wipe any copies of the data on its servers? What are the provider’s obligations if it is bought or sold, if it goes into bankruptcy, or if it shuts down for any other reason?

(9) Does the service agreement allow your provider to unilaterally modify its privacy and acceptable use policies without notice to you?

(10) What is your recourse if something goes wrong? Does the provider’s service agreement contain a disclaimer or limitation of liability provision?

The answers to these questions are as varied as the service agreements themselves. But knowing the answers will help you to assess knowledgeably the risks associated with the cloud service you are considering and to take reasonable precautions against unauthorized breaches of confidentiality, consistent with your ethical obligations.

**Keywords:** litigation, commercial, business, technology, cloud services, confidentiality, data, ethics, Model Rule 1.1, Model Rule 1.6, Model Rule 1.16, Model Rule 5.3

Amelia Toy Rudolph is with Sutherland Asbill & Brennan LLP in Atlanta, Georgia.

“Ethical Considerations in Dealing with Expert Witnesses,” by George Carr, Commercial and Business 16:2, Winter 2015, pp. 11–16. © 2015 by the American Bar Association. Reprinted with permission. All rights reserved.
NEWS & DEVELOPMENTS

May 9, 2015
New York Embraces "Likely to Succeed" Standard for Appeals

The New York Court of Appeals, in a case of first impression, recently recognized the “likely to succeed” standard in appeals of an underlying case leading up to the commencement of an attorney malpractice action. Grace v. Law, 2014 WL 53253632014, N.Y. Slip Op. 07089 (N.Y. Oct. 21, 2014). In short, prior to commencing a legal malpractice action, a party who is likely to succeed on appeal of the underlying action should file an appeal so that the appellate courts are given the opportunity to correct a trial court mistake and essentially vindicate the attorney’s representation. Yet, under the standard set forth in Grace v. Law, if the client is not likely to succeed on appeal, he or she can file a legal malpractice action without first pursuing an appeal of the underlying action.

In Grace, the plaintiff began receiving treatment for an eye condition with a specific ophthalmologist at a Veterans Administration (VA) clinic. In June 2003, the VA canceled an appointment and did not reschedule the plaintiff until August 2004. At that 2004 appointment, the plaintiff was diagnosed with glaucoma and subsequently became blind in one eye. The plaintiff alleged that had the glaucoma been diagnosed at his initial appointment, his blindness would have been prevented. In June 2006, the plaintiff retained a law firm to commence a medical malpractice lawsuit against the VA; he was then referred to a second firm to continue the suit. The second firm learned that the doctor was not a VA employee but an independent contractor, and it referred the case back to the original firm due to a conflict of interest. The plaintiff eventually amended his complaint to name the correct employer, but the court dismissed the claims against the doctor and new defendant as time-barred.

The plaintiff then sued both firms for legal malpractice for failing to timely sue the doctor and his correct employer. The firms argued that because the plaintiff had not appealed the dismissal of his medical malpractice action, he could not maintain the legal malpractice claim. The defendants argued that the plaintiff was estopped from commencing the legal malpractice action and moved for summary judgment on this issue. The trial court denied their motions.

The New York Court of Appeals recognized that previous lower court decisions “generally stand for the proposition that an attorney should be given the opportunity to vindicate him or herself on appeal of an underlying action prior to being subjected to a legal malpractice suit.” However, the court decided that there should be an exception to the general rule, pointing to decisions from other jurisdictions. To apply the “likely to succeed” standard, courts will determine whether a client can commence a legal malpractice action without taking an appeal in the underlying action based on the likelihood of success of that underlying appeal. The court opined that this standard was the “most efficient and fair to all parties.” Furthermore, because courts are routinely required to analyze whether the plaintiff would have been successful on the merits (i.e., a “case within a case”), the new standard aligned with typical analysis in malpractice actions.

In Grace, the court determined that the defendants failed to establish that the plaintiff was likely to succeed on appeal and affirmed the denial of summary judgment. The upshot of this new standard is that claimants will no longer be required to exhaust the appeal process for cases with little chance of success prior to suing for malpractice. One such example would be a decision involving a claim clearly barred by the statute of limitations. To make use of this defense in circumstances where an appeal could be meritorious, defendants will now need to provide sufficient evidence to show that the plaintiff would have been successful on the underlying appeal. But this approach poses difficulties. For one, it requires the client or subsequent malpractice counsel to make fundamental assumptions on how an appellate court would rule. This approach seems rooted in uncertainty leading many practitioners to follow the safest practice, which is to take an appeal as a matter of course before filing the malpractice lawsuit.
Recent SEC Publications Address Cybersecurity

In a February 3, 2015 press release, the Securities and Exchange Commission (SEC) announced its publication of a risk alert and an investor bulletin addressing cybersecurity risks at brokerage and advisory firms. These publications provide tips to investors, and also may be useful for broker-dealers and investment advisors to consider in addressing cybersecurity issues at their firms.

According to SEC Chair Mary Jo White, “[c]ybersecurity threats know no boundaries. That’s why assessing the readiness of market participants and providing investors with information on how to better protect their online investment accounts from cyber threats has been and will continue to be an important focus of the SEC . . . Through our engagement with other government agencies as well as with the industry and educating the investing public, we can all work together to reduce the risk of cyber attacks.”

The risk alert, from the SEC’s Office of Compliance Inspections and Examinations, contains information based on examinations of more than 100 broker-dealers and investment advisers. The risk alert provides information on how these various firms:

- identify cybersecurity risks;
- establish cybersecurity policies, procedures, and oversight processes;
- protect their networks and information;
- identify and address risks associated with remote access to client information, funds transfer requests, and third-party vendors;
- detect unauthorized activity.

Some of the examined firms’ procedures to address cybersecurity threats that the risk alert highlights include conducting firm-wide inventorying, cataloguing, or mapping of their technology resources, conducting periodic audits to ensure compliance with written information-security policies, and having a written policy to address how to determine whether the firm is responsible for client losses associated with cyber incidents. The risk alert also notes that many of the examined firms identify best practices through both formal and informal information-sharing networks, such as the Financial Services Information Sharing and Analysis Center (FS-ISAC). Underlining the importance of assessing and protecting against cybersecurity threats, the risk alert notes that 88 percent of the broker-dealers and 74 percent of the advisers included in the examination stated that they have experienced cyber-attacks directly or through one or more of their vendors, the majority of which related to malware and fraudulent emails.

The Investor Bulletin, issued by the SEC’s Office of Investor Education and Advocacy, provides key suggestions to help investors protect online investment accounts, including:

- pick a “strong” password
- use two-step verification
- exercise caution when using public networks and wireless connections

© 2015 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.
According to Office of Investor Education and advocacy director Lori J. Schock, "[t]his bulletin provides everyday investors with a set of useful tips to help protect themselves from cyber-criminals and online fraud."

Such practical information may prove useful to many firms in assessing how to shape and implement their own cybersecurity policies and procedures.

**Keywords:** litigation, cybersecurity, professional services liability, SEC

EDITORIAL BOARD

Newsletter Editors
» Patricia A. Gorham
» Saleel Sabnis

Committee Cochairs
» Bernard Amyot
» Carey Menasco

Web Editors
» Jonathan Walsh

Staff Editor
» J.R. Haugen

The views expressed herein are those of the author(s) and do not necessarily reflect the positions or policies of the American Bar Association, the Section of Litigation, this committee, or the employer(s) of the author(s).

ABA Section of Litigation Professional Services Liability Committee
http://apps.americanbar.org/litigation/committees/professional