

The **LEXIS PRACTICE ADVISOR** Journal™

Practical guidance backed by leading attorneys from Lexis Practice Advisor®

DRAFTING OFFICE RELATIONSHIP CONTRACTS PROTECTING EMPLOYERS

**Avoiding Disastrous
Force Majeure Clauses**

**Insurance Coverage Issues
Created by the Internet**





LexisNexis®

Lexis Advance®

THE FUTURE IS NOW

From predictive analytics to data visualization, the Lexis Advance® service brings the future forward with innovative features and tools that empower today's data-driven legal professionals.

Get started today at

[LEXISNEXIS.COM/FUTUREISNOW](https://www.lexisnexis.com/futureisnow)

OR CALL 800.628.3612

2.5

PETABYTES
OF LEGAL CONTENT

30+

YEARS
OF METADATA



EXCLUSIVE
PREDICTIVE ANALYTICS



PATENTED DATA
VISUALIZATION

PRACTICE NEWS

- 4** CURRENT UPDATES AND LEGAL DEVELOPMENTS
Intellectual Property, Finance, Labor & Employment

PRACTICE POINTERS

- 10** DRAFTING ADVICE: AVOIDING DISASTROUS FORCE MAJEURE CLAUSES
Commercial Transactions

- 16** TOP 10 PRACTICE TIPS: REIT IPOs
Capital Markets & Corporate Governance

GC ADVISORY

- 20** DRAFTING OFFICE RELATIONSHIP CONTRACTS PROTECTING EMPLOYERS
Labor & Employment

- 24** OFFICE RELATIONSHIP CONTRACT
Labor & Employment

- 27** CYBER RISKS IN THE WORKPLACE: GUIDANCE FOR EMPLOYERS ON MANAGING INSIDER THREATS
IP & Technology

PRACTICE PROJECTIONS

- 31** TAX CUTS AND JOBS ACT: INSIGHTS FOR CORPORATIONS AND BUSINESS RELATED TO THE NEW TAX LAW
Tax

PRACTICE TRENDS

- 39** BIOMETRIC INFORMATION PROTECTION: THE STAGE IS SET FOR EXPANSION OF CLAIMS
IP & Technology

- 43** PREPARING FOR RANDOM TRADEMARK REGISTRATION AUDITS
IP & Technology

PRACTICE NOTES

- 46** INSURANCE COVERAGE ISSUES CREATED BY THE INTERNET
Commercial Transactions

IN-HOUSE INSIGHTS

- 59** START-UP SEED FINANCING
Capital Markets & Corporate Governance

MARKET TRENDS

- 66** MARKET TRENDS: SHAREHOLDER PROPOSALS
Capital Markets & Corporate Governance

- 75** MARKET TRENDS: MIDDLE MARKET LOANS
Finance



EDITOR-IN-CHIEF	
Eric Bourget	
VP, LEXIS PRACTICE ADVISOR AND ANALYTICAL	Rachel Travers
VP, ANALYTICAL LAW & LEGAL NEWS	Aileen Stirling
MANAGING EDITOR	Lori Sieron
DESIGNER	Jennifer Shadbolt
MARKETING	Sarah Patrick Karen Victoriano Jake Miller
CONTRIBUTING EDITORS	
Finance, Financial Restructuring & Bankruptcy	Robyn Schneider
Banking Law	Matthew Burke
Capital Markets	Burcin Eren
Commercial Transactions	Anna Haliotis
Corporate Counsel	Carrie Wright
Employee Benefits & Executive Compensation	Bradley Benedict
Intellectual Property & Technology	Jessica McKinney
Labor & Employment	Elias Kahn
Mergers & Acquisitions	Dana Hamada
Oil & Gas, Jurisdictional	Cameron Kinvig
Real Estate	Lesley Vars
Tax	Jessica Kerner
ASSOCIATE EDITORS	Maureen McGuire Mary McMahon Shannon Weiner Ted Zwyer
PRINTED BY	Cenveo Publisher Services 3575 Hempland Road Lancaster, PA 17601



The Lexis Practice Advisor Journal (Pub No. 02380; ISBN: 978-1-63284-895-6) is a complimentary publication published quarterly for Lexis Practice Advisor® subscribers by LexisNexis, 230 Park Avenue, 7th Floor, New York, NY 10169. Email: lexispracticeadvisorjournal@lexisnexis.com | Website: www.lexisnexis.com/lexispracticeadvisorjournal

This publication may not be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine readable form, in whole or in part, without prior written consent of LexisNexis. Reproduction in any form by anyone of the material contained herein without the permission of LexisNexis is prohibited. Permission requests should be sent to: permissions@lexisnexis.com.

All information provided in this document is general in nature and is provided for educational purposes only. It may not reflect all recent legal developments and may not apply to the specific facts and circumstances of individual cases. It should not be construed as legal advice. For legal advice applicable to the facts of your particular situation, you should obtain the services of a qualified attorney licensed to practice in your state.

The publisher, its editors and contributors accept no responsibility or liability for any claims, losses or damages that might result from use of information contained in this publication. The views expressed in this publication by any contributor are not necessarily those of the publisher.

Send address changes to: The Lexis Practice Advisor Journal, 230 Park Avenue, 7th Floor, New York, NY 10169. Periodical Postage Paid at New York, New York, and additional mailing offices.

LexisNexis, the Knowledge Burst logo and Lexis Practice Advisor are registered trademarks and Lexis Practice Advisor Journal is a trademark of Reed Elsevier Properties Inc., used under license. Other products and services may be trademarks or registered trademarks of their respective companies.

Copyright 2018 LexisNexis. All rights reserved. No copyright is claimed as to any part of the original work prepared by a government officer or employee as part of that person's official duties.

Cover photo courtesy HelgaBragina / Shutterstock.com. Additional images used under license from Shutterstock.com.

EDITORIAL ADVISORY BOARD

Distinguished Editorial Advisory Board Members for The Lexis Practice Advisor Journal are seasoned practitioners with extensive background in the legal practice areas included in Lexis Practice Advisor®. Many are attorney authors who regularly provide their expertise to Lexis Practice Advisor online and have agreed to offer insight and guidance for The Lexis Practice Advisor Journal. Their collective knowledge comes together to keep you informed of current legal developments and ahead of the game when facing emerging issues impacting your practice.

Andrew Bettwy, Partner
Proskauer Rose LLP
Finance, Corporate

Julie M. Capell, Partner
Davis Wright Tremaine LLP
Labor & Employment

Candice Choh, Partner
Gibson Dunn & Crutcher LLP
Corporate Transactions,
Mergers & Acquisitions

**S. H. Spencer Compton, VP,
Special Counsel**
First American Title Insurance Co.
Real Estate

Linda L. Curtis, Partner
Gibson, Dunn & Crutcher LLP
Global Finance

Tyler B. Dempsey, Partner
Troutman Sanders LLP
Mergers & Acquisitions,
Joint Ventures

James G. Gatto, Partner
Sheppard, Mullin, Richter &
Hampton LLP
Intellectual Property, Technology

Ira Herman, Partner
Blank Rome LLP
Insolvency and Commercial Litigation

Ethan Horwitz, Partner
Carlton Fields Jorden Burt
Intellectual Property

Glen Lim, Partner
Katten Muchin Rosenman LLP
Commercial Finance

Joseph M. Marger, Partner
Reed Smith LLP
Real Estate

Alexandra Margolis, Partner
Nixon Peabody LLP
Banking & Finance

Matthew Merkle, Partner
Kirkland & Ellis International LLP
Capital Markets

Timothy Murray, Partner
Murray, Hogue & Lannis
Business Transactions

Michael R. Overly, Partner
Foley & Lardner
Intellectual Property, Technology

Leah S. Robinson, Partner
Mayer Brown LLP
State and Local Tax

Scott L. Semer, Partner
Torys LLP
Tax, Mergers and Acquisitions

Claudia K. Simon, Partner
Schulte Roth & Zabel
Corporate, Mergers & Acquisitions

**Lawrence Weinstein,
Corporate Counsel**
The Children's Place Inc.

**Kristin C. Wigness, First V.P.
& Associate General Counsel**
Israel Discount Bank of New York
Lending, Debt Restructuring,
Insolvency

Patrick J. Yingling, Partner
King & Spalding
Global Finance



Eric Bourget, Editor-in-Chief

THE TAX CUTS AND JOBS ACT HAS LEFT many trying to interpret the far-reaching effects of its changes to the tax code and how it will impact their clients. For businesses, the Act provides a favorable reduction in the maximum corporate tax from 35% to 21%. Will the Act lead to the level of business investment and job growth that is anticipated? Are there other unintended consequences that could arise from the new tax law? We bring you insights and guidance for business in a summary of the Act's key provisions impacting taxpayers doing business in the United States.

It's proxy season again and time to look at trends related to shareholder proposals. This mechanism reached its peak in 2015 and has

declined slightly over the past two seasons, along with investor support for shareholder proposals. As proxy season 2018 heats up, our market trends report looks at this and other related trends.

How can employers guard against the related complications of workplace romances? Some employers may not have policies or contracts in place when presented with consensual relationships between co-workers. This edition of the Lexis Practice Advisor Journal not only provides guidance on drafting office relationship contracts, it also offers you a sample agreement designed to protect employers.

Our other drafting advice relates to force majeure clauses and discusses the ways that botched versions of these clauses can actually expose your client to greater unforeseen risks. The article reviews circumstances when a force majeure clause may not be necessary and also provides insights into creative ways to use the clause as a risk allocation device to excuse a client from certain foreseeable risks that the client would consider intolerable.

Concerns about protecting biometric information are escalating as we see the expanded use of fingerprints, facial recognition, and retina scans to activate mobile devices, grant security access, or for employee time tracking. Who is retaining this data, where is it being stored, and is it always collected with our knowledge? Lawsuits alleging improper collection and storage of biometric data are increasing against employers and tech companies. Illinois is on the forefront

of biometric data privacy laws and several other states are considering similar legislation.

Additional guidance in this edition includes a look at cybersecurity risks from company insiders, new insurance coverage considerations brought on by the internet, and a look at the unique issues facing Real Estate Investment Trust Initial Public Offerings that are not typical with other types of IPOs.

We hope the Lexis® Practice Advisor Journal continues to provide you with helpful and insightful guidance on how to complete various tasks that cross your desk. Utilizing the digital version of this journal should optimize your experience using our online product, Lexis® Practice Advisor, as the URLs provided at the end of each article transport you directly to the content as it appears within the product. If you are a Lexis® Practice Advisor subscriber who has only received a print version and would like a digital copy, please visit our website here, at <https://www.lexisnexis.com/lexis-practice-advisor/the-journal/b/lpa/default.aspx> and request the same.

Our mission

The Lexis Practice Advisor Journal™ is designed to help attorneys start on point. This supplement to our online practical guidance resource, Lexis Practice Advisor®, brings you a sophisticated collection of practice insights, trends, and forward-thinking articles. Grounded in the real-world experience of our 850+ seasoned attorney authors, the Lexis Practice Advisor Journal offers fresh, contemporary perspectives and compelling insights on matters impacting your practice.

U.S. DEPARTMENT OF LABOR SETS NEW GUIDELINES FOR INTERN COMPENSATION

THE U.S. DEPARTMENT OF LABOR (DOL) HAS ADOPTED new guidelines for determining whether interns working at for-profit companies are entitled to compensation under the federal Fair Labor Standards Act (FLSA).

The DOL abandoned its six-part analysis for deciding if an intern meets the requirements for employee status under the FLSA in favor of a seven-factor test that has been adopted by four federal appeals courts, most recently by the U.S. Court of Appeals for the Ninth Circuit on December 19. See *Benjamin v. B&H Educ., Inc.*, 877 F.3d 1139 (9th Cir. 2017).

In a statement, the DOL said that it “will conform to these appellate court rulings by using the same ‘primary beneficiary’ test that these courts use to determine whether interns are employees under the FLSA.” The Wage and Hour Division (WHD) of the DOL updated its fact sheet on the issue, “Internship Programs under the Fair Labor Standards Act,” to reflect the seven-part inquiry to be used going forward.

The WHD stated that under the new guidelines, the emphasis is on the “economic reality” of the relationship between the intern and employer, specifically the question of which party is the “primary beneficiary” of the relationship. The test is flexible, noted the WHD, and the determination of whether an intern is an employee “necessarily depends on the unique circumstances of the case.”

The seven factors are:

- The extent to which the intern and employer clearly understand that there is no expectation of compensation
- The extent to which the internship provides training similar to that provided in an educational environment
- The extent to which the internship is tied to the intern’s formal education program by coursework or academic credit
- The extent to which the internship accommodates the intern’s academic commitments
- The extent to which the internship is limited in duration to the period in which it provides the intern with beneficial learning
- The extent to which the intern’s work complements, rather than displaces, the work of paid employees
- The extent to which the intern and employer understand that the internship does not guarantee a paid job

The WHD said that in addition to aligning with case law, adoption of the new standards will “eliminate unnecessary confusion among the regulated community” and provide its investigators “with increased flexibility to holistically analyze internships on a case-by-case basis.”

- Lexis Practice Advisor Staff



RESEARCH PATH: [Labor & Employment > Employment Contracts > Employment Agreements > Articles](#)



CALIFORNIA STATUTE LIMITS PRE-EMPLOYMENT CRIMINAL BACKGROUND INQUIRIES

WITH THE ENACTMENT OF THE FAIR CHANCE ACT (Assembly Bill No. 1008),¹ California became the tenth state to prohibit both private and public employers from requiring an applicant to submit to a criminal background check before making a conditional offer of employment. The statute, also called the Ban-the-Box-Law, became effective on January 1.

Under the new provisions, covered employers—those with five or more employees—may not require an applicant “to include on any application for employment any question that seeks the disclosure of an applicant’s conviction history.” In addition, covered employers may not “inquire into or consider the conviction history of an applicant until that applicant has received a conditional offer.” Further, when conducting the background check, the employer may not “consider, distribute, or disseminate information about” arrests not followed by conviction, referral to or participation in a pre-trial or post-trial diversion program, or convictions that have been sealed, dismissed, or expunged.

The statute does not preclude an employer from conducting a criminal conviction background check. However, if an employer intends to reject an applicant on the basis of the applicant’s conviction history, the employer must make “an individualized assessment of whether the applicant’s conviction has a direct and adverse relationship with the specific duties of the job that justify denying the applicant the position.”

If an employer makes a preliminary decision to reject an applicant on the basis of the applicant’s conviction history, the employer must notify the applicant in writing and include notice of the conviction at issue, a copy of the conviction history report, and an explanation of the applicant’s right to respond to the notification. The applicant then has at least five business days to respond and five additional days after that to provide any information disputing the accuracy of the report.

Notice of a final rejection based on conviction history must also be provided to the applicant in writing, along with information on how to challenge the decision or to file a complaint with the California Department of Fair Employment and Housing.

Section 1 of the statute notes that “roughly seven million Californians, or nearly one in three adults, have an arrest or conviction record than can significantly undermine their efforts to obtain gainful employment.” Experts have found, the statute says, that “employment is essential to helping formerly incarcerated people support themselves and their families, that a job develops prosocial behavior, strengthens community ties, enhances self-esteem, and improves mental health, all of which reduce recidivism.”

- Lexis Practice Advisor Staff



RESEARCH PATH: [Labor & Employment > Screening and Hiring > Recruiting and Screening > Articles](#)

¹ Cal. Assem. Bill No. 1008, 2017-2018 Reg. Sess. (Oct. 14, 2017) (AB 1008).





FEDERAL RESERVE BOARD PROPOSES MEASURES TO INCREASE TRANSPARENCY OF STRESS TESTING

THE BOARD OF GOVERNORS OF THE FEDERAL RESERVE System is seeking comment on several proposals that it says will “increase the transparency of its stress testing program while maintaining the Federal Reserve’s ability to test the resiliency of the nation’s largest and most complex banks.”

Among the proposals is the release of greater information about the models the Board uses in estimating hypothetical losses in its testing, particularly in its annual Comprehensive Capital Analysis and Review (CCAR). Under the proposal, the Board would publicly release for the first time a range of loss rates, estimated using the Board’s model, for loans held by CCAR firms; portfolios of hypothetical loans with loss rates estimated by the Board’s models; and more detailed descriptions of the Board’s models.

The Board is also seeking public comment on a proposed Stress Testing Policy Statement, which it described as an outline of “the key principles and policies governing the Board’s approach to the

development, implementation, and validation of models used in the supervisory stress test.”

