BY HOWARD M. PRIVETTE, D. SCOTT CARLTON, AND SARAH KELLY-KILGORE

The SEC Guidance on Cybersecurity Measures for Public Companies

DATA BREACHES INVOLVING the personal information of consumers have recently appeared prominently in headlines. In California, for example, it is estimated that over 2.5 million residents were put at risk by data breaches in 2012, including five major breaches that each affected the personal information of 100,000 or more people.[1] California businesses, which must give notice when a data breach results in unauthorized access to the unencrypted personal information of consumers, are under siege. As recently highlighted by an SEC roundtable, cybersecurity—including the issue of whether and how to disclose a breach—is receiving considerable scrutiny from legislators and regulators.

Disclosure of cybersecurity problems by public companies, for example, presents an interesting confluence of policy considerations for which there is still no consensus. On the one hand, investors may be interested in whether and to what extent a corporation may be burdened by cybersecurity expenses—whether they be the cost of building defenses or the losses arising from a breach. On the other hand, detailed discussion of the value of vulnerable assets or the reasons for their vulnerability may attract predators.

So far, the SEC has been taking a measured approach to the cybersecurity disclosure issue. In October 2011, the staff of the SEC's Division of Corporate Finance published written guidance.[2] The guidance followed a May 2011 letter from five senators to then-SEC Chair Mary Schapiro requesting that the commission "develop and publish interpretative guidance clarifying existing disclosure requirements pertaining to information security risk, including material information [about] security breaches involving intellectual property or trade secrets."[3] Although the guidance does not create any new rule or regulation, it does respond to the senators' request by offering the views of the corporate finance staff on how public companies may assess what disclosures should be provided about cybersecurity matters. The staff discussed the need to disclose risks that have materialized into breaches and risks of future incidents.[4]

In the October 2011 guidance, the staff notes that while no existing rules or regulations explicitly refer to the need for cybersecurity disclosure, a number of existing SEC requirements are broad enough to potentially encompass the issue. In particular, the staff opines that various provisions of the SEC's Regulation S-K[5] could touch on the need for cybersecurity disclosures in a company's periodic reports filed with the SEC. For example, citing Item 503(c) of Regulation S-K, the staff suggests that a company may consider disclosing "the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky." In addition, citing Item 303 of Regulation S-K, the staff indicates that a company may want to address cybersecurity matters in the section of its periodic filings devoted to "Management's Discussion and Analysis of Financial Condition and results of Operations." The section covers known incidents or risks of possible incidents that reach the level of a "material event, trend, or uncertainty that is reasonably likely to have a material effect on [a company's] results of operations, liquidity, or financial condition or would cause reported financial information not to be necessarily indicative of future operating results or financial condition." The staff also notes Item 103 of Regulation of S-K, which requires a brief description of material pending legal proceedings.[6]

RICHARD EWING

Apart from the technical discussion of which existing rules and regulations might be implicated by cybersecurity issues, the Corporate Finance staff made three general observations. First, the guidance recognizes that an assessment of whether and to what extent cybersecurity disclosures should be made in light of each company's "specific facts and circumstances." There is no one-size-fits-all analysis. Second, the staff states that "we are mindful of potential concerns that detailed disclosures could compromise cybersecurity issues—for example, by providing a 'roadmap' for those who seek to infiltrate a [company's] network security" and, therefore, "we emphasize that disclosures of that nature are not required under the federal securities

Howard M. Privette is a partner, and D. Scott Carlton and Sarah Kelly-Kilgore are associates, in the Los Angeles office of Paul Hastings LLP, where they focus on securities litigation and enforcement matters for U.S. and global clients.

laws." Third, in a related point, the staff explains that while companies "should provide disclosure tailored to their particular circumstances and avoid generic 'boilerplate' disclosure, we reiterate that the federal securities laws do not require disclosure that itself would compromise a [company's] cybersecurity."[7]

On this last point, the staff recommends that while companies should not make a disclosure that would compromise cybersecurity, they "should provide sufficient disclosure to allow investors to appreciate the nature of the risks faced by the particular [company] in a manner that would not have that consequence." The guidance does not explain how to do so. The tension between the risk of disclosure and the risk of nondisclosure may help explain the SEC's approach to cybersecurity after the guidance was published, which generally has been to evaluate the issue on a case-by-case basis.

