2018 Edition

CENTER FOR ADVANCED DUE DILIGENCE STUDIES

OCCASIONAL SCHOLARLY PAPERS SERIES

CADDS Scholars Press

www.cadds-edu.org

OCCASIONAL SCHOLARLY PAPERS SERIES

Morgan Francy, J.D.
SMU Dedman School of Law, 2018

Robert C. Uhl, J.D.
SMU Dedman School of Law, 2018

G.M. Lawrence, J.D.
Vanderbilt Law School, 1983

Edited by CADDS Editorial Staff

CADDS Scholars Press

OCCASIONAL SCHOLARLY PAPERS SERIES

2018 Edition

Table of Contents

UNDERWRITER DUE DILIGENCE AND OUTDATED INFORMATION INCORPORATED BY REFERENCE IN SHELF TAKEDOWNS

Morgan Francy*

INTRODUCTION

In the more than thirty-five years since the Securities and Exchange Commission's ("SEC") adoption of the integrated disclosure[1] and shelf registration[2] systems, many issuers have taken advantage of the availability of expedited offerings to quickly access the public securities markets when funding needs and perceived favorable market conditions align.[3] However, because shelf registrations for qualifying domestic issuers often involve incorporation by reference of an issuer's periodic reports under the Securities Exchange Act of 1934 (the "Exchange Act"), underwriters face unique due diligence and reliance-based decision challenges.[4] Many of these have been addressed in regulatory pronouncements and explored in scholarly and practitioner literature over the years.[5] However, one area that has received virtually no attention is the potential that some information incorporated by reference may have become outdated or been superseded by more recent disclosures, and how such a situation may bear on an underwriter's access to the affirmative due diligence defenses under the Securities Act of 1933 (the "Securities Act").

---

* J.D., SMU Dedman School of Law, 2018; B.B.A. in Marketing and B.S. in Applied Physiology and Sport Management, Southern Methodist University, 2014.

[1] The integrated disclosure system is a system designed to coordinate the disclosure requirements of the Securities Act of 1933 (the "Securities Act") and the Exchange Act of 1934 (the "Exchange Act"). *See* LOUIS LOSS & JOEL SELIGMAN, SECURITIES REGULATION § 2-D-1 (3d ed. 1988). In 1967, the SEC appointed Commissioner Francis Wheat to lead a study of the extent to which disclosure could improve the Commission's rule-making power. The result of the group's effort was a report analyzing the then current regulatory problems and laid the groundwork for the development of an integrated disclosure system. *See* Disclosure to Investors – A Reappraisal of Federal Administrative Policies under the '33 and '34 Acts, Report and Recommendations to the SEC from the Disclosure Policy Study (Mar. 27, 1969) [commonly referred to as "The Wheat Report"]; s*ee also* Adoption of Integrated Disclosure System, SEC Release 33-6383 (Mar. 3, 1982).

[2] *See* Shelf Registration, SEC Release 33-6499 (Nov. 17, 1983); 17 C.F.R. § 230.415. SEC Rule 415 under the Securities Act expanded the availability of shelf registration to primary debt and equity offerings. *See* LOSS & SELIGMAN, *supra* note 2, § 2-A-5.

[3] *Id.*

[4] *See* Circumstances Affecting the Determination of What Constitutes Reasonable Investigation & Reasonable Grounds for Belief Under Section 11 of the Securities Act, SEC Release 33-6335 at *11-13 (Aug. 6, 1981); ABA DUE DILIGENCE TASK FORCE REPORT at 1219.

[5] *See id.*

This paper aims to address the void by examining, albeit briefly, underwriter due diligence and reliance where the issuer has incorporated by reference outdated or superseded information in the offering documents for a shelf takedown. Initially, I offer an overview of shelf registrations/shelf takedowns and the concept of incorporation by reference. Next, I examine SEC Rule 412 regarding outdated information incorporated by reference and one example of a judicial interpretation of the rule. Finally, I offer selected guidance to underwriters regarding these matters.

SHELF TAKEDOWNS AND INCORPORATION BY REFERENCE

Overview

A shelf registration statement is a filing with the SEC for a public offering where the issuer intends to offer the securities on a continuous or delayed basis.[6] Once a shelf registration statement has been declared effective by the SEC, the issuer generally is free to issue the securities at a later date or over time.[7] Thus, shelf registration allows issuers to offer the securities whenever it feels that market conditions are favorable without the requirement of further SEC review.[8] This initial registration process is referred to as the "shelf registration" and any subsequent offering thereafter is referred to as a "shelf takedown."[9]

Notwithstanding the use of a shelf registration statement, the issuer also is required to prepare a prospectus supplement for each specific shelf takedown.[10] Where incorporation by reference is permitted, the prospectus supplement is typically a relatively abbreviated document (because information contained in the issuer's periodic reports that are filed under the Exchange Act, such as in its annual Form 10-K or proxy statement, are merely referenced, not reproduced).[11] Only

[6] 17 C.F.R. § 230.415. *See* SEC Release 33-6499, *supra* note 3.

[7] *Id.*

[8] *Id. See also Shelf Registration*, INVESTOPEDIA, https://www.investopedia.com/terms/s/shelfregistration.asp (last visited April 22, 2018).

[9] GARY M. LAWRENCE, DUE DILIGENCE: LAW, STANDARDS, AND PRACTICE 545 (1st ed. 2016).

[10] *See* Morrison & Foerster LLP, *Frequently Asked Questions About Shelf Offerings* (2017), *https://media2.mofo.com/documents/faqshelfofferings.pdf*.

[11] William K. Sjostrom, Jr., *The Due Diligence Defense Under Section 11 of the Securities Act of 1933*, 44 BRANDEIS L.J. 549, 560 (2006).

qualifying well-known seasoned issuers are permitted to use incorporation by reference.[12] As a result, in most instances, the prospectus supplement includes only new or updated information.[13]

The expedited timeframe for shelf takedowns and the incorporation by reference of certain information (especially considering that the underwriters may not have participated in drafting that referenced information) can present challenges for underwriters in performing due diligence investigations and making reliance-based decisions. Thus, while the ability to issue securities quickly and incorporate information already in the public domain is highly valuable to issuers, it presents due diligence and reliance-based decision complications for the underwriters.

Underwriter Due Diligence in Shelf Takedowns

The Securities Act provides for a number of causes of actions as well as defenses in performing due diligence. Under Section 11 of the Securities Act, any person who purchases a security issued pursuant to a public offering document that contains a material misstatement or omission has a private cause of action.[14] Section 12(a)(2) of the Securities Act also prohibits sellers from making materially false or misleading statements in a prospectus or oral communication.[15] Underwriters can be liable for violations of these sections, but also have two affirmative due diligence defenses under Section 11: a "reasonable investigation" defense for portions of the offering documents that are not expertised statements and a "reasonable reliance" defense for the portions of the offering documents that are expertised statements.[16] Similarly, Section 12(a)(2) offers a third affirmative due diligence defense ("reasonable care") provided the defendant can prove that it "did not know, and in the exercise of reasonable care, could not have known, of [the] untruth or omission."[17] Thus, one of the underwriters' primary concerns in conducting due diligence and making reliance-based

[12] *See* Morrison & Foerster, *supra* note 11. Well-known season issuers must register their securities on either Form S-3 or F-3 and meet other requirements of a "primary eligible" issuer under the applicable SEC Rules. *See* 17 C.F.R. 239.13; 17 C.F.R. 239.33.

[13] Eric Seitz, Comment, *Underwriter Due Diligence: It's [Not] a Whole New Ballgame*, 61 SMU L. REV. 1633, 1648 (2008) ("Normally, the only 'new' information contained in the registration statement pertains to details about the offering itself, the use of the proceeds, and any necessary updates on incorporated information.").

[14] 15 U.S.C. § 77k.