Finally, the Board is proposing amendments to its policy statement on the scenario design framework for stress testing. “The proposed amendments to the policy statement would clarify when the Board may adopt a change in the unemployment rate in the severely adverse scenario of less than 4 percentage points; institute a counter-cyclical guide for the change in the house price index in the severely adverse scenario; and provide notice that the Board plans to incorporate wholesale funding costs for banking organizations in the scenarios,” the Board said.

Public comments will be made available on the Board’s website at <http://www.federalreserve.gov/generalinfo/foia/ProposedRegs.aspx>.

- Lexis Practice Advisor Staff



RESEARCH PATH: [Finance > Financial Services Regulation](#)
> [Financial Institution Activities > Articles](#)

OVERALL RISKS TO FINANCIAL STABILITY REMAIN “MODERATE,” OFR SAYS

THE OFFICE OF FINANCIAL RESEARCH (OFR) SAYS THAT overall risks to financial stability are “moderate,” reflecting little change from last year.

The OFR, which was established in 2010 under the Dodd-Frank Act, issued its assessment in conjunction with the release of its 2017 Annual Report to Congress and its 2017 Financial Stability Report. The OFR is obligated to prepare and submit a report to Congress within 120 days of the end of each fiscal year. The Financial Stability Report serves as an adjunct to that report, providing more detailed analysis.

While concluding that the financial system is “far more resilient than it was when the financial crisis loomed a decade ago,” the two reports highlight three key threats to financial stability:

- Vulnerabilities to cybersecurity incidents
- Obstacles to resolving failing systemically important financial institutions
- Structural changes in markets and industry

The three key threats were selected “based on their potential impact, probability of occurring, probability of happening soon, and the preparedness of industry and government to manage them,” the OFR said.

The reports also introduce two new risk-assessment tools developed by the OFR: the Financial Systems Vulnerabilities Monitor and the Financial Stress Index, both of which are available on the OFR website, <https://www.financialresearch.gov/>, as part of the OFR’s quantitative monitoring toolkit. “They signal where potential vulnerabilities might require further investigation,” the OFR said. “We conduct those investigations using a wider set of data, qualitative information, and expert analysis.”

- Lexis Practice Advisor Staff



RESEARCH PATH: [Finance > Financial Services Regulation](#)
> [Financial Institution Activities > Articles](#)



PTAB RULINGS ON TIMELINESS OF REVIEW PETITIONS ARE APPEALABLE, FEDERAL CIRCUIT RULES

RULINGS BY THE PATENT TRIAL AND APPEAL BOARD

(PTAB) on the timeliness of petitions for inter partes review under the Leahy-Smith America Invents Act (AIA) are appealable, the U.S. Court of Appeals for the Federal Circuit has ruled.

In a 9-4 en banc decision, the Federal Circuit vacated a three-judge panel's September 2016 ruling upholding a PTAB decision invalidating a patent held by Wi-Fi One, LLC in a challenge brought by Broadcom Corp. *Wi-Fi One, LLC v. Broadcom Corp.*, 2018 U.S. App. LEXIS 387 (Fed. Cir. Jan. 8, 2018). The decision effectively overrules the Federal Circuit's ruling in *Achates Reference Publ. Inc. v. Apple Inc.*, Inc., which found that timeliness rulings under the AIA were not subject to appeal. 803 F.3d 652 (Fed. Cir. 2015).

The AIA, enacted in 2011, seeks to streamline patent infringement litigation by allowing a party sued for infringement to request a validity determination via inter partes review by the PTAB within a year after being served with the infringement complaint.

In 2010, Telefonaktiebolaget LM Ericsson (Ericsson) filed an infringement action against multiple defendants in the U.S. District Court for the Eastern District of Texas. A jury ruled for Ericsson and the Federal Circuit affirmed in part. *Ericsson Inc. v. D-Link Sys.*, 773 F.3d 1201 (Fed. Cir. 2014). In 2013, Broadcom filed three

separate petitions for inter partes review of the three Ericsson patents. During the pendency of the review, Ericsson transferred ownership of the patents to Wi-Fi, which argued that the petitions were time-barred because Broadcom was in privity with the defendants in the Texas action. The PTAB rejected Wi-Fi's argument and found its patents invalid.

On appeal, a three-judge panel of the Federal Circuit affirmed on the basis of the *Achates* decision. Wi-Fi petitioned for en banc review. The petition was granted in January 2017.

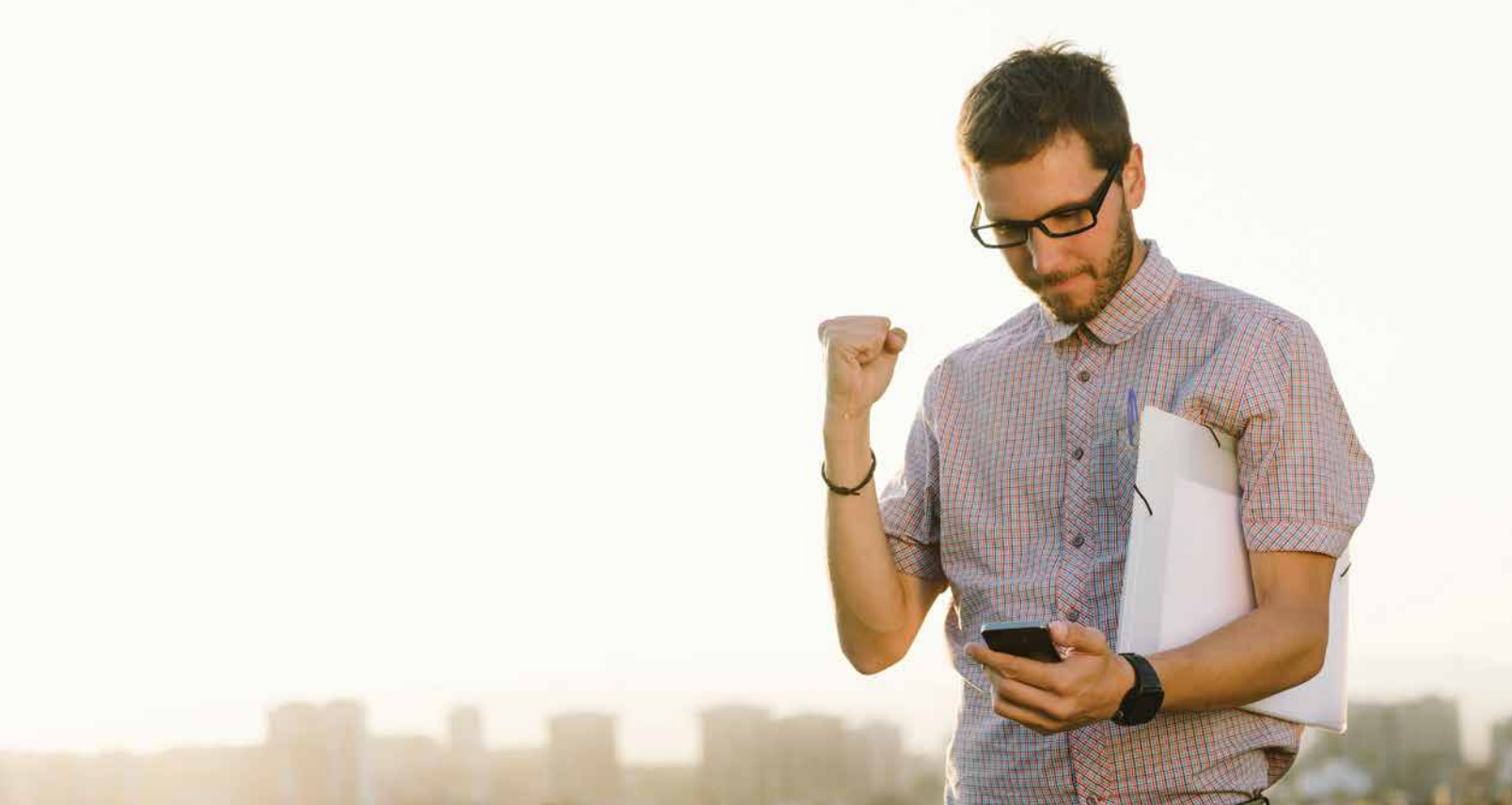
Reversing the panel decision, the Federal Circuit cited "the strong presumption" in favor of appealability of agency actions.

"To overcome this presumption, Congress must clearly and convincingly indicate its intent to prohibit judicial review," the majority said. "We find no clear and convincing indication of such congressional intent."

- Lexis Practice Advisor Attorney Team



RESEARCH PATH: [Intellectual Property & Technology > Patents > PTAB Proceedings > Articles](#)



EEOC LAUNCHES ONLINE SERVICE PORTAL

FOLLOWING A SIX-MONTH EVALUATION PILOT PROGRAM—conducted in Charlotte, Chicago, New Orleans, Phoenix, and Seattle—that provided online access to the Equal Employment Opportunity Commission (EEOC) to individuals seeking preliminary information about employment discrimination, the EEOC implemented the EEOC Public Portal on a nationwide basis. The Public Portal, a high-tech platform, represents "a giant leap forward for the EEOC in providing online services," according to EEOC Acting Chair Victoria A. Lipnic.

In fiscal 2017, the EEOC received nearly 700,000 preliminary inquiries in the form of telephone calls to its 800 number and visits to its regional offices. The Public Portal is intended to provide individuals with digital access to the information that would otherwise be acquired through those telephone calls and personal visits, making it easier for the inquiring public and vastly increasing agency efficiency by eliminating the need for staff to personally respond to that large number of inquiries.

Using the Public Portal, an individual will be able to submit online initial inquiries and requests for intake interviews with the EEOC,

which are normally the preliminary steps for an individual seeking to file a charge of discrimination. An individual will be able to digitally sign and file a charge prepared by the EEOC but will not be permitted to file charges of discrimination online that have not been prepared by the EEOC. Nor will an individual be able to file complaints of discrimination against federal agencies. No reason for this exclusion was provided in the public announcement of the Public Portal's launch.

After a charge is filed, the charging party will be able to use the Public Portal to provide and update contact information, agree to mediate the charge, upload documents to his or her charge file, receive documents and messages related to the charge from the agency, and check on the status of his or her charge.

- *Bender's Labor & Employment Bulletin*, Volume 18, Issue 1



RESEARCH PATH: [Labor & Employment > Discrimination and Retaliation > Claims and Investigations > Articles](#)



*Copyright © 2018. Matthew Bender & Company, Inc., a member of the LexisNexis Group. All rights reserved. Materials reproduced from Bender's Labor & Employment Bulletin with permission of Matthew Bender & Company, Inc. No part of this document may be copied, photocopied, reproduced, translated or reduced to any electronic medium or machine readable form, in whole or in part, without prior written consent of Matthew Bender & Company, Inc.

Timothy Murray MURRAY, HOGUE & LANNIS

DRAFTING ADVICE: AVOIDING DISASTROUS FORCE MAJEURE CLAUSES

Botched Force Majeure Clauses Expose Your Client to Needless Risk

As if on autopilot, attorneys sometimes tack onto their contracts generic force majeure clauses, just because everybody else does it, without bothering to tailor the clause to the particular transaction. Force majeure clauses are among the most misused provisions in the contract drafting milieu, and a botched force majeure clause can expose clients to enormous risk. It doesn't need to happen. Entire books are written on this subject, but this short article raises a few of the most troublesome issues as food for thought. Remember to consult the law of the pertinent jurisdiction because there are variations from state to state.

What Parties Automatically Get Without a Force Majeure Clause

For starters, we can't fully understand a force majeure clause if we don't understand the rights contracting parties have without one. Contracting parties automatically get the benefit of two related gap-filler doctrines that can excuse a party's obligations when an unanticipated, supervening event fundamentally alters the nature of the parties' contract: (1) impossibility, or as it is commonly called nowadays, impracticability, and (2) frustration of purpose.

Impossibility/Impracticability

The doctrine of impossibility can be traced to *Taylor v. Caldwell*,¹ where the owner of a music hall was excused of liability for failing to make the hall available due to an accidental fire that destroyed the building. Because literal impossibility was required to excuse a party's performance under this doctrine (e.g., death or destruction of the subject matter), contractual force majeure clauses that expanded the reasons to be excused from performance became all the rage.

Modern contract law, both at common law and under the Uniform Commercial Code (U.C.C.), has repackaged the impossibility doctrine as impracticability, though sometimes it's still called impossibility, and now, literal impossibility is no longer required. But old habits die hard, and parties continue to routinely include force majeure clauses, sometimes when the clauses don't add anything to what the law already provides.

Impracticability has been described in many ways, but essentially it is when a party is excused of his or her responsibilities because performance has been made excessively burdensome—impracticable—by a supervening event that was not caused by the party seeking to be excused and that is inconsistent with the basic assumption of the parties at the time the contract was made. The supervening event must be, in some sense, unforeseeable (but not

inconceivable)—that is, so unlikely that a reasonable party would not have guarded against it in the contract.

Frustration of Purpose

This aptly named doctrine focuses on the parties' purpose in making their contract and has nothing to do with a party's inability to perform. It applies where a supervening event fundamentally changes the nature of a contract and makes one party's performance worthless to the other. The best explanation for it is an example. In the landmark case of *Krell v. Henry*,² Henry rented a room from Krell for the purpose of viewing the coronation of King Edward VII. But the King fell ill, and the coronation was postponed. The very purpose of the contract—a room with a view of the coronation—was frustrated, and performance was excused.³

The Gap-Filler Doctrines Can Be Lost by Contract

Parties can lose the benefit of these gap-filler doctrines by including a force majeure clause that covers the same ground. The esteemed Judge Richard Posner wrote: "If . . . the parties include a force majeure clause in the contract, the clause supersedes the [impossibility] doctrine . . . [L]ike most contract doctrines, the doctrine of impossibility is an 'off-the-rack' provision that governs only if the parties have not drafted a specific assignment of the risk otherwise assigned by the provision."⁴

In *Aquila, Inc. v. C. W. Mining*,⁵ the court held that C. W. Mining (CWM) could not invoke these gap-filler doctrines to be excused of its contractual obligation to supply coal because the parties' contract contained a force majeure clause that expressly spelled out when supervening events would excuse performance. The terms of the force majeure clause—including a notice requirement—had not been satisfied, so "CWM cannot rely on common law defenses and the U.C.C., thereby circumventing the terms and limitations that the parties negotiated in the Contract."⁶

The protections of the gap-filler doctrines can also be lost by contractual provisions other than traditional force majeure clauses, as shown by *Trs. of Conneaut Lake Park, Inc. v. Park Restoration, LLC* (*In re Trs. of Conneaut Lake Park, Inc.*).⁷ The Trustees of Conneaut Lake Park (TCLP) contracted with Park Restoration for the latter to provide operational and management services to a building called the Beach Club. The parties' contract provided: "In the Event of termination for any reason, Park Restoration warrants and represents that it will vacate the premises ensuring that it is in broom clean condition without any damage to any equipment or property." Subsequently, the Beach Club was destroyed by a fire of unknown origin. TCLP terminated its agreement with Park Restoration and filed an adversary proceeding claiming breach of contract because Park Restoration failed to honor its obligation

¹ 3B. & S. 826, 32 L.J., Q.B. 164 [1863]. ² 2 K.B. 740 [1903]. ³ For a recent case that talks about *Krell v. Henry*, see *Wall v. Altium Grp., LLC*, 2017 U.S. Dist. LEXIS 44857 (W.D. Pa. Mar. 28, 2017). ⁴ *Commonwealth Edison Co. v. Allied-General Nuclear Services*, 731 F. Supp. 850, 855 (N.D. Ill. 1990). ⁵ 2007 U.S. Dist. LEXIS 80276 (D. Utah Oct. 30, 2007). ⁶ *Id.* at *16. ⁷ 564 B.R. 495 (Bankr. W.D. Pa. 2017).

... ATTEMPTS TO LIST EVERY CONTINGENCY THAT MIGHT BE CONSIDERED A FORCE MAJEURE EVENT MIGHT MISS THE ONE THAT ACTUALLY OCCURS. LISTING EVERY POSSIBLE CONTINGENCY IS, OF COURSE, AN IMPOSSIBILITY SINCE NO DRAFTER IS OMNISCIENT.

to return the premises in “broom clean” condition “without any damage.” Park Restoration argued that its obligations under the contract were excused under the doctrine of impossibility of performance because the existence of the Beach Club was necessary to carry out the purpose of the contract. The court rejected this argument because the plain words of the contract required Park Restoration to leave the premises “in broom clean condition without any damage.” The parties’ express allocation of risk left no room for the gap-filler doctrine of impossibility or impracticability to excuse Park Restoration of its obligations.

A Generic Force Majeure Clause May Not Provide as Much Protection as the Gap-Filler Doctrines

In drafting force majeure clauses, parties sometimes characterize force majeure events as a generic listing of unforeseen contingencies that fit the description of impracticability. The problem is, if one of those contingencies occurs, a party’s performance would be excused even without a force majeure clause. Why bother having the clause if it merely restates what the law already provides?