SEC Practice after the Guidance

According to SEC Chair Mary Jo White, in the 18 months following publication of the guidance, the Corporate Finance staff issued comments addressing cybersecurity matters to approximately 50 public companies of varying size and in a wide variety of industries.[8] Many comments focus on disclosure of past incidents.

For example, in a case in which a company stated that it "continue[s] to face increasing cyber security threats," the staff requested that the company provide it information on whether the company had experienced any "breaches, hacker attacks, unauthorized access and misuse, computer viruses and other cybersecurity risks and events in the past and, if so, what consideration you have given to disclosing such events in your risk factors."[9] In a similar case, the staff asked for information about whether a company had experienced any security breaches or attacks, even if they had not resulted in an adverse effect. The staff indicated that if the company had experienced such incidents, it should consider making investors aware.[10]

In a somewhat different vein, the staff has expressed doubt when companies claim that access to their computer systems by unauthorized users is unlikely. For example, in commenting on a foreign company's registration statement containing such an assertion, the staff requested that "[g]iven the risks associated with cybersecurity breaches," the company should "please consider revising" this assertion and, "[f]urthermore, tell us what consideration you gave to including risk factor disclosure."[11]

Some have questioned whether more should be done. In April 2013, Senator John D. Rockefeller IV wrote to White to urge that she make cybersecurity one of her highest priorities.[12] Rockefeller explained that he "applauded" the October 2011 guidance "as an important first step in the right direction," and noted that "it certainly made a positive impact on disclosures." However, he opined that public company "disclosures are generally still insufficient for investors to discern the true costs and benefits of companies' cybersecurity practices."

Rockefeller tied his concerns about the sufficiency of corporate cybersecurity disclosures to his general concern that the United States is not adequately protecting itself with respect to cybersecurity. He asserted that "[i]nvestors deserve to know whether companies are effectively addressing their cybersecurity risks," calling this information "indispensable to efficient markets." He explained his belief that, "as a country, we need the private sector to make significant investments in cybersecurity," and suggested that "[f]ormal guidance from the SEC on this issue will be a strong signal to the market that the companies need to take their cybersecurity efforts seriously." Thus, "given the growing significance of cybersecurity on investors' and stockholders' decisions, the SEC should elevate [the staff's] guidance and issue it at the Commission level as well."[13]

In her letter responding to Rockefeller, White agreed that cybersecurity disclosure "is a very important issue that is of increasing concern for public companies, our financial markets, and the nation." However, she demurred on the senator's request that the SEC elevate the existing Corporate Finance staff guidance to the Commission level, equating cybersecurity risks "with other business risks" that should be "among the factors a public company would consider in evaluating its disclosure obligations." Nevertheless, she praised the efforts of the SEC staff in promulgating the October 2011 guidance and in reviewing companies' disclosures, highlighting the number and breadth of the comments provided to individual companies on cybersecurity issues. White emphasized that the SEC staff "continues both to prioritize this important matter in its review of public company disclosures and to issue comments concerning cybersecurity." She also explained that the staff "is actively engaged in discussing publicly both cybersecurity matters and the guidance to remind public companies of the staff's view of the importance of cybersecurity disclosure" and "is using the information gathered through these efforts to evaluate the efficacy of the guidance." She concluded by telling the senator that she has "asked the staff to provide [her] with a briefing of the current disclosure practices and overall compliance with the guidance, as well as any recommendations they have regarding further action in this area."[14]

In the months following the exchange between Rockefeller and White, a series of high-profile data breaches rattled the public. In December 2013, for example, Target Corporation announced a data breach resulting in the theft of approximately 40 million credit and debit card account numbers. Then, in January 2014, the Neiman Marcus Group confirmed that a similar theft had occurred at its stores, resulting in a spike in fraudulent credit and debit charges on cards that had been used at those stores. In February, Las Vegas Sands Corporation, the world's largest casino company, revealed a cybersecurity breach that resulted in the theft of customer and employee data. These breaches echo previous events like those at T.J. Maxx in 2006, which resulted in the theft of approximately 45 million credit and debit card account numbers. Overall, according to the Identity Theft Resource Center, 2013 was a record year, with more than 600 breaches reported nationwide.