[15] 15 U.S.C. § 77l.

[16] 15 U.S.C. § 77k(b)(3). Non-expertised statements are those "not purporting to be made on the authority of an expert" and expertised statements are those "purporting to be made on the authority of an expert." *Id.*

[17] 15 U.S.C. §77l(a)(2); Seitz, *supra* note 14, at 1645.

decisions, whether in a shelf takedown or otherwise, is to endeavor to ensure that they can meet one or more of these due diligence defense standards should allegations of material misstatements and/or omissions arise after the offering. As explained above, shelf takedowns present challenges for underwriters in performing due diligence investigations and making reliance-based decisions. These challenges include: (i) the compressed amount of time available for the current due diligence, often spanning only a matter of days,[18] (ii) the extensive amount of information that may be incorporated by reference from documents that the underwriters may have played no role in drafting, and (iii) the fact that some of the incorporated information may be outdated or superseded by other, different disclosures.

Notwithstanding these challenges, both the SEC and the courts have made clear that the standard of reasonableness for purposes of an underwriter's statutory due diligence defenses is the same for both traditional offerings and shelf takedowns.[19] However, recognizing the due diligence and reliance challenges faced by underwriters in shelf takedowns, the SEC has acknowledged that underwriters may develop a "reservoir of knowledge" about companies, derived from their ongoing and prior due diligence activities.[20] For example, the SEC suggests the use of "periodic due diligence sessions," in which issuers hold meetings after the release of periodic reporting to provide prospective underwriters with an opportunity to discuss the information in the filings as well as business trends and financial developments.[21] The SEC also has commented upon the potential reliance-based decision making and due diligence benefits of issuers appointing a single

[18] *See* SEC Release 33-6335, *supra* note 5, at *5.

[19] "Reasonableness" as measured by the standard of conduct of a reasonable person in the management of his or her own property in a similar context. *See* In re Worldcom, Inc. Sec. Litig., 346 F. Supp. 2d 628, 670 (S.D.N.Y. 2004) (The SEC acknowledged that different investigatory methods would be needed "in view of the compressed preparation time and the volatile nature of the capital markets). SEC Release 33-6335, *supra* note 5, at *11. The SEC has expressed "mindfulness" of the due diligence challenges presented by these expedited offerings and have acknowledged that they may have to rely on pre-existing "reservoir of knowledge." *See* Robert J. Haft & Michele H. Hudson, Due Diligence – Periodic reports and Securities Offerings (West, 2009-200) at § 2.9 ("The nature of the due diligence investigation will vary considerably from one issue to another because of . . . the underwriter's involvement over time . . . . [T]he most effect due diligence is continuing investment banking relationship.").

[20] Joseph K. Leahy, *What Due Diligence Dilemma? Re-Envisioning Underwriters' Continuous Due Diligence After Worldcom*, 30 CARDOZO L. REV. 2001, 2021 (2009).

[21] Committee on Federal Regulation of Securities, *Report of Task Force on Sellers' Due Diligence and Similar Defenses Under the Federal Securities Laws*, 48 BUS. LAW. 1185, 1219 n.153 (1992-1993); Seitz, *supra* note 14, at 1651.

law firm as underwriter's counsel for a number of offerings.[22] Using this "designated counsel" practice allows the underwriters' counsel to develop its own reservoir of knowledge,[23] thereby facilitating due diligence and reliance-based decisions on expertised and non-expertised material (such as management statements) in a shelf takedown.

Thus, because of the expedited timeframe, underwriters have a limited—sometimes severely limited—timeframe in which to conduct current due diligence[24] and must rely to a greater degree on both cumulative due diligence conducted over an extended timeframe prior to the offering and on expertised and non-expertised material.[25]

OUTDATED INFORMATION INCORPORATED BY REFERENCE

SEC Rule 412

Each time an issuer makes an offering, any material changes to the registration information, whether it is contained in the shelf registration statement or incorporated by reference from Exchange Act reports, must be updated.[26] In 1981, the SEC proposed what became known as Rule 412 as part of its "comprehensive program to integrate the disclosure requirements of the Securities Act and the [Exchange Act]."[27] SEC Rule 412 addresses the issue of outdated information in a document that is incorporated by reference.[28] The main provisions of Rule 412 in this regard state the following:

---

[22] Committee on Federal Regulation of Securities, *supra* note 22, at 1220.

[23] *Id*.

[24] SEC Release 33-6335, *supra* note 5, at *5.

[25] Lawrence, *supra* note 10, at 127.

[26] Seitz *supra* note 14 at 1638.

[27] SEC Release 33-6335, *supra* note 5, at *1, *8; *see also* Reproposal of Comprehensive Revision to System for Registration of Securities Offerings, SEC Release 33-6331 (1981). Numbered Rule 418 at the time, it was subsequently renumbered when a different proposed Rule 412 was not adopted. Richard D. Bernstein & Zheyao Li, *The Review of Securities & Commodities Regulation*, WILLKIE (Feb. 6, 2013), http://www.willkie.com/~/media/Files/Publications/2013/02/SEC%20Rule%20412%20What%20Is%20Said%20Now%20Trumps%20What%20Was%20Sa__/Files/SECRule412WhatIsSaidNowTrumpsWhatWasSaidBeforepdf/FileAttachment/SEC_Rule_412_What_Is_Said_Now_Trumps_What_Was_Sa__.pdf.

[28] *See* 17 C.F.R. 230.412.

(a) Any statement contained in a document incorporated by reference shall be deemed to be modified or superseded to the extent that a statement in the prospectus modifies or replaces such statement,

(b) The modifying or superseding statement need not state that it has modified or superseded a prior statement, and

(c) Any statement so modified or superseded shall not be deemed to constitute a part of the registration statement or prospectus.[29]

Rule 412 effectively removes statements made in documents incorporated by reference from the application of the Securities Act when those statements have been superseded or modified by further disclosures.[30] The SEC further stated that the modifying or superseding statement is not deemed an admission that the modified or superseded statement was a violation of the federal securities laws when made.[31] Thus, Rule 412 was implemented to continue to encourage timely and meaningful disclosure by issuers.[32]

Case Law

Surprisingly, the implications of Rule 412 for underwriter due diligence and reliance-based decisions in the context of a shelf takedown have rarely been addressed by courts. However, in one federal district court case, the Rule formed the basis of the court's dismissal of Securities Act claims against General Electric (GE) and their underwriters.[33] Following is a brief review of that case.

In 2009, the State Universities Retirement System of Illinois brought a putative class action against GE and the underwriters of a 2008 public offering of $12 billion of GE common stock, asserting that the offering documents contained false and misleading statements regarding GE's ability to sell its commercial paper.[34] The offering was conducted pursuant to a shelf registration filed in

[29] *Id.*

[30] Bernstein & Li, *supra* note 28.

[31] *Id.*

[32] *Id.*

[33] *In re Gen. Elec. Co. Sec. Litig.*, 856 F. Supp. 2d 645 (S.D.N.Y. 2012); *See* Bernstein & Li, *supra* note 28.

[34] *In re Gen. Elec. Co. Sec. Litig.*, 856 F. Supp. 2d at 648-50.