Worse, attempts to list every contingency that might be considered a force majeure event might miss the one that actually occurs. Listing every possible contingency is, of course, an impossibility since no drafter is omniscient. Nevertheless, the canon of construction *expressio unius est exclusio alterius* would exclude any item that is not specifically listed. There are ways to draft around that, discussed below.

In short, an improperly drafted, generic force majeure clause can leave the parties with fewer protections than they would have under the law without it. If you’re going to have a force majeure clause, you need to do it right.

Drafting Force Majeure Clauses

Don’t Mirror the Doctrine of Impracticability

The force majeure clause is a tool to allocate the risks of supervening events—you can do that in an infinite variety of ways. Your force majeure clause shouldn’t mirror the doctrine of impracticability—if it did, it’s not necessary. Most importantly, your clause should not require that the force majeure events be unforeseeable, impossible, or impracticable.

Listing Force Majeure Events—Part I: Draft Around the Canons of Construction

The clause will list as force majeure events general contingencies (discussed in this section), and it should also list contingencies specific to your client (discussed in the next section). With respect to the general listing, there is an infinite variety of lists.⁸ As noted above, an attempt to list every contingency that might be considered a force majeure event is, itself, an impossibility. If you list some contingencies, the canon of construction *expressio unius est exclusio alterius* would exclude any item not specifically listed. Therefore, an incomplete listing may unwittingly surrender some of the protections that the common law and the U.C.C. provide without a force majeure clause.

The conventional wisdom counsels drafters to accompany any listing of force majeure events with a catch-all provision in an attempt to capture events beyond the ones specifically listed. But drafting the catch-all presents its own challenges. If it merely says “. . . or any other events or circumstances beyond the reasonable control of the party affected,” the canon of construction or interpretation *eiusdem generis* likely would limit the meaning of the catch-all to the same type of events as those listed specifically. Thus, the catch-all needs to make clear that it is not limited to the same type of events. A good example is “. . . or any other events or circumstances not within the reasonable control of the party affected, whether similar or dissimilar to any of the foregoing.”

8. Here’s one suggested by Corbin on Contracts:

Neither party shall be responsible for any resulting loss if the fulfillment of any of the terms or provisions of this agreement is delayed or prevented by revolutions, insurrections, riots, wars, acts of enemies, national emergency, strikes, floods, fires, acts of god, or by any cause not within the control of the party whose performance is interfered with, which by the exercise of reasonable diligence such party is unable to prevent, whether of the class of causes enumerated above or not. Corbin on Contracts § 74.19 (2017).



Listing Force Majeure Events—Part II: Talk to the Client

Often, the most important drafting is the part where the lawyer listens to the client before a single word is put on paper. To properly draft against the risk of supervening events, you need to talk to your client about what might go wrong in the course of performance of the contract that will make it intolerably burdensome to the client. You may need to urge your client to think the way you do and not assume things will go as planned after the contract is signed—clients generally aren’t as pessimistic as lawyers.

While no one can envision everything that might go wrong, there’s no excuse for missing the big risks. If your client is contracting to supply a product, what might happen to interfere with its production or supply? What might make the price of the components intolerable? If your client’s supply of a product depends on a raw material from a sole source of supply, the continued availability of that raw material ought to be listed as an express condition to your client’s performance obligations (and call it an express condition so

that there is no doubt in the event of a dispute). Perhaps your client will need to be excused from performing if the price of a particular raw material exceeds a certain level.

In the absence of a specific contractual provision, courts are loath to characterize financial hardship due to a supervening event as a force majeure event. In *Kyocera Corp. v. Hemlock Semiconductor, LLC*,⁹ Kyocera, a producer of solar panels, contracted under a take-or-pay arrangement to purchase from Hemlock a silicon called polysilicon that was used in the manufacture of solar panels. The contract contained a force majeure clause that provided: “Neither Buyer nor Seller shall be liable for delays or failures in performance of its obligations under this Agreement that arise out of or result from causes beyond such party’s control, including without limitation: . . . acts of the Government . . .” Thereafter, the Chinese government gave solar panel producers illegal subsidies, which prompted the United States to impose import tariffs on Chinese-manufactured components of solar panels.

9. 886 N.W.2d 445 (Mich. Ct. App. 2015).

THE LESSON IS THAT IF YOU WANT YOUR CLIENT TO BE DISCHARGED OF ITS OBLIGATION TO PERFORM IN THE EVENT OF A SPECIFIC CONTINGENCY, SPELL IT OUT PLAINLY.

Kyocera claimed that this caused the price of polysilicon to rise significantly, and it invoked the force majeure clause. The court held that despite the acts of the Chinese and U.S. governments, the force majeure clause was not triggered. Kyocera was able to perform, albeit under financial conditions not to its liking. The very purpose of a take-or-pay contract is “to insure payment to the producer in the event of substantial change in the marketplace.” Importantly, the court noted: “Plaintiff opted not to protect itself with a contractual limitation on the degree of market price risk that it would assume. It cannot now, by judicial action, manufacture a contractual limitation that it may in hindsight desire, by broadly interpreting the force majeure clause to say something that it does not.”¹⁰

10. 886 N.W.2d 445 (Mich. Ct. App. 2015).

The lesson is that if you want your client to be discharged of its obligation to perform in the event of a specific contingency, spell it out plainly. You will never hear a judge complain that a contract is too clear for him or her. Don’t hide what you want in the niceties of a generic listing of force majeure events—a court may not agree that the particular risk is encompassed by it. When you spell out the risk, don’t characterize or qualify it as unforeseen or impracticable because a court may conclude it is neither. If your client fears that being so blunt might hurt the negotiations or raise unnecessary red flags with the other party, make certain your client understands the legal risk of not contracting with specificity so that he or she can make an informed decision about how to proceed.

The Nuts and Bolts

When a force majeure event occurs, the contract needs to require the affected party to give notice and to keep the other party apprised of the progress of the event. Your clause might contain language similar to this:

Upon occurrence of a force majeure event (as defined below), the non-performing party shall promptly notify the other party that a force majeure event has occurred and its anticipated effect on performance, including its expected duration. The non-performing party shall furnish the other party with periodic reports regarding the progress of the force majeure event. The non-performing party shall use reasonable diligence to minimize damages and to resume performance.

You may want to impose time limits on the duty to notify and even make notification an express condition to invoking the force majeure clause.

When a force majeure event occurs, should it discharge the affected party’s obligations altogether? Or should it merely serve as an excusable delay to give the party additional time to complete performance? If so, how much additional time should it receive? It is critically important that the delay should not extend indefinitely—the timing needs to be spelled out. Perhaps some events should allow immediate discharge while others merely serve as an excusable delay for a stated period of time. As but one example, the client’s supplier may have suffered a catastrophic fire, given notice of the event, and informed the client that the supplier will be back up and operating in nine weeks. But the client needs a prompt supply. The client learns that another supplier can fill the need but requires a long-term commitment. A carefully drafted clause anticipates this possibility and affords the client the opportunity to cancel the initial contract.

You don’t have to deal with all supervening events that affect your client in a force majeure clause. Any number of other clauses can spell out how certain supervening events are dealt with. For example, you could include a flexible-pricing clause that allows your client to pass on increased costs to the other party.

You can also have a sort of reverse force majeure clause that makes clear that an otherwise-impracticable event will not be grounds for relief.¹¹

Conclusion

When contracts are being written, clients concentrate on putting together a good business deal, but attorneys focus a lot on protecting clients in the event things go wrong. Guarding against supervening events is a daunting task, and force majeure clauses are difficult to draft. The harm from a botched force majeure clause can be enormous. That’s why we need to avoid the temptation to draft these clauses by cutting and pasting from other contracts, as we might do for a garden-variety notice provision, without tailoring the language to the present transaction. There are no shortcuts to meticulous drafting when it comes to force majeure clauses. **L**

Timothy Murray, a partner in the Pittsburgh, PA law firm Murray, Hogue & Lannis, is coauthor of the Corbin on Contracts Desk Edition (2017) and writes the biannual supplements to Corbin on Contracts.

11. For example:
In the event the demised premises are damaged or destroyed by fire or other casualty, or damaged by the demolition of any portion of the building necessitated by the enforcement of any law or Ordinance, or declared unsafe by any public authority, the Landlord shall, at own cost and expense, immediately repair, reconstruct and replace the demised premises, including improvements, extensions, alterations and additions to building made by Landlord or Tenant, all such work to be done in compliance with State Laws and City Ordinances. Marcovich Land Corp. v. J. J. Newberry Co., 413 N.E.2d 935, 939 (Ind. App. 1980).

Related Content

For additional guidance in drafting a force majeure clause, see

> [DRAFTING A FORCE MAJEURE CLAUSE](#)

RESEARCH PATH: [Commercial Transactions](#) > [General Commercial and Contract Boilerplate](#) > [Contract Boilerplate and Clauses](#) > [Practice Notes](#)

For a selection of sample force majeure clauses, see

> [FORCE MAJEURE CLAUSES](#)

RESEARCH PATH: [Commercial Transactions](#) > [General Commercial and Contract Boilerplate](#) > [Contract Boilerplate and Clauses](#) > [Clauses](#)

For detailed advice on drafting enforceable contracts, see

> [CONTRACT DRAFTING LANDMINES](#)

RESEARCH PATH: [Commercial Transactions](#) > [General Commercial and Contract Boilerplate](#) > [Contract Boilerplate and Clauses](#) > [Practice Notes](#)

For a discussion on the common risk allocation mechanisms used in commercial contracts, see

> [ALLOCATING RISK IN COMMERCIAL CONTRACTS](#)

RESEARCH PATH: [Commercial Transactions](#) > [General Commercial and Contract Boilerplate](#) > [Contract Boilerplate and Clauses](#) > [Practice Notes](#)

For an overview on the various reasons that a party to a contract can justifiably avoid performance, see

> [UNDERSTANDING EXCUSES FOR NONPERFORMANCE - CONDITIONS FOLLOWING CONTRACT FORMATION](#)

RESEARCH PATH: [Commercial Transactions](#) > [General Commercial and Contract Boilerplate](#) > [Contract Boilerplate and Clauses](#) > [Practice Notes](#)

RESEARCH PATH: [Commercial Transactions](#) > [General Commercial and Contract Boilerplate](#) > [Contract Boilerplate and Clauses](#) > [Articles](#)



**Daniel P. Adams, Gilbert G. Menna,
and Ettore A. Santucci**

GOODWIN PROCTER LLP

Top 10 Practice Tips: Real Estate Investment Trust IPOs

Capital markets transactions for real estate investment trusts (REITs), including initial public offerings (IPOs), have much in common with comparable types of transactions for other companies.

LIKE ALL IPOs, THE FUNDAMENTAL PROCESS FOR A REIT IPO involves the preparation of a registration statement (albeit on a Form S-11 instead of a Form S-1), including a prospectus, and a roadshow to be used to market the offering, as well as numerous corporate governance documents necessary to prepare the company to be a public company and qualify its stock for listing on one of the stock exchanges. However, there are a number of issues that commonly arise in REIT IPOs that are either unique to REITs or less common in non-REIT IPOs. Below are ten practice points that can help you run a REIT IPO like a pro.

1 Understand your client's goals.

Completing a REIT IPO is a complex and time-consuming process. As a result, it is critical to understand your client's goals when evaluating the benefits of an IPO as compared to other alternatives. Different clients will have different motivations for completing a REIT IPO. These may include obtaining liquidity for themselves or private equity investors, raising equity capital to pay down debt, enhancing the risk-reward balance by rolling up assets into an operating company, or opportunistically accessing the public markets to facilitate future growth. For some clients, running a dual-track process for a REIT IPO or a sale of the portfolio may make sense. For others, obtaining access to the public equity markets through means other than a traditional IPO (such as through a merger with an existing public company or an entity spun off from an existing public company or through an exchange listing without a concurrent offering) may present more



attractive alternatives. The better you understand your client's goals, the better you will be able to assist with completing a successful transaction, whether that is ultimately a traditional IPO or an alternative transaction.

2 Manage client resources.

A REIT IPO will stretch the resources of even the most sophisticated private real estate operator. You should help your client focus on the right tasks at the right time. Initial

submissions of the registration statement for the IPO typically have limited or preliminary information on certain topics, including board members, executive compensation, founders' rights, distribution policy, new credit facilities, technical details of formation transactions, corporate governance documents, and exhibit filings. Other disclosures need to be more fully refined from the beginning, including the primary business discussion, the financial statements and related disclosure, the property tables, and the industry disclosure. Prioritize the right tasks, minimize false deadlines, and establish realistic timelines.

3 Learn from peers and precedent.

You should understand which companies will be considered peers of your client. Fundamentally, your client is seeking to attract investor dollars that would otherwise be invested (or may already be invested) in peer companies. Having a good understanding of where your client will fit in the existing REIT market is critical in preparing the prospectus for the offering and helping your client make important structuring decisions. Peers are typically determined based on asset class (e.g., office, retail, residential, industrial, hotel, etc.), asset quality, market and sub-market focus, and the expected size of the company. Your client and its underwriters will likely have a good sense of the most relevant peers, but easily accessible public resources can also be helpful to point you in the right direction. These include the lists of REIT index constituents (organized by sector and subsector and market capitalization) and historical REIT IPO listings on the National Association of Real Estate Investment Trusts' website.

4 Make accounting issues an early focus.

You should help make certain that the accounting analysis is an early focus. In a REIT IPO transaction involving the roll-up of separate private real estate funds or other pools of assets, it is not always straightforward to determine the accounting predecessor whose financial statements are required to be included in the registration statement. Often the first formal submission regarding the IPO will be a pre-clearance letter to the Securities and Exchange Commission's (SEC) accounting staff regarding the anticipated accounting presentation. This submission, if necessary, will first require a clear understanding of the formation transactions in the roll-up, discussed below. Understanding how the financial statements will appear will also inform other disclosures. Financial statements for pre-IPO periods are often very dissimilar from financial statements for post-IPO periods. Adjustments to create financial statements on a combined pro forma basis are commonplace in REIT IPOs. These can get extremely intricate and require extensive footnoting and sensitivity analysis. Supplemental information may be

**NO ONE LIKES UNPLEASANT SURPRISES,
ESPECIALLY WHEN INVESTING UNTOLD
HOURS OF TIME ON A PROJECT.**

useful to provide investors with more coherent historical data to demonstrate positive trends. Joint ventures are also commonplace. Supplemental disclosures such as pro rata financial information may be important to help investors understand the true financial impact of these arrangements. You should review these supplemental disclosures carefully to comply with the SEC's rules regarding financial measures not in accordance with generally accepted accounting principles (GAAP).

5 Also focus early on tax structuring.

The tax impact of pursuing various structures can significantly impact REIT roll-up transactions, including which assets may be rolled up in a tax-efficient manner, whether certain operations need to be held in a taxable REIT subsidiary or completely separated from the REIT, and what type of equity should be issued in the roll-up transaction (e.g., common stock vs. units in an operating partnership). You should focus on tax structuring at the outset of the transaction concurrently with the initial accounting analysis. Tax effects can be a powerful undercurrent in pre-IPO planning. Miscues regarding which structural or economic features could motivate key pre-IPO constituent owners to change their behavior are dangerous, particularly when investors' consent is required for the roll-up of material assets.

6 Help manage pricing expectations.

No one likes unpleasant surprises, especially when investing untold hours of time on a project. There is a natural tendency for clients to underestimate the differences between existing public companies focused on the same asset class (who may be trading at attractive prices) and their company. Additionally, the IPO discount is a real phenomenon in the REIT space. Clients should expect that they will have to articulate compelling post-IPO trends and strategies and offer valuation concessions to make the IPO attractive to institutional investors. Encourage your clients to obtain a realistic assessment of likely pricing and sensitivity analysis around key variables as early as possible to help minimize unhappy clients and busted deals.

7 Closely coordinate roll-up and IPO.

As noted above, REIT IPOs often involve the roll-up of separate private real estate funds or other pools of assets that the REIT will own following the IPO. As a result, a REIT IPO can effectively involve the structuring of multiple concurrent acquisition transactions in addition to the IPO. However, the structure of these transactions often differs from typical private real estate transactions. For example, roll-up transactions that require the REIT to acquire real estate assets for a fixed dollar amount in shares or cash (which are the norm for private real estate transactions) introduce levels of risk that are often unacceptable in a REIT IPO. This is particularly true for assets that are to be part of the REIT's core portfolio. Properly structuring these transactions and managing the third-party consent process are among the most critical aspects of a successful REIT IPO.