In the face of these events, in March the SEC hosted a roundtable to focus on cybersecurity and the challenges it raises for American companies, regulators, and law enforcement agencies. Participants included all five SEC commissioners, high-ranking officials from other government agencies, and industry leaders from the private sector. The issue of the disclosure obligations of public companies generated considerable discussion. Although the panelists participating in the roundtable seemed to agree that cybersecurity is of growing importance to market participants, there was little consensus on how best to address the issue of disclosure.[15]

Comments from the commissioners are illustrative. In her opening remarks, White focused on the materiality standard that is applicable generally to all financial disclosures. In contrast, the comments of Commissioner Kara Stein suggested that cybersecurity matters may need to be disclosed even absent materiality.[16] Other panelists, particularly those from the private sector, cautioned that the SEC should tread lightly in considering whether to change reporting requirements. Roberta Karmel, a former SEC commissioner and current law professor, suggested that disclosure may not be in the public's interest. Heavy-handed disclosure requirements could exacerbate risk by bringing breaches to the attention of those who may seek to exploit them, and, as the private sector participants argued, greater disclosure obligations could result in greater litigation risk without any increased investor protection. Commissioner Luis A. Aguilar may have summarized best: "There is no doubt that the SEC must play a role in this area. What is less clear is what that role should be."[17]

The SEC's interest in cybersecurity disclosures extends both to incidents that have

already occurred and to the risk of future incidents. The staff's comment letters, for example, have pushed companies for more information about the occurrence of past incidents and questioned how this history might reflect on the nature and scope of the risks that companies face.

Notably, public companies in the United States are already subject to a web of state laws mandating notice of data breaches involving the personal information of consumers. In this regard, California has been a leader in the field and is generally regarded as having among the most comprehensive rules.[18] Under California law, public and private companies doing business in California or with California residents are required to give notice when a data breach results in unauthorized access to certain unencrypted personal information of consumers.[19] If a breach triggers a company's disclosure obligations, the business must notify any and all California residents whose personal information was acquired, or is believed to have been acquired, "in the most expedient time possible and without unreasonable delay."[20] While comprehensive, California's notification requirement does not take into consideration the consequences resulting from the manner and timing of notification with respect to federally regulated securities.

The confluence of state consumer notification requirements and federal securities litigation is illustrated by the case of ChoicePoint. A spinoff from Equifax, the company aggregated personal data sourced from multiple public and private databases for sale to the government and the private sector. In 2005, it became the target of a shareholder securities class action alleging that the company had misrepresented the security of the private data it collected and sold. According to the allegations of the shareholder complaint, California law enforcement alerted ChoicePoint in September 2004 that criminals had gained access to its databases and were using stolen personal information. In turn, this triggered California's requirement to notify consumers of the theft of their personal information.[21]

According to the shareholder complaint, after receiving this alert from California law enforcement but before sending out the requisite consumer notices, ChoicePoint continued to issue press releases and file reports with the SEC that contained rote statements concerning the company's commitment to protecting private information. In addition, a number of senior officers sold millions of dollars of stock. Then, in early February 2005, without making any other public statement or announcement, the company began mailing the consumer notices required by California law. Within a week, the media began reporting on the matter, and soon there was a series

of news items and statements by the company that eventually disclosed that the breach covered by the California notices extended nationwide and had been preceded by similar breaches in the past. The private shareholder litigation commenced after an announcement of investigations by both the SEC and the FTC, and a drop in the company's stock price. After the company's motion to dismiss the shareholder litigation was denied, the case eventually settled for $10 million.[22]