2005, a preliminary prospectus filed in 2008, and a prospectus supplement filed in 2008.[35] Specifically, the plaintiff relied on statements in GE's four prior Form 10-K filings from 2004–2007, which were incorporated by reference into the offering documents.[36] Those prior filings characterized the commercial paper markets as "a reliable source of short-term financing" and called impaired access to those markets "unlikely."[37] However, the October 2008 prospectus supplement described: (i) "current levels of market disruption and volatility," (ii) the prospect of "further deterioration in the commercial paper and other credit markets," and (iii) how "there can be no assurance that such markets will continue to be a reliable source of short-term financing for GE Capital."[38]

In response to the allegations, the defendants argued that the 2008 prospectus supplement modified and superseded the earlier Form 10-Ks from 2004–2007 by replacing the statements with the new statements.[39] The court agreed. District Judge Denise Cote held that the complaint "improperly relied on . . . statements that were modified and superseded by later statements."[40] The court explained that "when the substance of a statement in the prospectus 'modifies or replaces' a prior statement in an incorporated filing, the prior statement 'shall not be deemed to constitute part of the registration statement,' regardless of whether the prospectus expressly states that it has modified or superseded that prior statement."[41]

PRACTICAL GUIDANCE FOR UNDERWRITERS REGARDING OUTDATED INFORMATION INCORPORATED BY REFERENCE

While both Rule 412 and the GE case are important benchmarks regarding outdated or superseded information in shelf takedown offering documents, neither offers much practical guidance to underwriters regarding their due diligence and reliance-based conduct in such contexts. However, by considering the upshot of each (i.e., that "when the substance of a statement in the prospectus

[35] *Id.*

[36] *Id.* at 655.

[37] Bernstein & Li, *supra* note 28.

[38] *Id.*

[39] *Id.*

[40] *Id.*; *In re Gen. Elec. Co. Sec. Litig.*, 856 F. Supp. 2d at 655.

[41] *In re Gen. Elec. Co. Sec. Litig.*, 856 F. Supp. 2d at 655.

'modifies or replaces' a prior statement in an incorporated filing, the prior statement 'shall not be deemed to constitute part of the registration statement…'"[42]) and the more general attributes of underwriter diligence in the context, one may reach a few conclusions regarding the matter.

First, underwriters of a shelf takedown involving incorporation by reference should make themselves familiar with the incorporated documents to relieve some of the reliance-based decision making. This does not mean that they must take ownership of them or assume responsibility for information they did not participate in preparing, but rather that the information, generally stated, should be part of the underwriters continuous and/or current due diligence and reliance-based process. Second, regarding incorporated information, the underwriters should be mindful of the risk that some information incorporated by reference may have changed over time. In this regard, an underwriter's consideration may benefit from distinguishing quantitative disclosures (such as earnings and accounting information that often change over time) and qualitative disclosures (such as market conditions, regulatory risk, and similar matters that may or may not change over time).[43] Third, if the underwriters identify any instances where information incorporated by reference has become outdated or superseded, they will need to endeavor to include the new information in the prospectus supplement (working with underwriters' counsel, the issuer, and perhaps others).

Regarding this third point, Judge Cote's ruling in *In re General Electric Company Securities Litigation* was significant in that it emphasized that the prospectus does not have to expressly state that it is superseding or modifying a particular outdated earlier statement in an incorporated document.[44] In that case, the older information was unmistakably superseded by the newer statements in the prospectus and it was clear that the new statements were drastically different from the earlier statements.[45] Thus, the burden is placed on the investor to understand whether the updated or new information is modifying or superseding the prior incorporated information and if so, how and what part of the prior information is being modified. Nonetheless, underwriters should

[42] *Id.* at 655-56.

[43] Seitz, *supra* note 14, at 1649; MARC I. STEINBERG, SECURITIES REGULATION: LIABILITIES AND REMEDIES §5.04[4] (2002).

[44] Bernstein & Li, *supra* note 28.

[45] *See In re Gen. Elec. Co. Sec. Litig.*, 856 F. Supp. 2d at 655-56.

endeavor to satisfy themselves that a reasonable investor would understand that the superseding information is in fact updating or correcting older information.[46]

CONCLUSION

While shelf registrations and incorporation by reference facilitates an issuer's ability to access public capital markets quickly, they present several due diligence challenges for underwriters, including the potential for outdated or superseded information in the incorporated documents. While neither Rule 412 nor *In re General Electric Company Securities Litigation* offers much in the way of practical guidance, taken together they make clear that (1) a prospectus supplement does not have to expressly state that it is superseding or modifying a particular outdated earlier statement in an incorporated document[47] and (2) that the offeree bears the burden of understanding what part of the prior information is being modified. Thus, underwriters can improve the quality of their due diligence and better position themselves to assert one or more statutory due diligence defenses by being mindful of general SEC guidance regarding shelf takedown due diligence (such as creating a reservoir of knowledge about the issuer and familiarizing itself with information incorporated by reference), considering the risk of both quantitative and qualitative information that may have become outdated or superseded, and by endeavoring to satisfy themselves that a reasonable investor would understand that the superseding information is in fact updating or correcting older information.

[46] *See* Bernstein & Li, *supra* note 28.

[47] Bernstein & Li, *supra* note 28.

BEYOND BREACH: CONFRONTING CYBERSECURITY AND PRIVACY RISKS IN NEGOTIATED TRANSACTION DUE DILIGENCE

Robert C. Uhl*

INTRODUCTION

In the weeks following the Cambridge Analytica data scandal,[1] Facebook's stock price plunged, costing the company nearly $80 billion in market capitalization.[2] More importantly, the affair focused a societal microscope on cybersecurity and raised renewed concerns among users, investors and government regulators.[3] Although Facebook's market cap still exceeds $450 billion, and the social media giant is unlikely to be acquired any time soon (if ever),[4] data breaches present a serious risk to acquirers of large and small enterprises alike.[5]

The commercial exploitation of customer data remains "big business" for many companies both in and outside the technology sector, and information is increasingly a significant part of a target's

* J.D., SMU Dedman School of Law, 2018; B.B.A., Finance, University of Notre Dame, 2015.

[1] Cambridge Analytica, a voter profiling firm hired to micro-target political ads, improperly used data from 270,000 Facebook users. A separate "personality prediction" Facebook app was allowed to gain access to information not only on its customers but also on its customers' Facebook friends through lax Facebook data privacy policies and default privacy settings. He app then broke Facebook's privacy policies by passing the information it collected to Cambridge Analytica, which used the extremely detailed and individually unique data to create voter personality profiles and target users with political messages. Craig Timberg & Elizabeth Dwoskin, *A voter profiling firm hired by Trump likely grabbed data for tens of millions of Facebook users*, THE WASHINGTON POST (Mar. 17, 2018) https://www.washingtonpost.com/news/the-switch/wp/2018/03/17/a-voter-profiling-firm-hired-by-trump-likely-grabbed-data-for-tens-of-millions-of-facebook-users/?utm_term=.bc9e3f5dc5a0.

[2] Paul R. La Monica, *Facebook has lost $80 billion in market value since its data scandal*, CNN MONEY (Mar. 27, 2018), http://money.cnn.com/2018/03/27/news/companies/facebook-stock-zuckerberg/index.html.

[3] In a voluntary appearance before Congress, Facebook CEO Mark Zuckerberg was pressed to account for how third-party partners could collect data without users' knowledge, what Facebook knew about data harvesting happening on its platform and in violation of its privacy policies, and whether Facebook or any social media company can regulate itself, even by banning people from its site. Senators struggled to define a right to privacy, but threatened to enact privacy rules and other regulations. *Mark Zuckerberg Testimony: Senators Question Facebook's Commitment to Privacy***,** THE NEW YORK TIMES (Apr. 10, 2018),

[4] FB: Summary for Facebook, Inc., YAHOO! FINANCE (accessed Apr. 12, 2018)

https://finance.yahoo.com/quote/FB?ltr=1.

[5] Many deals fall apart entirely. Verizon recently knocked $350 million from its purchase price of Yahoo! assets as a result of known and anticipated losses due to significant data breaches at Yahoo! that came to light after the deal was signed but before it closed. *See* Scott Moritz, *Verizon, Yahoo Cut Merger Price by $350 Million After Hacks*, BLOOMBERG BNA (Feb. 21, 2017) https://biglawbusiness.com/verizon-yahoo-cut-merger-price-by-350-m-after-hacks.

assets and risk profile. As a result, acquirers are well-advised to enhance the scope, character, and quality of their due diligence in this increasingly pivotal and risk-fraught area.