8 Navigate the corporate governance landscape.

Successfully navigating the corporate governance landscape for any IPO requires consideration of many factors, including stock exchange rules, state organizational law, peer analysis, client specific considerations, and the views of dedicated investors and advisory firms. For a typical REIT IPO, there are a number of unique considerations, including the structure of the REIT ownership limit, potential pass-through voting for unitholders in the operating partnership of an UPREIT (i.e., an umbrella partnership REIT, which is a common structure for REITs where substantially all of the REIT's assets are held indirectly through an operating partnership owned and controlled by the REIT), the corporate governance analysis of Green Street (an independent research and advisory firm in the commercial real estate sector), and the handling of unique Maryland-specific governance issues (where most REITs are organized). Governance choices can impact the REIT long after

Related Content


For a primer on real estate investment trusts (REITs), see

> [BASIC REIT STRUCTURES AND ENTITY TYPES](#)

 **RESEARCH PATH:** [Corporate and M&A](#) > [Real Estate Investment Trusts](#) > [REIT Transactions](#) > [Practice Notes](#)

To learn about drafting a REIT transaction, see

> [REIT TRANSACTION DRAFTING CONSIDERATIONS](#)

 **RESEARCH PATH:** [Corporate and M&A](#) > [Real Estate Investment Trusts](#) > [REIT Transactions](#) > [Practice Notes](#)

For an outline of factors to consider when setting up a REIT deal, see

> [REAL ESTATE INVESTMENT TRUST \(REIT\) DUE DILIGENCE CHECKLIST](#)


 **RESEARCH PATH:** [Corporate and M&A](#) > [Real Estate Investment Trusts](#) > [REIT Transactions](#) > [Checklists](#)

For information on avoiding pitfalls in REIT M&A deals, see

> [5 DO'S AND DON'TS FOR CRAFTING M&A DEALS IN HOT REIT MARKET](#)

 **RESEARCH PATH:** [Corporate and M&A](#) > [Real Estate Investment Trusts](#) > [REIT Transactions](#) > [Articles](#)

10 Avoid late surprises from the SEC.

You do not want to have to tell your client that a delayed launch of their IPO is necessary because you are concerned about clearing SEC comments prior to pricing. To avoid this result, you should ensure that early submissions of the registration statement or supplemental submissions include sufficient information to draw out SEC comments. Also, closely review the roadshow presentation to make sure key information is included in the IPO prospectus and identify non-GAAP financial measures and adjustments to GAAP numbers that are important to convey to investors well before numbers for the final quarter prior to the launch of the IPO are completed. Finally, ensure that a completed version of the distribution policy disclosure (commonly referred to as the magic page) is produced and shared with the SEC early in the process. 

Daniel P. Adams is a partner in Goodwin Procter's Business Law Department, where he is a member of the REITs and Real Estate M&A Group and Capital Markets Group. Mr. Adams focuses primarily on public and private offerings of securities, corporate governance, securities law compliance for public companies, executive compensation, and other matters of general corporate and securities law. Mr. Adams's experience in corporate finance includes representing public and private companies, including publicly traded REITs, and underwriters in transactions such as IPOs, follow-on and shelf offerings, and 144A offerings of equity and debt securities. **Gilbert G. Menna** is a co-chair of the firm's REITs and Real Estate M&A Practice. Mr. Menna also participates in the firm's Mergers & Acquisitions, Capital Markets, Public Companies, Real Estate Tax, and Private Investment Funds Practices. Mr. Menna represents many of the nation's leading publicly traded real estate operating companies in connection with their merger and acquisition, corporate finance, and corporate governance matters. In addition to his extensive knowledge of the public REIT industry, he also has significant experience representing a variety of real estate investment managers in connection with their private equity capital, merger and acquisition, and portfolio acquisition transactions. **Ettore A. Santucci**, a partner in the firm's Business Law Department, chairs the Capital Markets Group and co-chairs the REITs and Real Estate M&A Group. He focuses primarily on public and private securities offerings, corporate governance, securities law compliance, cross-border transactions, and mergers and acquisitions. Mr. Santucci has extensive experience in equity and debt capital markets transactions. He has special expertise in structuring leveraged transactions for enterprises with complex capitalization strategies seeking to access the capital markets.

the IPO is complete. As a result, to help your client make the best choices, you will need to consider the longer-term impact of various corporate governance choices as well as the structure that will give the IPO the best chance for success.

9 Focus on key non-GAAP financial and operational metrics.

Even more so than some other industries, the REIT industry has its own unique set of non-GAAP financial measures and other operational metrics that are key focal points for investors (e.g., funds from operations (FFO), adjusted FFO (AFFO), net operating income (NOI), net asset value (NAV), annualized base rent (ABR), and many others). You should invest in understanding these terms, if you don't already, including important definitional subtleties to help ensure consistency, collective understanding, and accurate and compliant disclosure.

 **RESEARCH PATH:** [Capital Markets & Corporate Governance](#) > [IPOs](#) > [Conducting an IPO](#) > [Practice Notes](#)



Julie M. Capell DAVIS WRIGHT TREMAINE LLP

DRAFTING OFFICE RELATIONSHIP CONTRACTS PROTECTING EMPLOYERS

This article provides guidance on the main terms of an office relationship contract. When an employer chooses to permit employees to date and/or marry—or must allow fraternization under the privacy laws of the relevant state—the employer should consider requiring that the employees execute an office relationship contract (sometimes called a love contract). The purpose of such a contract is to help avoid potential sexual harassment liability if the employees’ romantic relationship ends and one of the employees then makes a hostile work environment claim.

ONCE AN EMPLOYER BECOMES AWARE OF A CONSENSUAL, romantic relationship between two employees, the human resources manager, or other equivalent professional, should meet with the employees—separately—to discuss the office relationship contract. During these meetings, the company representative should fully explain the terms of the office relationship contract to the employees and confirm that the relationship is, in fact, entirely consensual. The employer should also give the employees the opportunity to review the contract and consult with an attorney before signing it. Unlike other contracts, executing an office relationship contract will rarely involve any negotiation because it contains straightforward terms and serves overall to acknowledge the consensual nature of the relationship. Continued employment for the employees, despite their romantic relationship, is considered adequate consideration for the terms and conditions of the agreement.

Consensual Nature of the Relationship

First and foremost, the employees should acknowledge that their relationship is welcome and consensual.

Equal Employment Opportunity Workplace

Next, the employees should acknowledge that they are aware that the employer is committed to providing a workplace free of harassment, discrimination, conflicts of interest, and favoritism, and that the employer will not tolerate unwelcome or offensive conduct, behavior that creates a hostile work environment, or sexual harassment. In other words, the employee must acknowledge that the employer is an equal employment opportunity employer, does not discriminate based on any protected characteristic, whether under federal, state, or local law, and that sexual harassment is strictly prohibited. Moreover, to help avoid retaliation claims, the office relationship contract should expressly state that the employee will not be subject to retaliation for ceasing a relationship with the other employee.

Conflicts of Interest


Employers should carefully consider how they want to avoid conflicts of interest between the romantically involved employees. The most conservative, and litigation adverse, approach is to prohibit the employees from having any ability to affect the terms

and conditions of the other’s employment. Depending on the circumstances, this may involve a lateral transfer or change in job duties, or, at worst, a demotion or termination. If a demotion or termination is necessary, you should advise the employer to ask the employees to decide whom the employer should demote or terminate.

Related Content


For an annotated retaliation policy, see

> [ANTI-RETALIATION POLICY \(WITH ACKNOWLEDGEMENT\)](#)

 **RESEARCH PATH:** Labor & Employment > Discrimination and Retaliation > Policies and Procedures > Forms & Guidance


For state-specific anti-retaliation policies, see

> [DISCRIMINATION AND RETALIATION STATE EXPERT FORMS AND CHECKLISTS CHART](#)

 **RESEARCH PATH:** Labor & Employment > Discrimination and Retaliation > Claims and Investigations > Forms & Guidance


For guidance on developing a workplace relationship policy, see

> [COMPOSING OFFICE RELATIONSHIP / FRATERNIZATION POLICIES](#)

 **RESEARCH PATH:** Labor & Employment > Employment Policies > Standards of Conduct > Practice Notes

For a detailed checklist on drafting arbitration agreements, see

> [MANDATORY ARBITRATION AGREEMENT DRAFTING CHECKLIST](#)

 **RESEARCH PATH:** Labor & Employment > Employment Contracts > Waivers and Releases > Checklists

THE OFFICE RELATIONSHIP CONTRACT SHOULD NOT GO AS FAR AS STATING THAT THE EMPLOYEES EXPRESSLY WAIVE ANY SEXUAL HARASSMENT CLAIM AGAINST THE EMPLOYER, AS SUCH A PROVISION WOULD LIKELY NOT BE ENFORCEABLE.

Specifically, if the employees are already in a reporting relationship when they disclose the romantic relationship, the employer should immediately remove that reporting relationship (i.e., transfer or change job duties). It is not recommended that the employer allow an office relationship between individuals in a reporting relationship. If the employees at issue do not have a reporting relationship, the agreement should specify that the employees will not seek out


jobs where one of them would be in a reporting relationship with the other. The employer should also decide whether to restrict this provision prohibiting the employees from affecting the terms and conditions of the other's employment only during the duration of the relationship. To minimize exposure from discrimination or retaliation claims, it is considered best practice to leave the prohibition in place even after the relationship ends.



Related Content


For detailed information on sexual harassment and other hostile work environment claims, see

> [EXAMINING HARASSMENT CLAIMS](#)

 **RESEARCH PATH:** [Labor & Employment > Discrimination and Retaliation > EEO Laws and Protections > Practice Notes](#)


Also see

> [FARAGHER-ELLERTH PROVISION FOR SUMMARY JUDGMENT BRIEF](#)

 **RESEARCH PATH:** [Labor & Employment > Discrimination and Retaliation > Claims and Investigations > Forms & Guidance](#)

For a non-jurisdictional arbitration clause and state-specific arbitration clauses, see

> [THE ARBITRATION AGREEMENTS COLUMN OF EMPLOYMENT LITIGATION STATE EXPERT FORMS AND CHECKLISTS CHART](#)


 **RESEARCH PATH:** [Labor & Employment > Employment Litigation > Class and Collective Actions > Forms](#)

General Employee Representations/Agreements

The balance of the office relationship contract should:

- Reinforce the consensual nature of the relationship.
- Set forth guidelines for appropriate workplace behavior (e.g., employees should agree not to engage in public displays of affection or in any behavior that could be construed as favoritism, and they should agree to behave professionally toward one another at all times).
- Explain that the agreement is confidential.
- Encourage the employees to consult with an attorney before signing the agreement.

The office relationship contract should not go as far as stating that the employees expressly waive any sexual harassment claim against the employer, as such a provision would likely not be enforceable.

The employer may also wish to include an arbitration provision in the agreement, which would govern any dispute arising from the romantic relationship (but carefully consider state and local laws to ensure enforcement of the arbitration provision). 



Julie M. Capell is a partner with Davis Wright Tremaine LLP and works with companies across the country to meet their labor and employment needs. She provides strategic guidance by crafting policies and procedures that protect employers and minimize the risk of litigation. Ms. Capell regularly counsels clients and presents trainings and seminars on personnel policies, wage and hour compliance, federal and state disability laws, sexual harassment, retaliation, and reasonable accommodation of disabilities.



RESEARCH PATH: [Labor & Employment > Discrimination and Retaliation > Claims and Investigations > Practice Notes](#)

Office Relationship Contract

This form is an office relationship contract (also known as a love contract) for use by an employer that allows romantic relationships at work. This form is intended for private employers and is based on federal law. As a result, this form does not address all potential state and local distinctions, and you should check any relevant state and local laws.

This form includes practical guidance, drafting notes, and alternate clauses.

Overall, the office relationship contract should acknowledge the consensual basis of the relationship and document the main ground rules associated with the employees' office relationship. This type of office relationship contract can help employers avoid potential liability for possible sexual harassment claims after the employees' relationship ends.

Section 1: Consensual relationship. We, the undersigned employees, hereby acknowledge that we have voluntarily entered into a consensual, romantic relationship. We understand and acknowledge that neither of us wants our relationship with one another to affect our jobs or the Company in any way.

Section 2: Equal Employment Opportunity Policy. We also acknowledge that it is the policy of the Company to provide its employees with an equal opportunity in hiring, employment, promotion, compensation, and all other employment-related decisions without regard to race, color, sex, religion, national origin, citizenship, age, disability, or any other basis set forth in the applicable federal, state, and local laws or regulations relating to discrimination in employment.

The Company's policy on these matters is attached to this agreement.

Acknowledgement regarding Equal Employment Opportunity Policy. The undersigned agree that they have received, read, and understand the Company's Equal Employment Opportunity Policy and agree to adhere to all of its terms.

Section 3: Anti-harassment Policy. The undersigned further recognize and acknowledge that the Company does not tolerate sexual harassment. Unwelcome sexual advances, requests for sexual favors, and other verbal, physical, or visual conduct based on sex constitute unlawful sexual harassment when (1) submission to such conduct becomes an implicit or explicit term or condition of employment; (2) submission to or rejection of the conduct is used as the basis for any employment decision; or (3) the conduct has the purpose or effect of unreasonably interfering with an individual's work performance or creating an intimidating, hostile, or offensive working environment. Other forms of sexual harassment include, but are not limited to, the following:

- Verbal sexual innuendoes, suggestive comments, jokes of a sexual nature, sexual propositions, and threats
- Comments or questions about an individual's body, sexual orientation, sexual prowess or sexual deficiencies, or the use of sexually degrading or vulgar words to describe an individual
- Non-verbal sexually suggestive objects or pictures (e.g., scantily clad models, cartoons, etc.), suggestive or insulting sounds, leering, whistling, and obscene gestures
- Unwanted physical contact, including touching, pinching, and brushing against the body

The Company's policy on these matters is attached to this agreement.

Acknowledgement regarding Anti-harassment Policy. The undersigned agree that they have received, read, and understand the Company's Anti-harassment Policy and agree to adhere to all of its terms.



Section 4: Conflicts of interest. We, the undersigned, agree not to participate in or directly or indirectly influence, either positively or negatively, any decision related to the other's employment, including, but not limited to, assignments of clients and/or projects, evaluations, discipline or discharge, compensation, promotion, and development. We also agree not to seek a position that would create a reporting relationship with one another. We understand that one or both of us may need to transfer to another department to remove any conflicts of interest in our working environment. If a transfer will not remove the conflict of interest, we also understand that one of us may have to resign or be demoted to resolve the conflict of interest. We further understand that we are responsible for choosing which of us will be subject to a transfer, demotion, or resignation. If we fail or refuse to choose, the Company will be forced to choose for us, and we understand that the Company will make such a decision without regard to any protected characteristic and in compliance with the Equal Employment Opportunity and Anti-harassment Policies. We agree to comply with this conflicts of interest provision for the duration of our employment and after the employment relationship ends.

Section 5: Further agreements and acknowledgments. We, the undersigned, further agree as follows:

- Our romantic relationship is voluntary, welcome, and consensual.
- Either of us may terminate the relationship at any time without suffering workplace retaliation of any form.
- We each understand and agree that employment with the Company may be terminated at any time, with or without cause.
- Neither of us will seek or accept a direct supervisory or reporting relationship with the other.



Lindsay Burke and Moriah Daugherty COVINGTON & BURLING LLP

Cyber Risks in the Workplace: Guidance for Employers on Managing Insider Threats

Today, among the most critical risks a company can face are the cyber risks associated with its own employees or contractors. Companies are confronting an increasingly complex series of cybersecurity challenges with employees in the workplace, including employees failing to comply with established cybersecurity policies, accidentally downloading an attachment containing malware or providing their credentials in response to a phishing scam, or intentionally stealing company information for the benefit of themselves or the company’s competitors by simply copying information to their email or a thumb drive and leaving the company.

CONTRACTORS OR CONSULTANTS WITH ACCESS TO COMPANY systems can pose these same challenges. To guard against these risks, companies can implement various policies and procedures to address an employee’s tenure, from pre-hiring to post-employment, and can implement many of these same precautions with respect to contractors, consultants, or any other third parties with access to company systems.