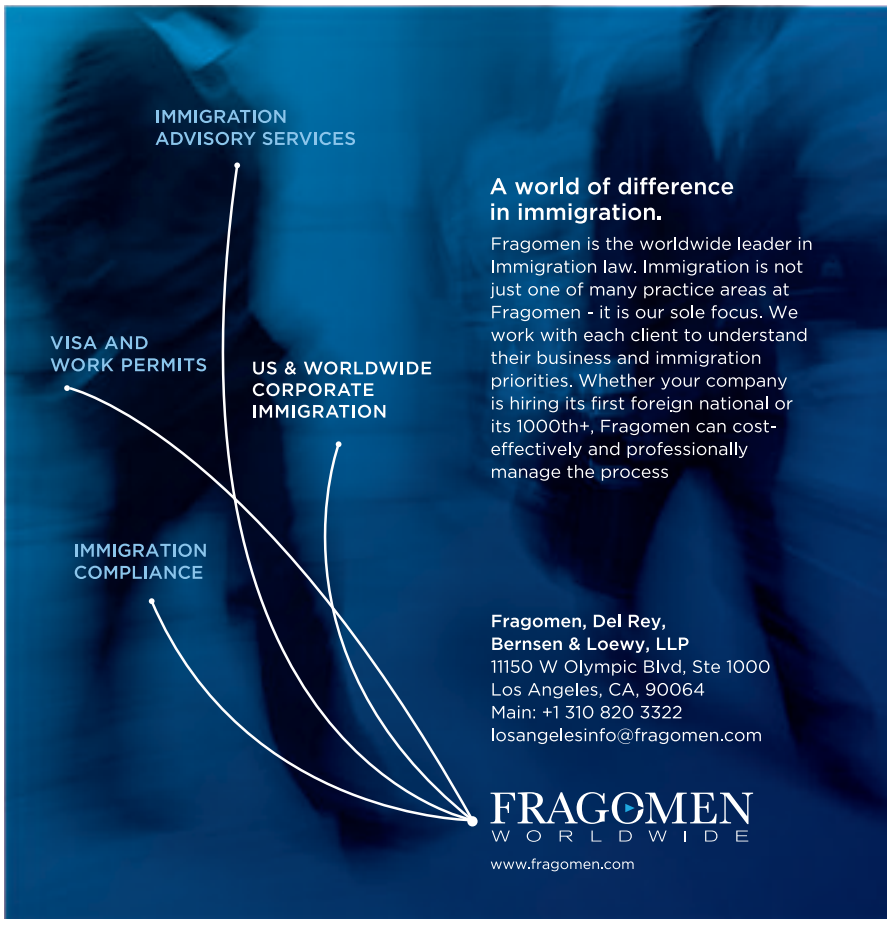
Securities Litigation Considerations

At the March 2014 SEC roundtable, private-sector panelists expressed concern that requiring increased disclosure of cybersecurity matters may lead to more shareholder class actions and derivative lawsuits. As an example, between 2005 and 2007, infamous hacker Albert Gonzalez and his accomplices targeted multiple companies, including TJX Companies (T.J. Maxx, Marshalls, and other retail chains) and Heartland Payment Systems.[23] The data breaches caused by Gonzalez's group ultimately resulted in the theft and sale of more than 90 million credit and debit card account numbers.[24] While TJX disclosed the data breach, other companies did not. As a result, according to Douglas Meal, a panelist at the SEC's cybersecurity roundtable, TJX experienced "all kinds" of litigation burdens while other companies that had been breached by the same hacking group did not.[25]

However, it is a dubious proposition that the absence of cybersecurity disclosures will insulate a company from shareholder litigation. As the SEC's staff guidance and ongoing review of cybersecurity issues make clear, the SEC considers these issues to be within the scope of existing disclosure requirements. Therefore, a public company that fails to address cybersecurity adequately in its filings will very likely find itself to be the subject of SEC scrutiny and, if a cyber incident occurs, the lack of disclosure itself may result in private shareholder litigation.