This "white paper" examines common elements of an acquirer's due diligence into a target's cybersecurity and privacy risks and suggests both a framework and some practical steps to assist acquirers in conducting effective due diligence.

CYBERSECURITY AND PRIVACY DILIGENCE GENERALLY

To minimize their risk, acquirers should develop due diligence processes and practices to understand and evaluate a target's vulnerabilities to cyberattacks, the effectiveness of its cyber defenses, and the magnitude of potential damage from a breach.[6] These processes and practices should facilitate an acquirer's assessment of a target's high-value digital assets and the risks presented to them.[7]

Often, a transaction may appear to be "privacy and cybersecurity light," but even where the access to or exchange of personal data is merely incidental,[8] the default rule for acquirer due diligence should be to include privacy and data security matters on its master diligence checklist and to appropriately investigate any cyber implications relevant in the context. In effect, acquirers and the professionals that make up their diligence team should never assume a target is of no interest to cyber-thieves or unexposed to other forms of cyber risk[9] unless or until the matter is clearly demonstrated to be irrelevant.

As with all due diligence, there is no "one size fits all" approach to privacy and cybersecurity risk investigation. Technological and criminal innovation, a constantly evolving regulatory framework, and varying levels of cyber sophistication across companies means diligence requires a unique approach to each target and in each context. For example, companies in the business of collecting, marketing, and selling data, as well as companies under heavy compliance requirements (like the Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA),

---

[6] Roland Trope & Tom Smedinghoff, *The Importance of Cybersecurity Due Diligence in M&A Transactions*, AMERICAN BAR ASSOCIATION: BUSINESS LAW TODAY (Sept. 4, 2017), https://www.americanbar.org/groups/business_law/publications/blt/2017/09/04_trope.html.

[7] *Id.*

[8] *See* Brian Krebs, *Target Hackers Broke in Via HVAC Company*, KREBS ON SECURITY (Feb. 2014) https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company.

[9] *Id.*

Fair Credit Reporting Act (FCRA), Electronic Communications Privacy Act (ECPA), or Children's Online Privacy Protection Act (COPPA)) present obvious cybersecurity risks and merit robust investigation in most contexts.[10] In other sectors like retail, hospitality, and financial services, cyber risks may be less apparent, but liability can be exponential given the sectors' large customer bases.[11] Moreover, smaller enterprises hungry for sales may disproportionally assume liability for data breaches involving their products[12] compared to, for example, large, mature corporations with robust financial resources and a history of regulatory compliance.[13]

Regardless of the industry sector or development stage of the target, the fundamental goal of negotiated transaction privacy and cybersecurity due diligence is to avoid buying a target's existing but undiscovered data breach and to determine a target's data security problems, which may burden the acquirer with costs later—the classic "ticking time bomb" problem.[14] Additionally, identifying the scope and character of cyber risks early in the diligence process can assist an acquirer in setting appropriate economic and contractual terms.

SELECTED CONSIDERATIONS IN CONDUCTING EFFECTIVE CYBERSECURITY AND PRIVACY DUE DILIGENCE

Because contexts, investment objectives, and risk tolerances vary, each acquirer decides the scope and character of its due diligence investigation based on what it considers to be in its best interests. However, each acquirer is expected to investigate material information in a manner that is "reasonable in the context." Reasonableness is understood to be what a prudent person in the management of his or her own property would have done in a similar context, and materiality is understood to mean information that a reasonable investor in a similar context would be substantially likely to consider important in making an investment decision. So "reasonableness in

[10] *Id.*

[11] John B. Kennedy, *Cybersecurity and Privacy in Business Transactions: Managing Data Risk in Deals*, 106 Corporate Practice Portfolio Series (BLOOMBERG BNA), http://corplawrc.bna.com/clrc/5423/split_display.adp?fedfid=64648231&vname=cpsporrcbus&wsn=511070000&fn=64648231&split=0.

[12] Kim S. Nash & Ezequiel Minaya, *Due Diligence on Cybersecurity Becomes Bigger Factor in M&A,* WALL ST. J. (Mar. 5, 2018), https://www.wsj.com/articles/companies-sharpen-cyber-due-diligence-as-m-a-activity-revs-up-1520226061.

[13] Kennedy, *supra* note 11.

[14] *Id.*

the context" of cybersecurity and privacy due diligence demands an increasingly expertized, nuanced, and industry-specific process.[15]

Unlike underwriter due diligence in the context of a public offering of securities, no entities such as the Securities and Exchange Commission or the Financial Industry Regulatory Authority exist in the negotiated transaction space to offer mandatory or informative guidance regarding the amount or character of due diligence an acquirer should conduct (regarding cybersecurity or any other matters). However, informative sources have proposed some best practices for acquirers to consider when deciding whether and to what extent to investigate cyber-related issues.

In this regard, there are three overarching themes for an acquirer's due diligence of a target's cybersecurity and privacy: (i) internal policies and assets, (ii) attack risk and defense testing, and (iii) executive accountability and governance. Investigating each of these themes commonly requires a framework tailored to the context of the proposed transaction[16] that encompasses six specific areas of focus: (1) the target's high-value digital assets and the relative importance of these assets to the target's business; (2) the target's internal cybersecurity programs and policies to protect those assets and how appropriate they are for the business; (3) the target's cyber risk management, risk assessments, defense testing, and general preparedness to withstand a direct attack; (4) the target's regulatory compliance, legal obligations, and response capabilities to prior breaches; (5) the target's organizational accountability and governance of privacy and cybersecurity issues; and (6) the importance of involving subject matter experts.[17]

Inventory Core Digital Assets

Perhaps the most fundamental task in any diligence endeavor is to determine exactly what the acquirer is buying. Preparing a comprehensive inventory of data assets allows an acquirer to identify high-value assets, determine network protections, and uncover gaps in company practices. Therefore, in most transactions, an acquirer (or a member of its diligence team) should inventory all network hardware (including devices allowed to access the network like smart phones, tablets,

[15] *See* Gary Lawrence, Due Diligence in Business Transaction §2.01 (Law Review Press, Release 36, 2012); *Escott v. BarChris Construction Corp.*, 283 F. Supp. 643 (S.D.N.Y. 1968).

[16] Governance Services, *Cybersecurity and the M&A Due Diligence Process*, NYSE (2016), https://www.nyse.com/publicdocs/Cybersecurity_and_the_M_and_A_Due_Diligence_Process.pdf.

[17] *See* Trope, *supra* note 6; Kennedy, *supra* note 11.

and remote storage) and any software installed on networked devices or permitted to access the network.[18]

Outline and Evaluate Data Security Policies and Privacy Training

Second, a company's data management, data classification, and data retention policies can be strong indicators of its overall cyber health; indeed, the mere existence of such policies is a positive indication of an appropriate level of attention to cybersecurity and privacy concerns. Organizations with well-developed protection and classification schemes that associate different levels of security with different types of data often are better prepared to identify weaknesses, respond to attacks, and involve management in cybersecurity processes.[19] A comprehensive written information security policy (WISP) is commonly considered a best practice,[20] detailing a company's risk detection and mitigation technologies, firewalls, traffic monitoring software, spam filters, malware detection and removal strategies, and data-loss prevention software as part of its larger web of network defenses.[21] However, a WISP is of limited value if it is not robustly implemented. Therefore, the acquirer's diligence should confirm that policies are actually followed, enforced, and updated regularly.