Policies and Procedures to Protect Employers

Before hiring employees or contractors, companies can ensure that they have policies and procedures in place to protect themselves. Particularly important policies include:

- Acceptable use of electronic devices and systems
- Mobile devices
- Data collection and retention
- Notice and consents for monitoring and collection of information on company systems –and–



- Background check policies that permit pre-employment and ongoing vetting of all employees

- We will not engage in any conduct that could reasonably be regarded by co-employees as favoritism.
- We will behave professionally toward one another at all times, even if the relationship ends.
- We will not engage in any public displays of affection or other inappropriate conduct in the workplace or at work-related functions.
- We acknowledge that our relationship does not violate the Company’s Equal Employment Opportunity and Anti-harassment Policies and that participation in the relationship has not been made a condition or term of employment. We also agree that we will comply at all times with the Company’s Equal Employment Opportunity and Anti-harassment Policies.
- We agree to inform the Company immediately if the relationship ends or if the conduct of the other employee is no longer welcome.
- We each agree that if the relationship ends, we will respect the other person's decision to end the relationship and will not retaliate against the other person, engage in any unprofessional or inappropriate efforts to resume the relationship, or engage in any other conduct toward the other person that could violate the Company’s Equal Employment Opportunity and Anti-harassment Policies.
- We acknowledge that this agreement is confidential and not intended to invade our privacy. Rather, it is meant only to affirm that both of us have received and agree to comply with all relevant policies.
- Finally, we acknowledge that we may consult with an attorney before signing this agreement.

Employees:

[name]

[date]

[name]

[date]



Form provided by **Julie M. Capell**, a partner with Davis Wright Tremaine LLP. She provides strategic guidance by crafting policies and procedures that protect employers and minimize the risk of litigation.



RESEARCH PATH: [Labor & Employment > Discrimination and Retaliation > Claims and Investigations > Forms](#)

EMPLOYEES SHOULD BE ASKED TO EXECUTE A NON-DISCLOSURE AGREEMENT AND OTHER DOCUMENTS THAT PROTECT THE COMPANY'S INFORMATION, AND THE EXECUTED COPIES OF THESE DOCUMENTS SHOULD BE SAFELY STORED IN THE COMPANY'S PERSONNEL FILE OR HUMAN RESOURCES SYSTEM.

Companies should enact enhanced screening and background checks for new hires who will have access to the company's crown jewels and systems that can connect to or access the same, and companies should require third parties that provide contractors to demonstrate that they are doing the same.

When drafting policies, companies should ensure all important stakeholders are coordinated—including human resources, information technology, and legal—and that all employee-related policies are aligned with other company policies, particularly the incident response plan, data security, and cybersecurity policies.

When onboarding employees, companies should use procedures including training, policy review, and key acknowledgements and consents to establish a culture of awareness and compliance. It is particularly important for companies to complete the following tasks during employee onboarding:

- Apprising new employees of the company's expectations regarding protection of confidential information and critical infrastructure (including ensuring that no new employee has brought any confidential information from another company with them)
- Providing a briefing of policies governing employee access to information and those that could implicate employees' privacy
- Notifying employees that they have no expectation of privacy if using personal devices for business purposes –and–
- Obtaining employee consent to any applicable monitoring

Employees should be asked to execute a non-disclosure agreement and other documents that protect the company's information, and the executed copies of these documents should be safely stored in the company's personnel file or human resources system.

Companies can and should also implement parallel procedures for outside directors, vendors, contractors, and third parties with access to company networks and systems.

Employers Must Regularly Assess Indicators of Any Potential Issues

After employees begin work, companies should regularly assess indicators of any potential issues, including:

- Any unusual systems accessed by employees
- What documents and information employees are downloading, printing, or emailing
- When employees are performing actions on company systems –and–
- Any efforts by employees to exceed access privileges or records of failed login attempts

Monitoring

Conducting real-time monitoring of employees has significant privacy implications, particularly outside the United States. As a result, a company will typically want to notify employees of the monitoring and obtain prior consent or acknowledgement that an employee's use of the system constitutes consent to the interception of their communications and the results of such monitoring may be disclosed to others, including law enforcement.

Training

Companies should conduct regular, required training with employees concerning cyber risks, including the risks associated with phishing attacks and fraudulent email solicitations. In addition, companies should make sure that compliance with security policies is included as a metric in performance evaluations for employees, particularly those employees with access to business critical information.

Contractors & Consultants

These same procedures should be in place for contractors, consultants, or any other third parties who have access to company systems and information. If necessary, companies should review the contracts they have with vendors or staffing agencies to ensure that proper procedures and consents are in place.



Disgruntled Employees or Insider Threats

If a company believes an employee is potentially disgruntled or an insider threat, the employee's manager should coordinate with other departments—including legal, human resources, and information technology—to obtain additional information and plan a course of action. Investigations can include forensic computer or network searches, preservation of affected systems, and interviews with employees. While developing the facts, a company should consider when and how to suspend or revoke a suspected insider threat's access or take additional action against the insider—but beware that taking action against a suspected employee is likely to implicate employment laws in the United States or elsewhere.

Off-boarding Employees

When off-boarding employees, companies should take steps to protect themselves. It is imperative for companies to develop policies and procedures for off-boarding employees that are directed at minimizing risks of data leakage. Exit interviews should be conducted wherever possible; they will allow companies to spot potential problems or identify red flags.

Resignations

When an employee resigns, a company should decide whether to institute a protocol to remove or limit the employee's access to confidential information even before the employee's last day at work. Human resources should work with the information technology department to audit the employee's most recent network access and email activity to ensure the employee has not harvested any confidential information.



Jerred Blanchard BAKER & MCKENZIE LLP

The Tax Cuts and Jobs Act: Insights and Planning Tips from Corporate/Business Portions of New Tax Law



Terminations

When the company is preparing to terminate an employee, the company should implement a protocol to protect company confidential information, including reducing the employee’s access to networks and systems before, or simultaneously with,

notifying the employee of the impending dismissal. The same should be done when a contract with a consultant, vendor, or contractor is nearing its end.

All employees who leave the company, and all contractors whose contracts end, should be reminded of ongoing obligations to protect the confidential information of the company and should be asked to return all company information, documents, and electronic equipment before their last day at work.

Conclusion

Employees can present a significant threat to a company’s business critical information, as can contractors or consultants with access to company systems. Companies should ensure that relevant departments within the company, such as the legal, human resources, and information technology departments, are coordinating to take steps to protect the company against such threats, including those set forth above. **L**

Lindsay Burke, a partner at Covington & Burling LLP, is vice chair of the firm’s employment practice group and regularly advises U.S., international, and multinational employers on employee management issues and international human resources compliance. Moriah Daugherty is an associate at the firm advising clients on a broad range of cybersecurity, data privacy, and national security matters. The authors may be contacted at lburke@cov.com and mdaugherty@cov.com.

Related Content

For a review of recommended cybersecurity measures to be taken by employers, see

> [CYBERSECURITY MEASURES TO PROTECT EMPLOYERS’ CONFIDENTIAL INFORMATION AND TRADE SECRETS](#)

RESEARCH PATH: [Intellectual Property](#) > [Privacy & Data Security](#) > [Privacy Policies](#) > [Practice Notes](#)

To learn how to craft cybersecurity policies for the workplace, see

> [CREATING POLICIES ON COMPUTERS, MOBILE PHONES, AND OTHER ELECTRONIC DEVICES](#)

RESEARCH PATH: [Labor and Employment](#) > [Privacy, Technology, and Social Media](#) > [Policies and Procedures](#) > [Practice Notes](#)

For a sample cybersecurity form for employers, see

> [MODEL POLICY ON THE USE OF ELECTRONIC COMMUNICATION SYSTEMS](#)

RESEARCH PATH: [Intellectual Property & Technology](#) > [Privacy & Data Security](#) > [Privacy Policies](#) > [Forms](#)

RESEARCH PATH: [Intellectual Property & Technology](#) > [Privacy & Data Security](#) > [Privacy Policies](#) > [Articles](#)

Background

On December 20, 2017, for the first time in 30 years, Congress passed major tax legislation in the form of the Tax Cuts and Jobs Act of 2017, Pub. Law No. 115-97 (Act), signed into law by President Donald J. Trump on December 22, 2017. The legislative text and a joint explanatory statement (Conference Agreement or Conference Report) were released by the Conference Committee on December 15, 2017. From a business

point of view, the Act is best known for its reduction of the maximum corporate tax rate from 35% to 21% and its shift to a territorial system for taxing earnings of multinationals.

On balance, it can be said that the Act is a laudatory piece of legislation that goes a long way toward encouraging both business investment in the United States and private-sector employment in the United States. However, many commenters have observed that the Act was quickly drafted and has not

been fully vetted by stakeholders, which means that the Act may contain drafting errors that lead to unintended consequences. Thus, a 2018 technical corrections bill likely will be drafted, although it will be very hard to pass since it would require affirmative votes of Democrats in the Senate to reach the 60-vote threshold needed for legislation for which reconciliation is not available. In the meantime, regulatory guidance from the U.S. Department of the Treasury will need to be swift and comprehensive. In addition, the Joint Committee on Taxation (JCT) is preparing a bluebook describing the legislation, yet to be released. Doubtless, taxpayers will want to forward comments to the Treasury Department, their representatives in the House and Senate, and JCT pointing out errors and unintended consequences that affect them and encouraging the enactment of technical corrections or Treasury regulations to solve those problems.

What follows is a short summary of key provisions of the Act of interest to taxpayers doing business in the United States, with occasional observations or planning thoughts. The summary is divided into two segments, the first addressing key provisions primarily affecting C corporations doing business in the United States, and the second more briefly addressing key provisions primarily affecting all other taxpayers doing business in the United States. Provisions addressing special industries, such as banks and insurance companies, are beyond the scope of this article.

Provisions Primarily Affecting C Corporations

Domestic Provisions

Corporate tax rate reduction and alternative minimum tax (AMT) repeal. The maximum corporate tax rate imposed on a domestic C corporation is reduced from 35% to 21% for tax years beginning after December 31, 2017, with partial benefit for corporations having fiscal years beginning in 2017. Also, the Act repeals the AMT for corporate taxpayers, substituting the Senate’s Base Erosion and Anti-Abuse Tax (BEAT).

Expensing. For depreciable property with a life of 20 years or less, if the property is acquired and placed in service on or after September 27, 2017, and on or before December 31, 2022, 100% of the cost of the property is deductible. This temporary 100% expensing regime phases out over the five years beginning after December 31, 2022.

Elimination or reduction of other domestic tax benefits. To partially pay for the foregoing tax benefits and achieve other goals (e.g., inhibit earnings stripping or base erosion):

- The domestic production deduction of I.R.C. § 199 is repealed for tax years beginning after December 31, 2017.
- The orphan drug credit is reduced from 50% to 25% of qualifying expenditures made in a tax year beginning after December 31, 2017.
- Effective for tax years beginning after December 31, 2021, the deduction for most R&D expenditures is repealed and five-year amortization substituted.

IN AT LEAST ONE IMPORTANT RESPECT, THE ACT GENERALLY BRINGS THE U.S. FOREIGN TAX SYSTEM IN LINE WITH INTERNATIONAL NORMS BY PROVIDING A PARTICIPATION EXEMPTION.

Like-kind exchanges under I.R.C. § 1031 are eliminated for property other than real estate, effective for exchanges completed after December 31, 2017.

For most accrual method taxpayers, effective for tax years beginning after December 31, 2017, (1) income received in a tax year cannot be deferred beyond the tax year in which the income is included on a taxpayer’s financial statement, and (2) advance payments for goods, services, or other specified items may not be deferred beyond the close of the tax year of receipt unless the income is also deferred for financial statement purposes.

In the case of a net operating loss (NOL) described in I.R.C. § 172, for NOLs arising in tax years beginning after December 31, 2017, (1) the carryback is repealed, (2) the carryover limitation is repealed (i.e., the NOL can be carried forward indefinitely), and (3) an NOL carried over to a tax year cannot be used to offset more than 80% of the taxable income earned in that year. Note that, unlike the Conference Report, the statutory language states that the modifications to the carryovers and carrybacks apply to NOLs arising in tax years ending after December 31, 2017.

Effective for tax years beginning after December 31, 2017, I.R.C. § 163(j)’s limitation on the deductibility of interest is significantly expanded.

International Provisions

The Act makes fundamental and sweeping changes to the U.S. taxation of international businesses. The overarching purposes of this new international tax regime include making U.S. multinationals more competitive with companies based in other countries, removing impediments to the repatriation of profits to the United States, reducing opportunities to shift income offshore to low-tax jurisdictions, incentivizing exports of products and services from the United States, and preventing erosion of the U.S. tax base by foreign companies. The following is a summary of the key changes to the system.

Forced deemed repatriation. Generally, new I.R.C. § 965 increases the Subpart F income of a CFC (controlled foreign corporation), or a foreign corporation with at least one 10% U.S. shareholder that is a domestic corporation, for its last tax year ending before January 1, 2018, by the greater of (1) the CFC’s

“accumulated post-1986 deferred foreign income” determined as of November 2, 2017, without regard to distributions, or (2) such income determined as of December 31, 2017.

Participation exemption. In at least one important respect, the Act generally brings the U.S. foreign tax system in line with international norms by providing a participation exemption. Under the participation exemption in new I.R.C. § 245A, eligible dividends a U.S. corporation receives from an eligible foreign corporation qualify for a deduction equal to the full amount of the dividend sourced to foreign earnings. As a result, qualifying dividends are only subject to foreign tax and are effectively exempt from U.S. tax.

Deduction for foreign-derived intangible income (FDII). New I.R.C. § 250 provides a special deduction for a domestic corporation’s FDII. In summary, the provision provides a lower rate of tax on a portion of profits derived from sales into foreign markets. In the language of the Conference Report, a domestic corporation’s FDII is the portion of its income “that is derived from serving foreign markets,” in excess of a deemed return on tangible assets (the “applicable deemed tangible income return”). Broadly speaking, a domestic corporation is allowed a deduction under new I.R.C. § 250 in an amount equal to 37.5% of its FDII, resulting in an effective tax rate on FDII of 13.125%. The deductible percentage of FDII declines to 21.875% in tax years beginning in 2026 and beyond, resulting in an effective tax rate on FDII of 16.406%.

Global intangible low-taxed income (GILTI). In addition to the new FDII regime, the Senate bill introduced a new category of income, GILTI, similar to Subpart F income. This provision is the stick designed to encourage U.S. multinationals to move foreign operations into the United States, made more difficult by the Act’s failure to include the carrot (I.R.C. § 966), which generally would have allowed a CFC to distribute its intangible assets to its U.S. shareholders without recognizing I.R.C. § 311(b) gain. In broad strokes, GILTI taxes the aggregate net income of all of a U.S. shareholder’s CFC income not otherwise captured under the Subpart F and ECI (effectively connected income) provisions of the Internal Revenue Code’s net CFC tested income, less a return on the tangible assets held by those CFCs used for the production of tested income in a trade or business (deemed tangible income return).



Base erosion. The Conference Agreement adopted in large part the BEAT, an AMT found in new I.R.C. § 59A designed to prevent base erosion through deductible payments. The BEAT will apply to base erosion payments paid or accrued in taxable years beginning after December 31, 2017. Under the BEAT, an applicable taxpayer is required to pay a tax equal to the base erosion minimum tax amount for the taxable year. The BEAT applies to corporations with average annual gross receipts for a three-taxable-year period of at least \$500 million and a “base erosion percentage” for the taxable year of at least 3% (2% for banks and registered securities dealers).

Foreign tax credits. Under the territorial taxation regime of new I.R.C. § 245A, earnings of foreign subsidiaries of a U.S. corporation are no longer subject to U.S. income taxation when distributed as a dividend to the U.S.-resident shareholder. Consequently, the deemed-paid credit of I.R.C. § 902 is no longer required to prevent double taxation of these earnings and has therefore been repealed in its entirety in Section 14301 of the Act. In contrast to the treatment of actual dividends, Subpart F income inclusions under I.R.C. § 951 are still subject to full income taxation in the United States. I.R.C. § 960 will be amended to deem a U.S. corporate shareholder to have borne its pro rata share of the foreign income taxes imposed on the Subpart F income of its CFC without relying on repealed I.R.C. § 902. The U.S. corporate shareholder is also deemed to bear any additional foreign income taxes imposed on an actual distribution of earnings described in I.R.C. § 959 as having been previously taxed under I.R.C. § 951 and is entitled to a foreign tax credit equal to 80% of foreign income tax imposed on its GILTI inclusion. Under the new territorial regime, the CFC no longer tracks a pool of earnings and taxes. Instead, the deemed-paid taxes under I.R.C. § 960 are those that are allocated to the Subpart F income of the CFC, under rules similar to those that currently govern the allocation of taxes to the separate foreign tax credit baskets. Conforming amendments have been made to other sections of the I.R.C., including the I.R.C. § 78 gross-up.