This point is illustrated by the case of Wyndham Worldwide Corporation. WWC was the target of a series of data breaches from April 2008 to January 2010. These breaches resulted in an investigation and a high-profile lawsuit by the FTC, alleging that WWC's security practices were unfair and deceptive.[26] In 2014, a shareholder derivative lawsuit was filed, piggybacking on these allegations and seeking to bring breach of fiduciary duty claims against WWC's board of directors and several of its executives (including the general counsel).[27] The shareholder also complained that the company did not disclose the data breaches until it announced the filing of the FTC's lawsuit in a Form 10-Q with the SEC in July 2012, more than two and-a-half years after the occurrence of the last breach.[28] That disclosure was also the subject of a comment letter sent by the SEC a week after the Form 10-Q was filed. Noting that WWC's filing included a discussion of the risk of future cyber incidents, and referring to the October 2011 Corporate Finance disclosure guidance, the August 1, 2012, comment letter requested that, "[b]eginning with your next Form 10-Q, please state that you have experienced data breach incidents in the past in order to provide the proper context for your risk factor disclosure."[29]

Ultimately, the question is not whether a publicly held company should provide cybersecurity disclosures, but how it should do so effectively. Heartland's experience provides an example of how disclosures can help defeat shareholder litigation. In 2009, a group of investors sued Heartland in the District Court of New Jersey, alleging that Heartland had fraudulently concealed the occurrence of the data breach and fraudulently misrepresented the general state of Heartland's cybersecurity.[30] The court, evaluating Heartland's motion to dismiss, explained that omissions are "only fraudulent in the presence of a duty to disclose, which usually arises only when there is insider trading, a statute requiring disclosure, or an inaccurate, incomplete,



or misleading prior disclosure."[31]

Further, the court explained, "[T]here is no general duty on the part of issuers to disclose every material fact to investors."[32] Finding that Heartland had no duty to disclose the data breach when it occurred, the court determined that Heartland's subsequent statements regarding the general state of its security did not amount to fraudulent concealments or misrepresentations.[33] In effect, the court recognized that there is no statute expressly requiring the disclosure of cybersecurity incidents and, so long as a company has not otherwise made an inaccurate, incomplete, or misleading disclosure on cybersecurity matters, no legal liability should attach to the failure to disclose.

As cybersecurity becomes a more critical part of modern business, the laws and regulations addressing cybersecurity will continue to evolve. Whether this will lead to specific new disclosure standards and requirements for public companies in the United States, however, remains an open question. In the meantime, companies addressing these issues should pay careful attention to the October 2011 guidance before deciding whether and how to make disclosures. A step in the wrong direction—which could be either too much or too little disclosure—may lead to greater litigation risks or greater scrutiny from the SEC. ■

---

[1] KAMALA D. HARRIS, DATA BREACH REPORT 2012 (2012), *available at* http://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/2012data_breach_rpt.pdf.

[2] SEC, DIV. OF CORP. FIN., CF DISCLOSURE GUIDANCE: TOPIC NO. 2: CYBERSECURITY (2011) [hereinafter GUIDANCE], *available at* http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[3] *See* Letter from Sens. John D. Rockefeller IV, Robert Menendez, Sheldon Whitehouse, Mark Warner & Richard Blumenthal, to Mary Schapiro, Chair, SEC (May 11, 2011), *available at* http://www.commerce.senate.gov.

[4] *See* GUIDANCE, *supra* note 2.

[5] Standard Instructions for Filing Forms under Securities Act of 1933, Securities Exchange Act of 1934 and Energy Policy and Conservation Act of 1975—Regulation S-K, 17 C.F.R. §229.10-.1208 (2011).