In those instances where the target lacks a WISP, an acquirer will need to undertake additional investigative measures such as management interviews or questionnaires to explain the target's specific cybersecurity practices.[22] Among other things, this investigation should endeavor to locate any internal information security policies, acceptable use policies for data, systems, or devices, incident response policies, data retention and disposal policies, and human resources policies. Internal information security policies should describe the minimum security requirements of hardware, software, networks, digital and physical data centers, and portable electronic devices.[23] Acceptable use policies should include computer use, internet use, data facility use, and "bring your own device" (BYOD) use. Policies should also evaluate which applications (like e-mail,

[18] *Id.*

[19] Kennedy, *supra* note 11.

[20] Massachusetts requires one by statute. *See* Mass. Regs. Code tit. 201, §17.03.

[21] *Id.*

[22] Kennedy, *supra* note 11.

[23] *Id.*

cloud services, and social media) and which employees or contractors are covered.[24] Moreover, BYOD policies should explain the security risks of using mobile devices for business purposes and should outline permitted download practices, application use, procedures for lost or stolen devices, and conditions for remotely wiping data from covered devices.[25] Data retention and disposal policies should reveal how securely the company destroys personal information and potential liabilities or costs incurred in maintaining old data.[26] Finally, humans are often the weakest link in data protection—both from intentional acts and negligence.[27]Accordingly, careful examination of training programs for employees, independent contractors, temporary hires, and even customers can be helpful and may indicate how seriously the company takes cybersecurity.[28] Such programs should establish the "rules of the road" when handling data and should raise awareness of high-risk activities like phishing and deleting sensitive information. Similarly, measuring the target's oversight of its human risk factor may uncover other sources of potential liability or suggest topics for further investigation.

Best practices also commonly consider written procedures that specify how an organization will respond to and recover from a security breach beneficial.[29] Therefore, an acquirer should ensure that even a target with no history of privacy or cybersecurity issues at least has a plan for dealing with such situations. The lack of a prepared response strategy can be a red flag, and the lack of written policies generally should concern most acquirers. Still, written policies are no guarantee of safety—the diligence process should verify the soundness of policies for the particular business, not simply their existence.[30]

Test Cyber Defenses and Highlight Risky Practices

Security is a continuous and evolving process. Therefore, acquirers will typically want to undertake an ongoing assessment of the target's safety framework and familiarity with the latest

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *See* Verizon, *Data Breach Investigations Report* (2018), https://www.verizonenterprise.com/verizon-insights-lab/dbir.

[28] Kennedy, *supra* note 11.

[29] Some organizations incorporate incident response plans into the entity's WISP. *Id*.

[30] *Id.*

threats. Moreover, in many contexts a target should periodically and formally audit and test its digital and physical cyber defenses to evaluate their effectiveness. Such reviews may include both unannounced internal checks and hiring third party "white hat hacker" contractors to find holes in the system.[31] Overall, the acquirer's diligence process should be directed toward discovering what measures the company has in place to detect anomalies, improve its detection processes, encrypt data sets, and involve management, all of which can indicate the target's familiarity with its cybersecurity practices, its comfort in shielding critical information, and its ability to prevent future attacks. Here too, consulting experts can be a valuable resource in investigating technology systems and intricacies and can guide further diligence into the effectiveness of the company's defenses.

Unfortunately, internal controls are not a target's only source of liability. A single "bad actor" contractor with access to the target's information systems or sensitive data can create severe problems, regardless of the target's formal policies and procedures. Third party contractors and service providers pose a particularly significant supply chain risk to data. Thus, diligence requests will ordinarily extend to third party contracts, particularly for outsourced IT functions, software development, data storage, or other cloud-hosted services.[32] In this regard, potential red flags can include: (a) extensive outsourcing or subcontracting, especially involving sensitive data and without a standardized approach to vendor compliance with privacy and security standards; (b) heavy reliance on public cloud providers' contract forms when licensing sensitive data, as opposed to vetting third parties and demanding certain contract provisions; and (c) a lack of written policies setting minimum privacy and cybersecurity standards when contracting with third parties and explaining the company's stance on these issues.[33]

Review Breach History and Assess Company Response

Often, an acquirer's best source of knowledge is observing the target's response to a prior incident. For example, how the target defines the constituent elements of a security breach can reveal a range of basic information, including how many breaches the target has experienced, how it became aware of those breaches, what the impact of the breaches was, how the target adjusted

[31] *Id.*

[32] *Id.*

[33] *Id.*

following the breach, and whether any breach investigations are currently pending.[34] With a baseline is established, the acquirer may find it constructive to investigate each breach, understanding, among other things:

- What data might the attackers have gained—or still be gaining?
- Did intruders make copies of or modify data, or change permissions so that they could log in and appear authorized?
- Might the intruders be able to attack again without the company's knowledge?[35]

In this sense, appropriate diligence may include a search for evidence of an intruder "lying in wait," undetected by the company. Additionally, future threats may arise not simply from an attacker's access to the system, but from what the attacker forced the system to reveal about its protective capabilities. Macro system information or a "hidden open back door" may be more valuable than the data the system guards. Therefore, acquirer due diligence should seek to uncover these traps, probing whether each layer of defense is intact and whether those layers cover the breadth of the company's assets effectively.[36] Moreover, after a breach, the target may be obligated to make certain public disclosures.[37] Therefore, the diligence process is enhanced by surveying the company's legal compliance, internal and external investigations, litigation, and other incident reports—particularly with applicable privacy laws and regulations—since these can create continued liability exposure, costs, and obligations.[38]

Question Management's Knowledge Base and Accountability

Fifth, company-wide protection is only as effective as the leaders responsible for it. If senior management does not demonstrate an appropriate understanding of data security risks and protection systems, accountability for cybersecurity may be siloed within a few IT professionals.[39]

---

[34] *Id.*

[35] *See* Trope, *supra* note 6.

[36] *Id.*

[37] SEC Adopts Statement And Interpretive Guidance On Public Company Cybersecurity Disclosures, S.E.C. 18-22 (2018), https://www.sec.gov/news/press-release/2018-22.

[38] Kennedy, *supra* note 11.

[39] Diane Reynolds, *Cybersecurity Due Diligence: 6 Key Questions To Ask Your CIO Before An Acquisition*, CHIEF EXECUTIVE (Oct. 27, 2017), https://chiefexecutive.net/cybersecurity-due-diligence-6-key-questions-ask-cio-acquisition.

Such limited direct responsibility for privacy and security issues can constitute a red flag that a company is not conscious of data risks, or at least is not adequately focused on them, and may be vulnerable. In such instances, an acquirer may wish to request (a) an organizational chart detailing which offices or roles are assigned responsibility for privacy and cybersecurity concerns and (b) an explanation of the company's mechanisms to "translate policies into practices"—taking broad policy goals down from senior management and the board of directors to IT for implementation and reporting back up the chain to keep management and the board aware of current threats and defenses.[40]

Interviewing C-level officers can also be a valuable part of acquirer due diligence. These interviews commonly involve questions such as:

- Does the organization have a chief information security officer (CISO), chief information officer (CIO), or chief privacy officer (CPO)?
- Whose job description includes responsibility for the organization's information security systems?
- Who certifies the company's compliance with privacy policies, laws, regulations, and industry codes of conduct?
- Which cybersecurity functions are outsourced and who oversees and monitors those functions?
- Who has primary responsibility for making changes to IT systems and what kind of management or board oversight is necessary?[41]

Even a detailed questionnaire to management asking for layman explanations of the technicalities of their company's network can reveal management's knowledge base and direct awareness of the privacy and cyber issues they face.

Subject Matter Experts

Finally, given cybersecurity's inherent complexity, subject matter experts can play an important role in facilitating an effective acquirer investigation. For example, every information technology

[40] Kennedy, *supra* note 11.