Provisions Primarily Affecting Non-corporate Taxpayers

Domestic Provisions

Tax rate reduction. The bill reduces the maximum marginal tax rate for individuals from 39.6% to 37%. The maximum 37% rate applies in 2018 to married individuals filing joint returns with income over \$600,000 and single individuals with income over \$500,000. The Act also effectively doubles the amount of the standard deduction and makes changes to many popular deductions, such as the state and local tax deduction and the mortgage interest deduction. Unlike the income tax rate reduction for corporations, which is permanent, the income

tax rate reduction and other changes for individual taxpayers are temporary and scheduled to expire in 2026. The Act maintains the AMT for individuals but increases the exemption amount and the threshold amount after which the exemption is phased out for tax years 2018 through 2025. For tax year 2018, the exemption amounts and phase-out thresholds would be \$109,400 and \$1,000,000 for joint filers and \$70,300 and \$500,000 for single filers, respectively.

Expensing. For depreciable property with a life of 20 years or less, if the property is acquired and placed in service on or after September 27, 2017, and on or before December 31, 2022, 100% of the cost of the property is deductible. The provisions (including the phase-out) are the same as for corporate taxpayers.

Special deduction for sole proprietorships and pass-through entities. The Conference Agreement largely followed the Senate bill and provides that a non-corporate taxpayer (such as an individual, estate, or trust) doing business via a partnership, S corporation, or sole proprietorship is entitled to a potential deduction based on newly defined “qualified business income” such that a full deduction effectively reduces the maximum marginal tax rate from 37% to 29.6%. Non-corporate taxpayers may deduct, in any tax year beginning after December 31, 2017, and before January 1, 2026, the lesser of (1) 20% of the taxpayer’s combined qualified business income or (2) the greater of 50% of the W-2 wages paid with respect to the qualified trade or business, or the sum of 25% of the W-2 wages with respect to the qualified trade or business plus 2.5% of the unadjusted basis, immediately after acquisition, of all qualified property (i.e., property used and depreciated in a qualified business).

■ Qualified business income includes income (with certain exclusions) generated from a qualifying U.S. trade or business. The W-2 wage base includes all wages, including withholding amounts and amounts an employee elects to defer. A qualifying trade or business is any trade or business other than (1) a newly defined “specified service trade or business,” and (2) the trade or business of performing services as an employee. A “specified trade or business” excluded from the definition of qualifying business is expressly defined to include health, law, accounting, actuarial science, performing arts, consulting, athletics, financial services, brokerage services, or any trade or business in which the principal asset is the reputation or skill of one or more of its employees. Additionally, a “specified trade or business” includes the performance of services consisting of investing and investment management, trading, or dealing in securities, partnership interests, or commodities. Notably, performing engineering or architectural service constitutes a qualifying trade or business.

■ The new rules also contain income thresholds; phase-in limitations; and rules intended to prevent guaranteed payments, reasonable compensation, and payments paid to partners in non-partner capacities from qualifying for the 20% deduction. A special rule also allows a deduction of 20% of qualified real estate investment trusts and publicly traded partnership income. Finally, for partnerships and S corporations, the deduction is applied at the partner or shareholder level.

Special limitation on active business losses. Effective for tax years beginning after December 31, 2017, and before January 1, 2026, under new I.R.C. § 461(l), a taxpayer’s excess aggregate trade or business losses are disallowed for the current taxable year and not usable against other non-business income, such as wages, dividends, and interest income. This limitation is applied after the I.R.C. § 469 passive loss limitations and is applied at the partner or S corporation shareholder level.

■ “Excess business losses” are the excess of (1) the aggregate business deductions of a taxpayer over (2) the sum of (a) the gross income derived from the business plus (b) a threshold amount of \$250,000 for a single person and \$500,000 for a joint return.

■ Excess business losses disallowed in the current taxable year are treated as NOLs in subsequent taxable years with indefinite carryover subject to the new limitation of NOLs to 80% of taxable income for taxable years beginning after December 31, 2017.

New three-year holding period for carried interest. After many prior attempts to tax service partner carried interests as compensation income, the Conference Agreement reached a compromise that retained the capital nature of the income

but requires a three-year holding period to obtain the benefits of long-term capital gain rates. Specifically, this rule applies to taxpayers receiving partnership interests in connection with the performance of substantial services in any applicable trade or business consisting of (1) raising or returning capital and (2) either investing in (or disposing of) specified assets (or identifying specified assets for investing or disposition) or developing specified assets. Specified assets generally means securities; commodities; real estate held for rental or investment; cash or cash equivalents, options or derivative contracts with respect to such securities, commodities, real estate, cash or cash equivalents; as well as an interest in a partnership to the extent of the partnership’s proportionate interest in the foregoing. Holders of partnership interests that transfer their interests to related parties prior to three years in certain instances will trigger immediate gain taxed as short-term capital gain. The provision applies to tax years beginning after December 31, 2017.

Elimination or reduction of other domestic tax benefits.

Non-corporate taxpayers engaged in business will suffer the same eliminations or reductions in domestic tax benefits as corporate taxpayers, including the limitation on interest deductions in new I.R.C. § 163(j).

International Provisions

Most of the international provisions (other than the participation exemption and the BEAT, which are limited to corporations) apply to non-corporate taxpayers. However, high net worth individuals, estates, and trusts may want to focus on the following international provisions, effective for tax years beginning after December 31, 2017.



Elimination of CFC 30-day rule. The Act eliminates the requirement that a U.S. shareholder must control a non-U.S. corporation for an uninterrupted 30-day period before Subpart F inclusions apply.

CFC downward attribution. Further, the bill eliminates I.R.C. § 958(b)(4), which prevents downward attribution of stock from certain non-U.S. partnerships, estates, trusts, and corporations to U.S. persons for purposes of determining whether the CFC and U.S. shareholder tests are satisfied. This repeal may result in unintended tax and reporting consequences. For example, by eliminating this provision, a domestic corporation owned by a non-U.S. individual shareholder could be considered to own the shares of non-U.S. corporations owned by the non-U.S. individual shareholder. This could result in the non-U.S. corporations being constructively owned CFCs of the domestic corporation in certain circumstances. The domestic corporation may have a reporting obligation or an income inclusion if it directly or indirectly owns shares in the foreign corporation under I.R.C. §958(a).

Expansion of U.S. shareholder definition. The bill expands the definition of a U.S. shareholder to include any U.S. person who owns 10% or more of the total vote or value of all shares of all classes of stock of a foreign corporation. Under current law, the definition of a U.S. shareholder required the shareholder to hold 10% or more of the voting power of the CFC. Therefore, individuals who own non-voting shares in a foreign corporation that were not previously considered U.S. shareholders should determine if their non-voting shares will cause them to become U.S. shareholders and also cause the entity to become a CFC.


Repeal of indirect foreign tax credit (FTC) for non-corporate shareholders. Taxpayers that are individuals, estates, or trusts are no longer entitled to claim indirect FTCs under I.R.C. §§ 902 (also repealed for corporations) and 960 (not repealed for corporations). For example, unlike a U.S. shareholder that is a domestic corporation, an individual's Subpart F inclusion under I.R.C. § 951(a) will not entitle the individual to a FTC under I.R.C. § 960.

GILTI. The GILTI regime may cause income of a CFC (including a foreign corporation with a 10% shareholder that is a domestic corporation) that is not otherwise caught by the existing Subpart F rules to be includable in the gross income of its U.S. shareholders. This regime will affect almost all U.S. individuals, estates, and trusts that own CFCs, unless the CFC has a significant investment in tangible assets. This regime would apply to U.S. shareholders of foreign IP-rich CFCs, service provider CFCs, and CFCs with low-basis assets, and which otherwise would not cause Subpart F inclusions for its U.S.

Related Content


For more information on the use of pass-through entities to minimize taxes, see

> [TAXATION OF PASS-THROUGH ENTITIES](#)

 **RESEARCH PATH:** [General Practice > Corporations > Corporations \(General\) > Practice Notes](#)


For guidance on the federal income tax treatment of carried interest, see

> [TAXATION OF CARRIED INTEREST](#)

 **RESEARCH PATH:** [Corporate and M&A > Private Equity > Tax Matters > Practice Notes](#)


For an overview on the taxation of effectively connected income, see

> [EFFECTIVELY CONNECTED INCOME \(ECI\) AND PRIVATE EQUITY FUNDS](#)

 **RESEARCH PATH:** [Corporate and M&A > Private Equity > Tax Matters > Practice Notes](#)


For information on how taxes impact the selection of a business entity, see

> [FEDERAL INCOME TAXES](#)

 **RESEARCH PATH:** [General Practice > Taxes \(Business\) > Federal Income Taxes > Practice Notes](#)

For a discussion on the effort to eliminate corporate inversions that seek to reduce taxes, see

> [CORPORATE INVERSION REGULATION](#)

 **RESEARCH PATH:** [General Practice > Taxes \(Business\) > Federal Income Taxes > Practice Notes](#)

shareholders. That said, the GILTI regime should not apply if the CFC's foreign income is subject to foreign tax at a rate of 13.125% or more for C corporation shareholders and 18.9% or more for non-C corporation shareholders.


No participation exemption. The provision that exempts 100% of foreign source dividends paid by a specified 10%-owned foreign corporation would apply only to U.S. C corporation shareholders. When a U.S. shareholder that is an individual, estate, or trust receives a dividend from a foreign corporation, the dividend is includable in the shareholder's gross income. These U.S. shareholders of CFCs cannot claim indirect FTCs for foreign income taxes paid by the CFC.

Forced deemed repatriation. New I.R.C. § 965's forced deemed repatriation rule applies to a U.S. individual, estate, or trust that owns 10% or more of the stock of a CFC or foreign corporation that has at least one 10% shareholder that is a U.S. corporation. In simple terms, the tax applies as a Subpart F inclusion on all of the CFC's pre-effective date foreign earnings at a rate of approximately 8% for non-cash earnings and profits and 15.5% for earnings and profits held in cash. Individuals, estates, and trusts will not be afforded the benefit of FTCs for any foreign tax imposed on the CFC's earnings. That said, individuals may be afforded a partial tax credit for any foreign withholding tax imposed on the distribution of any of the foreign corporation's earnings that was subject to the forced repatriation tax. Furthermore, the new provision will allow for an eight-year deferral on payment of the tax owed, meaning the majority of payments will be owed in the later part of the eight-year period. Finally, if the CFC was owned by an S corporation, there is an indefinite deferral of the tax that may apply until one of three triggering events is met. The first triggering event is a change in the status of the corporation as an S corporation. The second category includes liquidation, sale of substantially all corporate assets, termination of business, or any similar event, including reorganization in bankruptcy. The third is a transfer of shares of stock in the S corporation by the electing taxpayer, whether by sale, death, or otherwise, unless the transferee of the stock agrees with the Secretary of the Treasury to be liable for net tax liability in the same manner as the transferor.

Sale of interest in partnership engaged in a U.S. business. The Conference Agreement codifies the aggregate theory of Rev. Rul. 91-32, to the effect that a foreign partner's gain on a sale of a partnership interest is effectively connected income to the extent the partner's distributive share of gain on a sale of partnership assets would be ECI. Additionally, a new withholding rule is enacted that requires the transferee of the partnership interest to withhold 10% of the amount realized on the sale or exchange of a partnership interest absent certification that the transferor is exempt from withholding. Congress intends for the provision to apply to a broad range of transactions, including many tax-free transfers in which taxpayers continue to retain indirect interests in the

partnership interest. As a backup enforcement mechanism, failure to withhold imposes an obligation on the partnership to deduct and withhold from distributions to the transferee partner those amounts that should have been withheld by the transferee, plus interest.

Conclusion

Although many taxpayers have been focused on immediate planning, such as deferring income beyond 2017 or accelerating deductions into 2017, it is important not to lose sight of additional legislative and regulatory events. Enacting a significant tax act is often only the first step in a prolonged process. Although Congressional leadership intends to pursue a technical corrections bill, taxpayers should not count on the passage of a technical corrections bill to correct any errors in the Act or unintended consequences caused by the Act. Instead, taxpayers should focus their energy on understanding the new provisions and determining how to comply with them in a timely fashion. Moreover, taxpayers should not be coy about contacting the Treasury Department to alert them to challenges and ambiguities that they have identified in the Act. Because many of the provisions in the Act are effective for tax years beginning after December 31, 2017, the Treasury Department will need to issue guidance on a variety of topics with great dispatch. Thus, taxpayers can provide valuable insight from the beginning of that process, helping to smooth the implementation of the Act for all parties involved. 

Jerred G. Blanchard Jr. is counsel in the Houston office of Baker & McKenzie LLP and a member of the firm's tax practice group. He is a coauthor of a well-known consolidated return treatise, has written numerous articles in various professional journals on multiple corporate tax topics, and is a frequent speaker at various legal and professional programs across the country. Prior to joining the firm, Mr. Blanchard was a principal at a Big Four accounting firm. He is one of 813 professionals recommended by The International Who's Who of Corporate Tax Lawyers.



RESEARCH PATH: [General Practice > Taxes \(Business\) > Federal Income Taxes > Articles](#)



Lexis Practice Advisor®

START HERE TO GET IT RIGHT

Practical guidance clarifies all facets of employee benefits and executive compensation to help you complete your work effectively and efficiently. Includes access to Transactions Search powered by Intelligize®, so you can glean insights into the latest trends from publicly filed contracts to support your drafting.

Lexis Practice Advisor® Employee
Benefits & Executive Compensation

LEXISNEXIS.COM/PRACTICE-ADVISOR
800.628.3612

4x

MORE PRACTICING
ATTORNEY AUTHORS



GUIDANCE LINKED
TO DEEPER RESEARCH

As compared to Thomson Reuters Practical Law network. Comparison data based on information available as of December 2017.

LexisNexis and the Knowledge Burst logo are registered trademarks of RELX, Group, used under license. © 2017 LexisNexis. All rights reserved.

PRACTICE TRENDS | Lexis Practice Advisor® IP & Technology



**Torsten M. Kracht,
Michael J. Mueller,
Lisa J. Sotto, and Daniella Sterns**
HUNTON & WILLIAMS LLP

Biometric Information Protection: The Stage is Set for Expansion of Claims

Litigation alleging the improper collection and storage of biometric data is being driven by the Illinois Biometric Information Protection Act (BIPA). The authors of this article discuss two headline-grabbing cases and which technologies and jurisdictions are next.

ALTHOUGH SEVERAL STATES HAVE ENACTED OR PROPOSED laws protecting individuals' biometric data, Illinois is the only state with an act on the books that currently permits a private cause of action for the unlawful capture and storage of biometric data. Thus, BIPA¹ is the national engine driving litigation alleging the improper collection and storage of biometric data. Dozens of new putative class actions have been filed under the law in the last six months alone, both inside and outside Illinois, with class lawyers lured by visions of penalties ranging up to \$5,000 for each willful violation and \$1,000 for each negligent violation.²

Headline-Grabbing BIPA Cases

The most headline-grabbing cases under BIPA were waged early on against tech giants Shutterfly, SnapChat, Google, and Facebook for their purportedly unauthorized application of facial-recognition technologies to static photos, but the majority of cases have been filed against companies that use ubiquitous fingerprint-capture technology in connection with access control and employee timekeeping systems. For example, grocery retailer Marianos, health club operator Life Time Fitness, Four Seasons Hotels, and United Airlines have all



been sued for collecting employee fingerprints to track work hours. Restaurant operator Superossa Restaurant Group has been sued for using fingerprint scans to track cash register use, and tanning salon operator LA Tan and daycare provider Crème de la Crème have been sued for using fingerprint capture for customer access control.

¹ 740 Ill. Comp. Stat. 14/1-14/99. ² Texas (the Texas Statute on the Capture or Use of Biometric Identifier, Tex. Bus. & Com. Code Ann. § 503.001) and Washington (2017 Bill Text WA H.B. 1493) are the only other states that have statutes addressing the collection of biometric information by private businesses.



Although one case reportedly settled for \$1.5 million in late 2016 and others³ have been dismissed for lack of standing, most private claims under the law are relatively new, and there is not yet a good track record of success or failure on which to accurately assess risk. But, if activity earlier this year in the headline-grabbing cases is any indicator, no silver bullet for eliminating the cases has appeared yet.

Shutterfly

In September, an Illinois federal judge denied a motion to dismiss the putative class action accusing Shutterfly of violating BIPA by collecting and storing without the plaintiff's consent facial recognition data from pictures uploaded to the Shutterfly website.⁴ Shutterfly's motion to dismiss argued that (1) BIPA does not apply to scans of biometric data derived from photographs, (2) application of BIPA to the complaint would give it extraterritorial effect in violation of the Dormant Commerce Clause, and (3) the plaintiff failed to allege actual damages resulting from Shutterfly's conduct. The court rejected all three arguments.