[6] The staff also indicated that cybersecurity issues may be considered under Items 101 and 307 of Regulation S-K and cited several specific accounting standards applicable to corporate financial statements that may be implicated by costs incurred as a result of cyber incidents. *See* Regulation S-K, 17 C.F.R. §§229.10-1208 (2011).

[7] *See* GUIDANCE, *supra* note 2.

[8] *See* Letter from Mary Jo White, Chair, SEC, to Sen. John D. Rockefeller, IV, Chairman, Comm. on Commerce, Sci., & Transp. (May 1, 2013), *available at* http://www.commerce.senate.gov.

[9] *See* Letter from Suzanne Hayes, Assistant Dir., SEC, to James J. Malerba, Exec. Vice President, Corporate Controller & Chief Accounting Officer, State Street Corp. (Apr. 9, 2012), *available at* http://www.sec.gov.

[10] *See* DELOITTE & TOUCHE, SEC COMMENT LETTERS—INCLUDING INDUSTRY INSIGHTS: CONSTRUCTING CLEAR DISCLOSURES 67 (7th ed. 2013).

[11] *See* Letter from Maryse Mills-Apenteng, Special Counsel SEC, to Dana Gallovicova, Chief Enforcement Officer, Zlato Inc. (June 11, 2013), *available at* http://www.sec.gov.

[12] *See* Letter from Sen. John D. Rockefeller IV, Chair, Comm. on Commerce, Sci. & Transp., to Mary Jo White, Chair, SEC (Apr. 9, 2013), *available at* http://www.commerce.senate.gov.

[13] Letter from John D. Rockefeller IV to Mary Jo White, Chair, SEC (Apr. 9, 2013), *available at* http://www.privacyandsecuritymatters.com/files/2013/04/Rockefeller-SEC-letter.pdf.

[14] Letter from Mary Jo White, Chair, SEC, to Sen. John D. Rockefeller, IV, Chairman, Comm. on Commerce, Sci., & Transp. (May 1, 2013), *available at* http://www.commerce.senate.gov.

[15] Following the SEC's roundtable in March 2014, the SEC has received several comment letters from academics, software companies, and other interested parties generally expressing support for the SEC's efforts to provide guidance to public companies. *See* Comments on Cybersecurity Roundtable, *available at* http://www.sec.gov/comments/4-673/4-673.shtml.

[16] *See* Susan D. Resley et al., SEC Hosts Roundtable on Cybersecurity Issues and Challenges (Mar. 31, 2014), http://www.lexology.com.

[17] Commissioner Aguilar has also indicated that directors of public company boards should more proactively confront the risks of cyber-attacks, including by encouraging boards to follow the guidelines set forth by the National Institute of Standards and Technology regarding best practices for managing cybersecurity risks. *See* Luis A. Aguilar, Commissioner of the U.S. Securities and Exchange Commission, Cyber Risks and the Boardroom, Conference at the New York Stock Exchange (June 10, 2014).

[18] *See* CIV. CODE §§1798.80-1798.84. Effective Jan. 1, 2014, Civil Code §§1798.80-1798.84 were amended to include a "user name or email address, in combination with a password or security question and answer that would permit access to an online account" in the definition of electronic personal information. *See* CIV. CODE §§1798.82(h)(2).

[19] *See* CIV. CODE §§1798.82.

[20] *See* CIV. CODE §§1798.82(a). California's Office of Privacy Protection recommends that notice be provided within 10 business days of an organization's determination that personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

[21] *See* In re Choicepoint, Inc., Sec. Litig., No. 1:05-cv-00686-JTC, 2006 U.S. Dist. LEXIS 97903, at *3-7 (N.D. Ga. Nov. 19, 2006).

[22] Stipulation of Settlement, In re Choicepoint, Inc., Sec. Litig., No. 1:05-cv-00686-JTC (N.D. Ga. Mar. 7, 2008) (No. 66).

[23] *See* Kim Zetter, *TJX Hacker Gets 20 Years in Prison*, WIRED (Mar. 25, 2010), http://www.wired.com/2010/03/tjx-sentencing.