[41] *Id.*

(IT) system is different, so it is unlikely that an acquirer's internal team will always be sufficiently familiar with the nuances of every system or have a sufficient base of knowledge and experience to conduct effective due diligence. Therefore, outside IT professionals can be a valuable resource, assisting acquirers in understanding and probing the risks present in a given context.[42] Among other things, they can enhance the quality and effectiveness of due diligence questionnaires, site visits, interviews with key personnel, and tests of security measures across the six areas of focus.[43]

CONCLUSION

While each acquirer decides the scope and character of its due diligence based on factors such as its industry knowledge, investment objectives, and risk tolerances, most acquirers should also consider privacy and cybersecurity in most contexts. The overall goal of this kind of buy-side investigation is to reveal and quantify risks. Industry guidance regarding best practices suggests that where such an investigation is deemed appropriate, it should consider, among other things: (1) the target's specific mix of data assets critical to its business (2) the target's tailoring of its data policies to its business; (3) the target's technical cyber defense capabilities; (4) the target's breach history; (5) the target's management's interest in cybersecurity; and (6) involving subject matter experts.[44]

Omitting cybersecurity assessments, conducting only a superficial evaluation, or limiting the scope of inquiry too narrowly can invite serious risks that could diminish the value of the proposed transaction and lead to litigation, bankruptcy, and malpractice liability for attorneys and other professionals.[45] For these reasons, buy-side privacy and cybersecurity diligence should often be as much a part of the entire diligence process as an investigation of the target company's financials, employment agreements, and material contracts.

[42] Nash, *supra* note 12.

[43] *Id.*

[44] *See* Trope, *supra* note 6; Kennedy, *supra* note 11.

[45] Trope, *supra* note 6.

SELECTED CHARACTERISTICS OF RECENT SECTION 11 CASES INVOLVING INITIAL PUBLIC OFFERINGS

By G.M. Lawrence©

INTRODUCTION

In the United States, a public offering of securities, such as an initial public offering (IPO), must be registered with the Securities and Exchange Commission (SEC). Such securities are then issued pursuant to a registration statement and prospectus (collectively, offering documents) filed in accordance with the Securities Act. Under Section 11 of the Securities Act of 1933 (the Securities Act)[1], any person who purchases such a security on the basis of offering documents that contain a material misstatement or omission has a private cause of action.[2] Although the determination of materiality depends on both the context in which a statement or omission was made and the connection between the issuer's actual statement and other factors, courts generally consider something material if a reasonable investor, considering the "total mix" of information, would deem it important to his investment decision.[3]

In an IPO context, plaintiffs often are a class of individuals and/or institutions who purchased securities in the IPO. Defendants typically include one or more of the issuer and its directors and officers; signatories of the registration statement; underwriters; accountants and other experts. Unlike claims brought under the anti-fraud provisions of the Securities Exchange Act of 1934, Securities Act claims do not require plaintiffs to prove scienter (*i.e.*, culpable state of mind), but merely the presence of a material misstatement or omission.

Issuers are strictly liable for material misstatements and omissions, but other potential defendants, including underwriters and directors, have two affirmative due diligence defenses under Section 11. The first is the "reasonable investigation" defense which applies to non-expertized material. The second is the "reasonable reliance" defense which applies to expertized material. In both instances, "reasonableness" is defined as what a reasonable person in a similar context would have

[1] 15 U.S.C. § 77k and 15 U.S.C. § 77l.

[2] 15 U.S.C. § 77k.

[3] *See, e.g.*, Basic, Inc. v. Levinson, 485 U.S. 224, 231–32, 108 S. Ct. 978, 983, 99 L.Ed.2d 194 (1988).

done in the management of his or her own property.[4] The standard is applied using a "sliding scale" wherein the bar for establishing reasonableness is higher for insiders, such as officers and inside directors, than for outsiders such as underwriters and outside directors.[5] Thus, what constitutes a reasonable investigation or reasonable reliance in one context may or may not be sufficient in another context. This means that there is no "one-size-fits-all" approach to a reasonable investigations or reasonable reliance, nor is there safe harbor list of specific steps or practices that investigators can follow in every setting or circumstance to achieve "reasonableness."

This white paper focuses on recent industry, defendant and allegation trends in class action lawsuits involving IPOs brought under Section 11 and is based on aggregate information from a range of published databases over the three-year period between 2014 and 2016. These suits typically allege material misstatements or omissions in the offering documents relating to historical or projected financial information, inadequate risk disclosure and/or fraud. Defendants usually include the issuers, directors, underwriters and accountants, among others.

THE HISTORY BEHIND THE TRENDS

Before examining the recent trendline data regarding Section 11 class action lawsuits, it is helpful to have some perspective regarding the history of the Section 11 due diligence defenses.

For nearly 35 years after passage of the Securities Act, no court substantively addressed the due diligence defenses or the kinds of conduct required to assert them successfully. However, in 1968, Judge McLean of the Federal District Court for the Southern District of New York issued what *The Wall Street Journal* called a "Legal Blockbuster,"[6] *Escott v. BarChris Construction*, the first fulsome judicial examination of these matters.[7]

---

[4] 15 U.S.C. § 77k.

[5] *See, e.g.*, Federal Housing Finance Agency v. Nomura Holding America, Inc., No. 11cv6201 (S.D. N.Y., Dec. 18, 2014) ("As these factors suggest, there is a 'sliding scale' in the diligence required of parties, with heavier demands of those with more central roles and greater access to the information and expertise needed to confirm the accuracy of the registration statement."); WorldCom, 346 F. Supp. 2d at 675 ("Feit [referring to Feit v. Leasco Data Processing Equip. Corp., 332 F. Supp. 544 (E.D.N.Y. 1971)] insists that '[w]hat constitutes reasonable investigation and a reasonable ground to believe will vary with the degree of involvement of the individual, his expertise, and his access to the pertinent information and data.").

[6] The Wall Street Journal, May 14, 1968, at 1, col. 6.

[7] Escott v. BarChris Constr. Corp., 283 F. Supp. 643, 697 (S.D.N.Y. 1968).

In a lengthy and sometimes nuanced opinion, the Court ruled that the offering documents contained material misstatements and omissions, and that the due diligence conducted by the underwriters, directors, officers and accountants did not meet the statutory standard of "reasonableness." Thus, *BarChris* marked the beginning of an era of increasing judicial scrutiny of the affirmative due diligence defenses under the Securities Act.

In the nearly 60 years since the *BarChris* ruling, courts have issued a modest but steady stream of decisions addressing the due diligence defenses. Notable among these is Judge Cotes' denial of the underwriters' motion for summary judgment *In re WorldCom Securities Litigation*."[8] In that case, the court held that audited financial statements (a form of expertised material that, for many decades, courts had confirmed did not require a "reasonable investigation" but rather only "reasonable reliance") may contain "red flags" that require investigation. Understandably, the ruling sent shockwaves through the industry, in part because it rejected Justice Powell's dissenting opinion in *John Nuveen & Co. v. Sanders* that "almost by definition, it is reasonable to rely on financial statements certified by public accountants."[9] And, more recently, Judge Cote ruled in *FHFA v. Nomura*[10] that the underwriter's due diligence was not reasonable as a matter of law, the first ever ruling of its kind.

The collective impact of these kinds of rulings has been a marked increase in due diligence-based securities litigation. For example, according to a recent study conducted by Stanford Law School Securities Class Action Clearinghouse and Cornerstone Research, 226 new federal class action securities cases were filed in the first six months of 2017, a number that was "135 percent above the 1997–2016 historical semiannual average of 96 filings and the highest filing rate since the

[8] In re WorldCom, Inc. Sec. Litig., 346 F. Supp. 2d 628 (S.D.N.Y. 2004)

[9] Sanders v. John Nuveen & Co., 619 F.2d 1222, 1228 (7th Cir.1980), cert. denied, 450 U.S. 1005, 101 S. Ct. 1719, 68 L.Ed.2d 210 (1981). Justice Powell further observed that reliance on certified financial statements "is essential to the proper functioning of securities marketing, to the trading in securities, to the lending of money by banks and financial institutions, and to the reliance by stockholders on the reports of their corporations." Id., 450 U.S. 1005 at 1010, note 4. He also stated that "where breaches by accountants occur, it is the accountants themselves—not those who rely in good faith on their professional expertise—who are at fault and who should be held responsible." Id. Note that he used the term "certified" not "audited" thus leaving open the issue of whether his comments should apply both to audited information and unaudited information which is the subject of an auditor's comfort letter.