First, while recognizing that the statute expressly excludes photographs from the definition of biometric identifier, the court determined that data obtained from a photograph may nevertheless constitute a biometric identifier. Second, the court found that although the plaintiff is a resident of Florida, it would be inappropriate to conclude that the lawsuit requires extraterritorial application of BIPA or violates the Dormant Commerce Clause at the dismissal motion stage, given that the complaint alleges that the photo was uploaded to Shutterfly's website from a device located in Illinois by a citizen of Illinois and the circumstances surrounding the claim are not fully known. Lastly, the court held that a showing of actual damages was not necessary to state a claim under BIPA, analogizing to other consumer protection statutes with statutory damages provisions such as the Fair Credit Reporting Act, the Fair Debt Collection Practices Act, and the Truth in Lending Act. In a footnote, the court also found that the plaintiff sufficiently alleged an injury-in-fact for Article III and *Spokeo, Inc. v. Robins*⁵ purposes by alleging a violation of his right to privacy.


3. See *McCollough v. Smarte Carte, Inc.*, 2016 U.S. Dist. LEXIS 100404 (N.D. Ill. Aug. 1, 2016); *Vigil v. Take-Two Interactive Software, Inc.*, 235 F. Supp. 3d 499 (S.D.N.Y. 2017). 4. *Monroy v. Shutterfly, Inc.*, 2017 U.S. Dist. LEXIS 149604 (N.D. Ill. Sept. 15, 2017). 5. 136 S. Ct. 1540 (2016).

WHILE WE WILL ALMOST CERTAINLY SEE A LARGE NUMBER OF SUITS CONTINUE ALONG THE TECHNOLOGY LINES OF THE EXISTING SUITS . . . WE ARE ALSO LIKELY TO SEE CLASS CASES BEING FILED AGAINST COMPANIES USING MORE SOPHISTICATED METHODS OF BIOMETRIC CAPTURE FOR OTHER MARKETING AND SECURITY PURPOSES.

Related Content

For an overview of state laws governing notification of data breaches, including those involving biometric data, see

CHART – KEY REQUIREMENTS OF STATE DATA BREACH LAWS: PROTECTED PERSONAL INFORMATION, NOTICE TO STATE AGENCIES AND/OR CREDIT REPORTING AGENCIES, AND SUBSTITUTE NOTICE

 **RESEARCH PATH:** *Intellectual Property & Technology > Privacy & Data Security > Data Breaches > Practice Notes*

For information on drafting a privacy policy, see

DRAFTING PRIVACY POLICIES

 **RESEARCH PATH:** *Intellectual Property & Technology > Privacy & Data Security > Privacy Policies > Practice Notes*

For a discussion on the key privacy issues that application developers should take into account when designing, developing, and marketing mobile apps, see

MOBILE APP PRIVACY CONSIDERATIONS

 **RESEARCH PATH:** *Intellectual Property & Technology > Privacy & Data Security > Privacy & Data Security Compliance > Practice Notes*

For a sample privacy disclosure to be used by mobile application developers, see

PRIVACY DISCLOSURE FOR MOBILE APPLICATIONS (SHORT FORM)

 **RESEARCH PATH:** *Intellectual Property & Technology > Privacy & Data Security > Privacy Policies > Forms*

Google, Inc.

In February 2017, another Illinois federal judge denied a motion to dismiss two complaints brought by individuals who alleged Google captured biometric data from facial scans of images taken with Google Droid devices in Illinois without the plaintiffs' consent in violation of BIPA.⁶ And in May 2016, a California federal judge denied a motion to dismiss a putative class action of Illinois residents who alleged Facebook scanned and captured their biometric data from images uploaded to Facebook without their consent in violation of BIPA.⁷ Like Shutterfly, both Google and Facebook argued that BIPA does not apply to scans of photographs, and Google also argued that the application of BIPA to the plaintiff's claims would give the statute extraterritorial effect and violate the Dormant Commerce Clause. The courts in both cases rejected these arguments and permitted the cases to move forward.

Which Technologies are Next?

While we will almost certainly see a large number of suits continue along the technology lines of the existing litigation (in particular for fingerprint scans used to control access or monitor timekeepers and cashiers), we are also likely to see class cases being filed against companies using more sophisticated methods of biometric capture for other marketing and security purposes. For example:

- Brick-and-mortar operators that use facial recognition to identify and track the movement of shoppers in their stores
- Retailers that use facial recognition to identify returning shoplifters
- App providers that use fingerprint or facial recognition for secured or streamlined access to their app

6. *Rivera v. Google, Inc.*, 238 F. Supp. 3d 1088 (N.D. Ill. 2017). 7. *In re Facebook Biometric Info. Privacy Litig.*, 185 F. Supp. 3d 1155 (N.D. Cal. 2016).

Which Jurisdictions are Next?

Although Illinois is the only state that currently permits a private right of action for violations of its biometric data privacy laws, other states have similar laws pending, including:

- **Michigan, 2017 Bill Text MI H.B. 5019.** This bill provides a private cause of action with statutory damages of \$1,000 for negligent violations and \$5,000 for intentional or reckless violations.
- **New Hampshire, 2017 Bill Text NH H.B. 523.** This bill provides a private cause of action with statutory damages of \$1,000 for negligent violations and \$5,000 for reckless or intentional violations.
- **Alaska, 2017 Bill Text AK H.B. 72.** This bill provides a private cause of action only for intentional violations of the statute. The statutory damages are \$1,000 for intentional violations and \$5,000 for intentional violations that result in profit or monetary gain.
- **Montana, 2017 Bill Text MT H.B. 518.** This bill provides a private cause of action with statutory damages of \$1,000 for purposeful or knowing violations and \$5,000 for violations that result in profit or monetary gain. (Note, however, that no action has been taken on the bill since April 28, 2017, and it may have died in Standing Committee.)

Although the Texas and Washington laws mentioned above do not provide private causes of action, they also need to be considered when establishing policies and procedures for

complying with biometric data privacy laws. If, for example, a private Illinois action was to succeed at trial or result in a large settlement, the defendant might be a soft target for a follow-on action pursued by a state attorney general.

Conclusion

It is crucial that retailers ensure that their policies and procedures regarding the capture, retention, and disposal of biometric data comply with the various notice and consent requirements outlined in BIPA as well as the Texas and Washington laws. Retailers should also track the development of similar proposed legislation in other states to ensure the continued lawfulness of such policies and procedures. ■

Torsten M. Kracht (tkracht@hunton.com) is a partner at Hunton & Williams LLP representing clients from the United States and abroad in complex commercial litigation and arbitration. Michael J. Mueller (mmueller@hunton.com) is a partner at the firm handling class actions and other complex cases. Lisa J. Sotto (lsotto@hunton.com) is the managing partner of the firm's New York office and chair of its global privacy and cybersecurity practice. Daniella Sterns (dsterns@hunton.com) is a litigation associate at the firm.



RESEARCH PATH: [Intellectual Property & Technology](#)
[> Privacy & Data Security](#) > [Privacy & Data Security](#)
[Compliance > Articles](#)

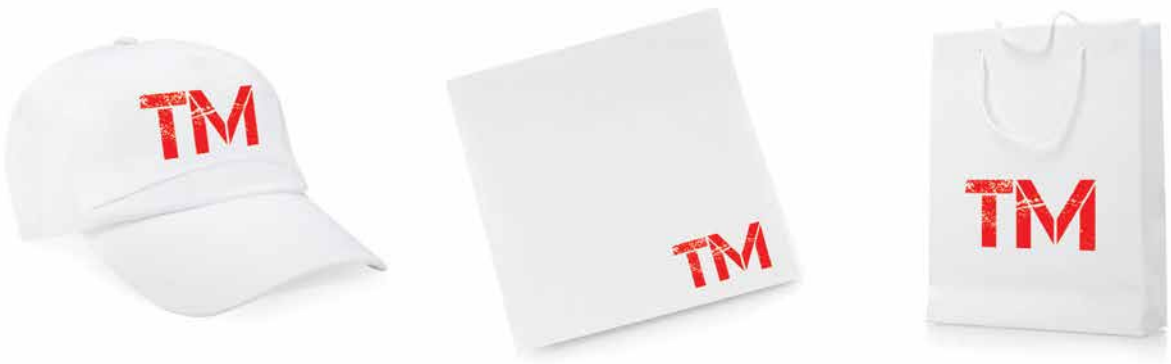
This article was first published in the January 2018 issue of Pratt's Privacy & Cybersecurity Law Report. All rights reserved. Visit the website to subscribe, <https://store.lexisnexis.com/>



Janet Marvel PATTISHALL, MCAULIFFE, NEWBURY, HILLIARD & GERALDSON LLP

Preparing for Random Trademark Registration Audits

The U.S. Patent and Trademark Office (USPTO) is commencing random audits of trademark registrations in which Declarations of Use have been filed to verify that the registered mark is in use on all of the goods and services in the registration. All applicants and registrants, particularly those foreign companies that have filed under the Madrid Protocol or a corresponding home country registration, need to be prepared. If you do not properly respond to the audit request, you could lose your registration, in part or in whole.



BETWEEN THE FIFTH AND SIXTH YEAR AFTER A MARK IS registered, the registrant must file a Declaration of Use attesting, under oath, that the registered mark is in use in U.S. commerce on all the goods or services in the registration. The registrant must also submit a specimen label, product photo, or the like, showing the use of the mark on one product or service in each class in the registration. The registrant must delete any goods and services for which the registered mark is no longer in use.

The USPTO piloted an audit of Declarations of Use a few years ago. It randomly selected 500 registrations for

which registrants had submitted Declarations of Use and accompanying specimens of use. In those cases, the USPTO requested that the registrants submit additional specimens for certain goods and services in the registrations. The USPTO found that in over half of the cases selected, the registrants did not or could not show the additional proof of use. Based on this pilot program, the USPTO determined that audits would help maintain the accuracy and integrity of the federal trademark register by removing deadwood (i.e., abandoned) goods and services.






Related Content


For an overview of the trademark application process, see

> [FACTORS TO CONSIDER BEFORE FILING A TRADEMARK APPLICATION](#)

 **RESEARCH PATH:** [Intellectual Property & Technology > Trademarks > Trademark Registration > Practice Notes](#)


For a discussion of the Madrid Protocol, see

> [MAINTAINING & RENEWING MADRID PROTOCOL REGISTRATIONS](#)

 **RESEARCH PATH:** [Intellectual Property & Technology > Trademarks > International Trademark Considerations > Practice Notes](#)


For more information on Declarations of Use, see

> [MAINTAINING & RENEWING U.S. TRADEMARK REGISTRATIONS](#)

 **RESEARCH PATH:** [Intellectual Property & Technology > Trademarks > Trademark Registration > Practice Notes](#)

For guidance on conducting a trademark audit, either internally or by outside counsel, see

> [TRADEMARK AUDITS](#)

 **RESEARCH PATH:** [Intellectual Property & Technology > Trademarks > Trademark Counseling & Transactions > Practice Notes](#)

The pilot audit is now a permanent program. The USPTO will randomly audit Declarations of Use for:

- Single-class registrations with four or more goods or services in the class, for example:
 - Umbrellas, duffels, wallets, backpacks, briefcases, suitcases, and handbags in Class 18
- Multi-class registrations in which at least two classes have two or more goods or services, for example:
 - Notebooks, stickers, paper napkins, erasers, and pens in Class 16
 - Umbrellas in Class 18
 - Mugs, cups, and bottle openers in Class 21
 - T-shirts in Class 25

For each audited registration, the USPTO will issue an Office Action after examining the registrant's Declaration of Use. The Office Action will require the registrant to submit specimens of use for two additional products or services in each class, as appropriate.

The registrant must then either submit additional specimens of use or delete any audited goods or services for which it is not using the registered mark in U.S. commerce. If the registrant deletes any goods or services, the USPTO will, as appropriate, issue another Office Action requiring specimens of use for everything else in the registration. The registrant has six months to respond to each Office Action. If the registrant does not respond, the registration will be cancelled. If the registrant does respond, but does not provide proper specimens of use for some of the goods/services, those goods/services will be deleted from the registration.


Applicants and registrants should do two things to make sure they are ready for audits:

When you file a Declaration of Use, gather evidence for every product or service in your application. You now need to be even more careful when filing a Declaration of Use. Check for use and assemble specimens showing the mark as used on each item in your registration before you file the Declaration of Use. Then before you file, delete the goods for which you are not using the registered mark in the United States. That way, you will be prepared to defend your registration if it is selected for a random audit.

Make sure you have a bona fide intent to use your mark on all of the goods or services in your application. You must have a bona fide intention to use your mark in order to get a valid registration. That is true even if the U.S. application is based on a home country registration or the Madrid Protocol. You should keep documentary evidence of your plans and steps to use the mark for the specified products in the United States, such as business plans, marketing plans, or correspondence with potential distributors or manufacturers.

Foreign companies' trademark applications are often drafted to cover long lists of goods and services, as this approach is dictated by local practice outside the United States. Sometimes, the applicant does not have a bona fide intent to use the mark on everything in the application, or at least a provable bona fide intent. For example, a recent application included

wimples, mustache wax, agates, unwrought silver, albs, ascots, chasubles, animal harnesses, wet suits for waterskiing, and horse blinkers. Such unusual and diverse product lines invite questions regarding bona fide intent to use.

Madrid and treaty-based applications and resulting registrations, with long lists of goods, could be a driving factor for the audit program. However, even if you are a domestic applicant, you should take care to include only those goods you actually intend to use the registered mark on, as of the time of filing, in your application, and you should document your intent. 

*Janet Marvel is a partner at Pattishall, McAuliffe, Newbury, Hilliard & Geraldson LLP. She protects brands, copyrighted works, and domain names throughout the world. As part of her practice, Janet represents plaintiffs and defendants in a wide variety of disputes involving trademark, copyright, rights of publicity, breach of contract, unfair competition, and false advertising. She has successfully tried cases and litigated around the country in state and federal courts and before the USPTO. Janet writes the comprehensive treatise **Hilliard, Welch & Marvel, Trademarks and Unfair Competition** (8th ed., 2017, Lexis Nexis); online edition (2017, Lexis Nexis).*

 **RESEARCH PATH:** [Intellectual Property & Technology > Trademarks > Trademark Counseling & Transactions > Articles](#)





Ellen MacDonald Farrell and Rachel P. Raphael
CROWELL & MORING

INSURANCE COVERAGE ISSUES CREATED BY THE INTERNET



Today, billions of different devices are connected to the internet, and the internet-capability of everyday objects is expected to grow exponentially in the years to come. The Internet of Things (IoT) refers to the network of these devices that collect and exchange data. Connected devices may include everything from automobiles to implantable medical devices to home appliances. The large-scale use of these devices is already revolutionizing many aspects of our daily lives by increasing the availability of information and changing the ways that business and consumers interact. But at the same time, it is creating a host of new cyber-related risks, as a wealth of new information may be open for attack. This article focuses on the complex insurance issues raised by IoT devices.

CYBER-RELATED BREACHES APPEAR NOW TO BE AN everyday occurrence. And as more devices become part of the IoT, the more consumers and businesses are put at risk. Personal and confidential data is more susceptible to hackers; manipulations of wireless medical devices risk bodily injury and even death; and cyber incidents involving (for example) power grids, connected planes, trains, and automobiles could have devastating impacts.

Controlled demonstrations and data breach incidents have shown that there are still improvements to be made in the techniques used to secure IoT devices. The exposure of vulnerabilities has led to lawsuits against companies involved in the production, sale, distribution, and marketing of internet-connected products. When facing potential liability, companies commonly turn to their insurance policies for coverage. But with complicated risks come complicated insurance issues. The tangible and intangible nature of data breaches involving IoT products raises interesting issues under both standalone cyber insurance and more traditional liability policies.