[24] *See id.*

[25] Joel Schectman, *When to Disclose a Data Breach: How about Never?*, WALL ST. J. (Mar. 27, 2014), http://blogs.wsj.com/riskandcompliance/2014/03/27/when-to-disclose-a-data-breach-how-about-never.

[26] There is considerable controversy over the FTC's claim of statutory authority to regulate cybersecurity matters. However, U.S. District Judge Esther Salas's decision in *Wyndham* upheld the FTC's authority in that case. *See* FTC v. Wyndham Worldwide Corp., No. 2:13-cv-01887-ES-JAD, ____ F. Supp. 2d ____, 2014 WL 1349019, at *6-7 (D. N.J. Apr. 07, 2014).

[27] Complaint at 1-4, Palkon v. Homes, No. 2:14-cv-01234-SRC-CLW (D. N.J. May 2, 2014) (No. 12).

[28] *See id.* at 3.

[29] *Id.* at 25.

[30] *See* In re Heartland Payment Sys., Inc. Sec. Litig., No. 09-1043 (D. N.J. Dec. 7, 2009).

[31] *Id.* at 10 (internal quotation marks and citations omitted).

[32] *Id.* at 11.

[33] *See id.*

THE NATIONAL ACADEMY OF DISTINGUISHED NEUTRALS

Selecting A Top-Tier Neut

CALIFORNIA'S FOREMOST MEDIATOR

The Academy is pleased to recognize over 60 m


Lynne S. Bassis
(213) 683-1600


John Bates, Jr.
(510) 220-0102


Michael J. Bayard
(213) 383-9399


Daniel Ben-Zvi
(310) 201-0010


Lee Jay Berman
(310) 203-0700


Hon. Steven Cohen
(310) 315-5404


Greg Derin
(310) 552-1062


Michael Diliberto
(310) 201-0010


William Fitzgerald
(310) 440-9090


Kenneth C. Gibbs
(213) 253-9776


Ronald Mandell
(310) 271-8912


Christine Masters
(818) 955-8518


Steve Mehta
(661) 284-1818


Jeffrey Palmer
(626) 795-7916


Hon. Layn Phillips
(949) 760-5288

At **www.CaliforniaNeutrals.org** you can search by subject matter expertise, location and preferred ADR service in just seconds. You can also determine availability by viewing many members' ONLINE CALENDARS, finding the ideal neutral for your case in a way that saves both time and money.

The Academy is an invite-only association of over 900 mediators and arbitrators across the US, all of whom have substantial experience in the resolution of commercial and civil disputes. All members have been recognized for their accomplishments through the Academy's peer nomination system and extensive attorney-client review process. In 2013, NADN was appointed exclusive Neutrals Database Partner to the nation's largest plaintiffs bar association (AAJ) & defense bar association (DRI).

To access our free National Directory of over 900 litigator-rated mediators & arbitrators, please visit *www.NADN.org/directory*

VISIT OUR CALIFORNIA CHAPTER MEMBERS AT

WWW.CALIFORNIANEUTRALS.ORG

ral Has Never Been Easier

s & Arbitrators Profiled Online

embers across Southern California, including...

Viggo Boserup
(714) 937-8252

Ernest C. Brown
(800) 832-6946

Kenneth Byrum
(661) 861-6191

George Calkins
(310) 309-6206

R.A. Carrington
(805) 565-1487

Reginald Holmes
(626) 432-7222

Joan Kessler
(310) 552-9800

Linda Klibanow
(626) 204-4000

Louise LaMothe
(805) 563-2800

Leonard Levy
(310) 201-0010

Barry Ross
(818) 840-0950

Deborah Rothman
(310) 452-9891

Henry Silberberg
(310) 276-6671

Ivan K. Stevenson
(310) 782-7716

Hon. John Leo Wagner
(800) 488-8805

To find the best neutral for your case, visit our California members at

www.CaliforniaNeutrals.org

Need a top-rated mediator /arbitrator outside of California? Visit www.NADN.org

SmartPhone Link