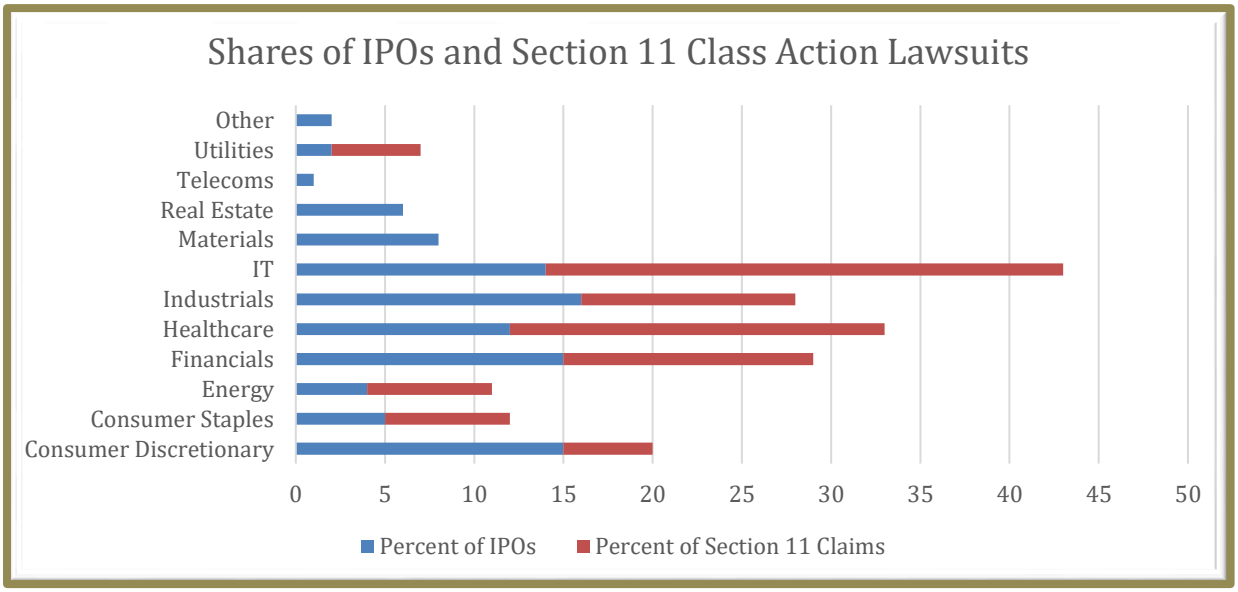
[10] Federal Housing Finance Agency vs. Nomura Holding America, Inc., 68 F.Supp.3d 439 (S.D.N.Y. 2014). At the time of publication of this white paper, the ruling is before the Second Circuit on appeal.

Securities Clearinghouse began tracking these data."[11] By understanding the characteristics of recent Section 11 class action lawsuits, defendants may be better positioned to make decisions about the nature and character of their due diligence and reliance in pending and future securities offerings.

RECENT TRENDS

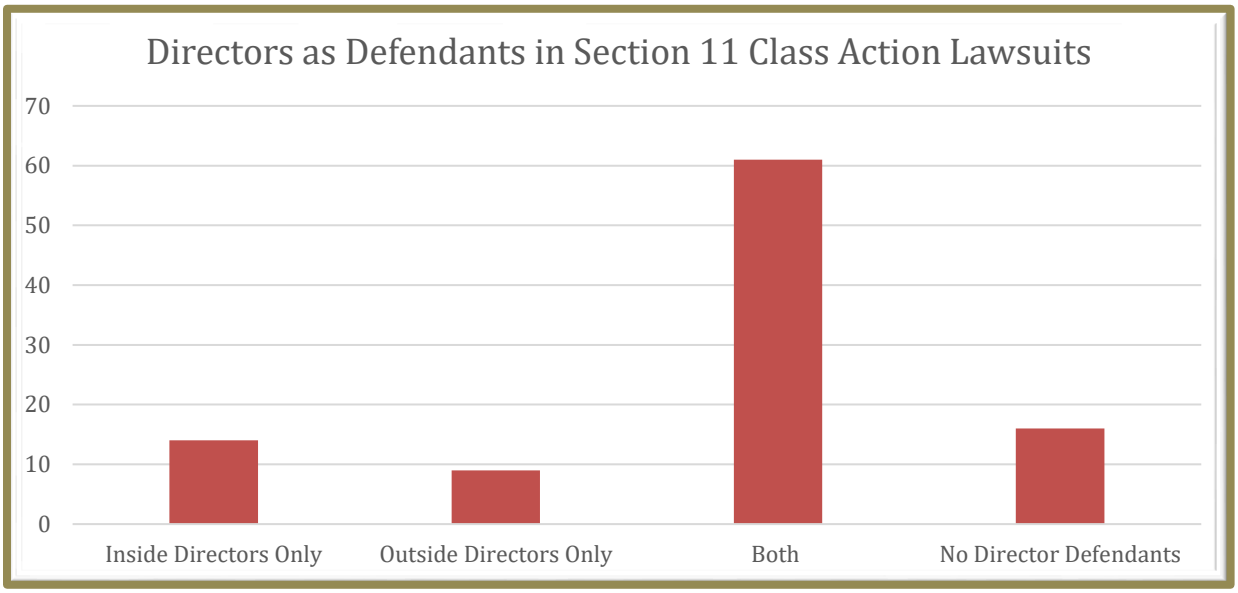
To better understand the current class action securities litigation landscape for IPOs and the role of the due diligence defenses in those cases, it is instructive to examine various characteristics of the industries, defendants and allegations involved. Following are several charts reflecting aggregate information from a range of public and private databases.

The first chart compares the number of IPOs across different industries with the number of suits involving Section 11 allegations related to IPOs over the three-year period between 2014 and 2016. As is evident from this chart, the share of IPOs and suits with Section 11 allegations are approximately equal for most industries. However, information technology, for example, has a share of Section 11 lawsuits approximately twice that of its IPOs. And, consumer discretionary has a share of Section 11 lawsuits that is approximately one-third of its share of IPOs. Thus, different industry sectors have different levels of risk regarding such claims.



[11] https://corpgov.law.harvard.edu/2017/08/07/federal-class-action-securities-fraud-filings-hit-record-pace-in-h1-2017/.

Moreover, different potential defendants have different risk exposure to class action securities lawsuits. Most important among these are directors and underwriters, each of which is named in a high percentage of such lawsuits. For example, directors were named in approximately 85% of the sample, as shown by the following chart.

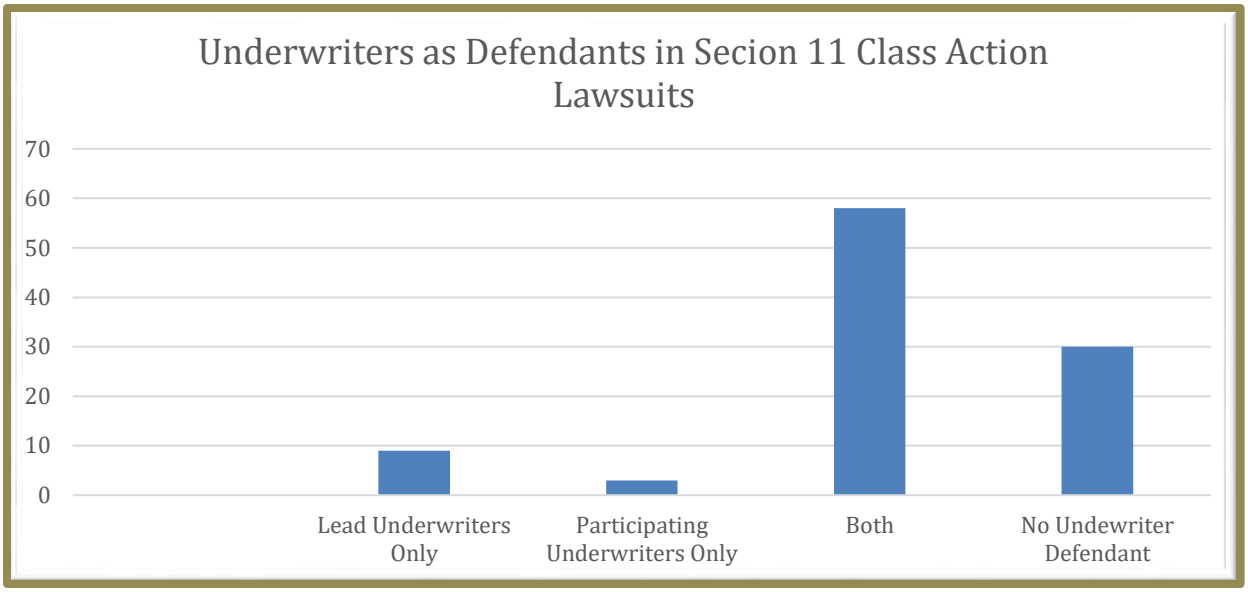


The preponderance of these cases named both inside and outside directors as defendants.[12]

Over 70% of the sampled Section 11 class action lawsuits named lead and/or participating underwriters as defendants.[13] The following chart shows the share of suits that include allegations against underwriters by role.

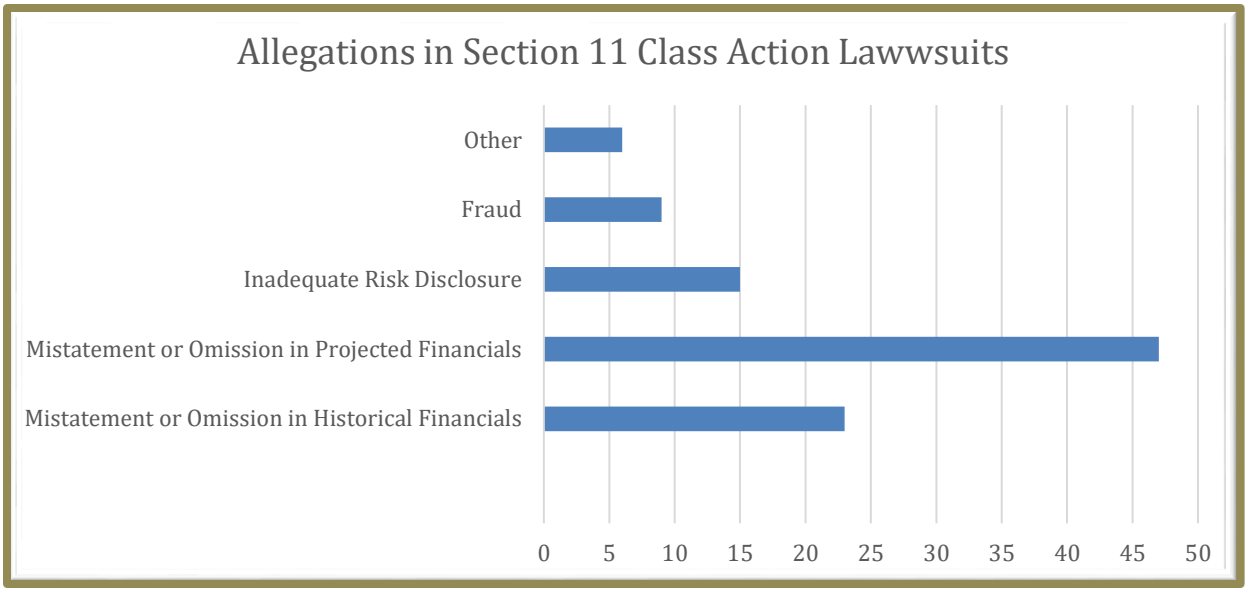
[12] There is no statutory definition of what constitutes an inside or outside director. Categorization of the directors as inside or outside here is based on descriptions in the reviewed complaints.

[13] Categorization of the underwriters as lead or participating is based on descriptions in the reviewed complaints and prospectuses.



Thus, over half of the cases sampled named both lead and participating underwriters, while lead underwriters alone were only named in 9% of cases. Participating underwriters only were named in just 3% of cases.

Finally, it is also instructive to consider the specific types of allegations made in Section 11 cases, as different allegations can have different implications for the nature and scope of due diligence that courts may require of directors, underwriters, and others. As the chart below shows, nearly half of the sampled Section 11 cases involved allegations of a misstatement or omission regarding *projected* financial information, with the remainder including alleged misstatements of *historical* financial information, failure to disclose risks, and failure to disclose existence of fraud. This distribution, however, varied among industries. For example, the largest proportion of Financial Industry claims in these cases involved alleged fraud (43%) whereas for Information Technology and Healthcare the largest proportion (69% and 56%, respectively) involved alleged projected financial performance misstatements and/or omissions.



CONCLUSION

As shown in the recent Stanford/Cornerstone analysis cited above, the number of class action securities litigation claims under Section 11 continues to grow. Moreover, directors and underwriters are frequently named among the defendants in those cases. By understanding the characteristics of recent Section 11 class action lawsuits, defendants may be better positioned to make decisions about the nature and character of their due diligence and reliance in pending and future securities offerings.

ABOUT THE AUTHOR

G. M. Lawrence is a prominent transactional and due diligence scholar whose academic work has been cited authoritatively in numerous publications, by the Federal District Court for the Southern District of New York and in pleadings before the Supreme Court of the United States. He also has advised the U.S. Securities and Exchange Commission and has served as a consulting expert in a number of high profile cases.

Professor Lawrence is a member of the adjunct faculty of the Dedman School of Law of Southern Methodist University where he teaches due diligence studies to MBA, JD and LLM candidates, the founder and executive director of the independent Center for Advanced Due Diligence Studies. He also is executive chairman of the investment firm, Pacific Financial Group.

He is the author of the two-volume treatise *Due Diligence in Business Transactions*, a leading work in the field for more than 20 years, and the graduate textbooks *Due Diligence, Reliance and Verification: Law, Standards and Practice*; *Due Diligence: Law, Standards and Practice* and *Due Diligence, a Scholarly Study*. He is co-author of the treatise *Representing High Tech Companies*. Recently, he served as Visiting Due Diligence Scholar in Residence at the University of London.

Professor Lawrence holds a FINRA Series 65 license, a professional certification in Strategic Decision and Risk Management from Stanford University's Center for Professional Development and a J.D. degree from Vanderbilt Law School.

He is a current or former member of or active in, among others, the Securities Industry and Financial Markets Association Compliance and Legal Society, Investment Management Consultants Association, the National Association of Retirement Plan Advisors, the National Association of Corporate Directors, the Society of Decision Professionals, the Global Association of Risk Professionals, the Society for Judgment and Decision Making, the Academy of Financial Services and the American Securitization Forum, and has been admitted to the state bars of New York, the District of Columbia and Texas.

Previously, Professor Lawrence was a managing partner with a global law firm where he founded and taught the firm's due diligence training program, managed the firm's investment fund and chaired the technology, media and telecommunications practice. He was a member of the firm's management, strategic planning, partner compensation and other committees. Professor Lawrence also has served on the board of directors and various committees of public and privately held companies.