Background on the IoT

IoT¹ is generally understood to refer to a decentralized network of physical objects that are connected to the Internet and enable communication between humans, computers, objects, applications, and devices.² To put it simply, “[t]he IoT is what we get when we connect Things, which are not operated by humans, to the Internet.”³ “Things” here may include any object for which remote communication, data collection, or control is useful; for example, “streetlights, thermostats, electric meters, fitness trackers, factory equipment, automobiles, unmanned aircraft systems (UASs or drones), or even cows or sheep in a field.”⁴ An object becomes

part of the IoT once it has two features: (1) an Internet Protocol (IP) address, which allows the object to be uniquely identified; and (2) internet connectivity, which allows the object to send and receive information from computers and other smart objects in the IoT.⁵

The number of connected objects in the IoT is growing at a rapid rate. The network has expanded significantly in the last 20 years due to the “explosive growth in mobile devices and applications and the broad availability of wireless connectivity.”⁶ In 2003, approximately 500 million devices were connected to the internet.⁷ Today, there are more than 6.4 billion such devices, with approximately 5.5 million more connecting to the internet each day.⁸ By 2020, the number of devices in the IoT is predicted to exceed 20 billion⁹—possibly reaching as many as 40 to 50 billion.¹⁰ Global spending on IoT products is forecasted to reach \$737 billion by 2016 and grow at a compound annual rate of 15.5% from 2015–2020 to \$1.29 trillion.¹¹ By 2020, consumer IoT products are expected to be the third largest segment of market purchases,¹² with each person in the world owning an average of more than six connected devices.¹³

Risks Associated with the IoT

Privacy

Within the IoT, billions of sensors around the world are constantly acquiring information about their surroundings, and new ways of capturing and using personal information continue to emerge.¹⁴ One of the government’s top concerns regarding growth of the IoT is the unpermitted access to and misuse of personal information and consumer data.¹⁵ This could occur in a variety of situations. For example, a company could store for later use data collected from the IoT in ways its consumers did not authorize.¹⁶ Or, an employer could

1. The term “Internet of Things” was coined as early as 1999 by Kevin Ashton, a British technology pioneer who was then working at Procter & Gamble as an assistant brand manager. See Shawn DuBravac & Carlo Ratti, *The Internet of Things: Evolution or Revolution?* 6 (2015). 2. Nasrine Olson, *The Internet of Things*, 18 NEW MEDIA & Soc’y 680 (2016) (book review); National Sec. Telecomms. Advisory Comm., *NSTAC Report to the President on the Internet of Things* (2014). 3. Peter Waher, *Learning Internet of Things 2* (2015). 4. Eric A. Fischer, Cong. Research Serv., R44227, *The Internet of Things: Frequently Asked Questions 2* (2015). 5. *Id.* at 3. 6. DuBravac & Ratti, *supra* note 1, at 7. 7. *Id.* 8. H. Michael O’Brien, *The Internet of Things and its Future Impact on Product Liability* (2015). 9. *Id.* 10. DuBravac & Ratti, *supra* note 1, at 2. 11. *Internet of Things Spending to Reach US\$1.29 trillion by 2020, Insurance Industry to See Fast Spending Growth*, CANADIAN UNDERWRITER (Jan. 5, 2017), <http://www.canadianunderwriter.ca/insurance/internet-things-spending-reach-us1-29-trillion-2020-insurance-industry-see-fast-spending-growth-report-1004106299/>. 12. *Id.* 13. Lea Toms, *Beware! Data and Identity Theft in the IoT*, GLOBALSIGN BLOG (Mar. 22, 2016), <https://www.globalsign.com/en/blog/identity-theft-in-the-iot/>. 14. DuBravac & Ratti, *supra* note 1, at 15. 15. Mohana Ravindranath, *Who’s in Charge of Regulating the Internet of Things?*, NEXTGOV (Sept. 1, 2016), <http://www.nextgov.com/emerging-tech/2016/09/internet-things-regulating-charge/131208/>. 16. *Id.*



use sensors to monitor an employee's behavior after work hours without the employee's permission.¹⁷

Another privacy concern is the ease with which hackers may conduct identity theft. "General data available on the internet, combined with social media information, plus data from smart watches, fitness trackers and if available smart meters, smart fridges and many more" provide hackers with "a great all-round idea" of individual identities.¹⁸ Fitness watches and smartphones contain some of the most private information, including a person's name, address, date of birth, credit card information, and health information.¹⁹ Smartphones also contain unprotected access to a person's email, business, and social media accounts, and online banking information.²⁰

Cybersecurity

As the number of smart objects in the IoT grows, so does the potential risk of cyber-attacks and the costs associated with such incidents. Cybersecurity is designed to protect "information systems, their components and contents, and the networks that connect them from intrusions or attacks involving theft, disruption, damage

or other unauthorized or wrongful actions."²¹ Today, cyber-attacks pose a significant threat to businesses, costing approximately \$400 billion every year.²² Such attacks do not just result in the theft of data. Sometimes data breaches—especially those involving IoT products—can cause bodily injury and property damage.²³

For example, in 2008, hackers accessed a Turkish pipeline through surveillance camera software and caused an explosion by super-pressurizing the oil in the pipeline after shutting down its alarms.²⁴ The next year, a former employee was responsible for a computer intrusion of a large power company in Texas that crippled the company's energy forecast system and caused the company to incur more than \$26,000 in damages.²⁵

In 2014, the German Federal Office of Information Security announced that hackers had gained access to a German steel factory's production networks and caused system components to fail by tampering with the controls of its blast furnace.²⁶ Then in 2015, hackers obtained control of a power grid in western Ukraine, opening up circuit breakers and knocking out power stations.²⁷

ANOTHER PRIVACY CONCERN IS THE EASE WITH WHICH HACKERS MAY CONDUCT IDENTITY THEFT.

More recently, in January 2017, hackers infiltrated an Austrian hotel's electronic key system, locking guests out of their rooms and forcing the hotel to give in to the hackers' ransom demand.²⁸ Finally, just eight days before President Trump's inauguration, hackers tampered with 70% of storage devices that record data from police surveillance cameras in Washington, D.C., "forcing major citywide reinstallation efforts."²⁹

Safety

Of the risks inherent in an expansive IoT system, the most significant is the risk to our health and safety. For example, in 2014, the Federal Bureau of Investigation (FBI) warned hospitals to discontinue use of a particular line of infusion pumps produced by Hospira due to security flaws that could allow a user to remotely change medication doses.³⁰ And in January 2017, the Food and Drug Administration (FDA) confirmed that St. Jude Medical's implantable cardiac devices had vulnerabilities that could allow a hacker to access them and deplete their batteries and/or administer incorrect pacing or shocks.³¹

The possibility of such intrusions does not come as a surprise. In 2011, a former security guard hacked a hospital's computer network and took control of the HVAC system, putting vulnerable patients and treatments (such as temperature-sensitive drugs and supplies) at risk.³² A few years later, as part of a demonstration at the University of South Alabama, students hacked a pacemaker and showed that they could speed up and slow down heart rates.³³

Hackers can also endanger our safety by targeting different modes of transportation. For example, in 2008, a teenage boy hacked into a Polish train system, causing a train derailment and injuring at least 12 people.³⁴ Additionally, in April 2015, the U.S. Government Accountability Office (GAO) published a report

addressing cybersecurity issues with commercial aircraft.³⁵ In its report, the GAO noted that the increasing interconnectedness of modern aircraft creates the possibility of unauthorized access to aircraft avionics systems.³⁶ Similarly, "[w]hile there have been no known cyber-attacks against vehicles . . . most experts believe 'real-world attacks with safety implications could occur in the near future, particularly as automakers begin deploying autonomous (i.e., self-driving) vehicles and connected vehicle technologies.'"³⁷ The possibility of such intrusions was confirmed in mid-2015 when two individuals conducting a white hat hacking experiment were able to manipulate systems and then disable a sport utility vehicle speeding on a busy highway 10 miles away.³⁸

Insurance Coverage Issues Raised by the IoT

Cases Dealing with the Definition of Property Damage

Courts have long grappled with whether cyber-related losses are covered under first- and third-party insurance policies. In early cases, courts addressed coverage for losses to data or functionality of electronic devices that resulted from causes such as faulty equipment, power outages, or malware. Today, courts all over the country continue to address these issues.

Generally speaking, policyholders have sought coverage for the loss of use of data or functionality of electronic devices on the ground that such losses involved property damage, which has been typically defined as including injury to or the loss of use of tangible property. In contrast, insurers have argued that such losses were not covered because those losses did not involve injury to or the loss of use of such property. Although courts have reached different conclusions on these issues, their reasoning may be instructive as courts begin to deal more specifically with coverage for tangible losses relating to IoT devices.

At one end of the spectrum is *Am. Guar. & Liab. Ins. Co. v. Ingram Micro, Inc.*³⁹ The policyholder in that case, Ingram Micro, distributed "microcomputer products" and used a network (Impulse) to track orders and keep information on its customers and products.⁴⁰ Due to a power outage, programming information that had been stored on Ingram Micro's mainframe computers was lost and had to be reprogrammed, and Ingram Micro's data center was disconnected from the Impulse network for eight hours until a system switch was fixed.⁴¹ Ingram Micro sought coverage for its resulting business and service interruption losses under an all risks policy that Ingram Micro had procured from American Guarantee and Liability Insurance


17. DuBravac & Ratti, *supra* note 1, at 13. 18. Toms, *supra* note 16. 19. *Id.* 20. *Id.* 21. Cong. Research Serv., *supra* note 4, at 14. 22. DuBravac & Ratti, *supra* note 1, at 16. 23. Cong. Research Serv., *supra* note 4, at 14. 24. Jordan Robertson & Michael Riley, *Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar*, BLOOMBERG TECH. (Dec. 10, 2014, 5:00 AM), <https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar>. 25. Kevin Poulsen, *Ex-Employee Fingering in Texas Power Company Hack*, WIRED (May 29, 2009, 4:36 PM), <https://www.wired.com/2009/05/efh/>. 26. *Hack Attack Causes 'Massive Damage' at Steel Works*, BBC (Dec. 22, 2014), <http://www.bbc.com/news/technology-30575104>; Andrew Roth, *Not Just the DNC: Five More Hacks the West Has Tied To Russia*, WASH. POST (June 15, 2016), https://www.washingtonpost.com/news/worldviews/wp/2016/06/15/not-just-the-dnc-five-more-hacks-the-west-has-tied-to-russia/?utm_term=.d0fd4b683b32. 27. Roth, *supra* note 26; Kim Zetter, *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*, WIRED (Mar. 3, 2016, 7:00 AM), <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>.

28. Dan Bilefsky, *Hackers Use New Tactic at Austrian Hotel: Locking the Doors*, N.Y. TIMES, Jan. 30, 2017, https://www.nytimes.com/2017/01/30/world/europe/hotel-austria-bitcoin-ransom.html?_r=0. 29. Clarence Williams, *Hackers Hit D.C. Police Closed-Circuit Camera Network, City Officials Disclose*, WASH. POST, Jan. 27, 2017, https://www.washingtonpost.com/local/public-safety/hackers-hit-dc-police-closed-circuit-camera-network-city-officials-disclose/2017/01/27/d285a4a4-e4f5-11e6-ba11-63c4b4fb5a63_story.html?utm_term=.7ccd6a0e1b23. 30. Jessica Conditt, *FDA Tells Hospitals to Ditch IV Pumps That Can be Hacked Remotely*, ENGADGET (July 31, 2015), <https://www.engadget.com/2015/07/31/fda-security-warning-hackers/>. 31. Press Release, FDA, *Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication* (Jan. 9, 2017). 32. Press Release, FBI, *Former Security Guard Who Hacked Into Hospital's Computer System Sentenced to 110 Months in Federal Prison* (Mar. 18, 2011). 33. Jason Koebler, *Hackers Killed a Simulated Human by Turning Off Its Pacemaker*, MOTHERBOARD (Sept. 7, 2015), https://motherboard.vice.com/en_us/article/hackers-killed-a-simulated-human-by-turning-off-its-pacemaker. 34. Graeme Baker, *Schoolboy Hacks Into City's Tram System*, TELEGRAPH (Jan. 11, 2008), <http://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html>. 35. U.S. Gov't Accountability Office, GAO-15-370, *Air Traffic Control—FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen* (2015). 36. *Id.* 37. See Paul Merriam, *House Smart Car Caucus Revs Up Vehicle Cybersecurity Issue*, CONGRESSIONAL QUARTERLY ROLL CALL (April 28, 2016). 38. Michael E. Miller, *'Car Hacking' Just Got Real: In Experiment, Hackers Disable SUV on Busy Highway*, WASH. POST, July 22, 2015, https://www.washingtonpost.com/news/morning-mix/wp/2015/07/22/car-hacking-just-got-real-hackers-disable-suv-on-busy-highway/?utm_term=.7a30e09871f9. 39. 2000 U.S. Dist. LEXIS 7299 (D. Ariz. Apr. 18, 2000). 40. *Id.* at *2-*3. 41. *Id.* at *3-*5.

Related Content

For more information on the coverage of cyber claims by commercial general liability insurance policies, see

> [INTELLECTUAL PROPERTY INFRINGEMENT AND CYBER CLAIMS UNDER A COMMERCIAL GENERAL LIABILITY POLICY](#)

 **RESEARCH PATH:** [Commercial Transactions](#) > [Insurance](#) > [Understanding Business Insurance](#) > [Practice Notes](#)

For a checklist of the items that are important in determining whether to purchase a particular cybersecurity insurance policy, see

> [CYBER-SECURITY INSURANCE POLICIES REVIEW CHECKLIST](#)

 **RESEARCH PATH:** [Commercial Transactions](#) > [Insurance](#) > [Insurance Policies](#) > [Checklists](#)


For an overview of the coverage and exclusions in commercial general liability insurance, see

> [COMMERCIAL GENERAL LIABILITY INSURANCE](#)

 **RESEARCH PATH:** [Commercial Transactions](#) > [Insurance](#) > [Insurance Policies](#) > [Practice Notes](#)

For a detailed discussion on the benefits and risks surrounding the Internet of Things, including privacy laws and data security regulation, see

> [THE INTERNET OF THINGS: KEY LEGAL ISSUES](#)

 **RESEARCH PATH:** [Commercial Transactions](#) > [E-Commerce](#) > [Internet Business & New Media](#) > [Practice Notes](#)

For guidance on how an organization should plan for and manage a data breach, see

> [PLANNING FOR & MANAGING A DATA BREACH](#)

 **RESEARCH PATH:** [Commercial Transactions](#) > [E-Commerce](#) > [Privacy & Data Security on the Internet](#) > [Practice Notes](#)

Company (AGLIC).⁴² This policy provided coverage for “[a]ll Risks of direct physical loss or damage from any cause, howsoever or wheresoever occurring”⁴³

AGLIC argued that the all risks policy did not cover Ingram Micro’s business and service interruption losses because Ingram Micro’s computer systems were not physically damaged, since the “power outage did not adversely affect the equipment’s inherent ability to accept and process data and configuration settings when they were subsequently reentered into the computer system.”⁴⁴ By contrast, Ingram Micro argued that the computer systems had been physically damaged because they had lost their functionality.⁴⁵

The U.S. District Court for the District of Arizona sided with Ingram Micro, concluding that loss of programming information and customer configurations did constitute physical damage to tangible property. In so doing, the court explained:

At a time when computer technology dominates our professional as well as personal lives, the Court must side with . . . [the] broader definition of “physical damage.” The Court finds that “physical damage” is not restricted to the physical destruction or harm of computer circuitry but includes loss of access, loss of use, and loss of functionality.⁴⁶

Similarly, in *Eyeblaster, Inc. v. Fed. Ins. Co.*, the U.S. Court of Appeals for the Eighth Circuit held that allegations in an underlying complaint, that a computer was damaged due to malware, alleged physical damage under a general liability policy.⁴⁷ Specifically, the plaintiff (Sefton) alleged in an underlying complaint that Eyeblaster’s online advertising malware had caused Sefton’s computer to crash, causing Sefton to lose data on a tax return that he had been preparing. Sefton further alleged that even after his computer was repaired, the computer continued to run slowly and freeze up.⁴⁸

Eyeblaster tendered defense of Sefton’s complaint to its general liability carrier, Federal Insurance Company, but Federal Insurance denied the claim (*inter alia*) on the ground that the underlying complaint did not allege property damage caused by an occurrence.⁴⁹ The policy at issue defined “property damage” as “physical injury to tangible property, including resulting loss of use of that property . . . or loss of use of tangible property that is not physically injured.”⁵⁰

Even though this definition excluded “any software, data or other information that is in electronic form,”⁵¹ the court held that Sefton’s complaint alleged property damage, since Sefton had alleged that his computer itself was damaged by Eyeblaster’s malware.⁵²



Am. Online, Inc. v. St. Paul Mercury Ins. Co. represents the other end of the spectrum in these cases.⁵³ There, multiple class action suits had been filed against America Online (AOL), alleging that AOL’s access software Version 5.0 caused plaintiffs’ operating systems to crash and their computers to lose stored data.

AOL tendered the defense of those suits to St. Paul Mercury Insurance Company, which had issued a commercial general liability (CGL) insurance policy to AOL.⁵⁴ The policy covered property damage, which was defined as

physical damage to tangible property of others, including all resulting loss of use of that property; or loss of use of tangible property of others that isn’t physically damaged.⁵⁵

St. Paul denied AOL’s claim on the ground that the underlying complaints did “not allege damage to ‘tangible’ property” under the CGL policy.⁵⁶

In the resulting coverage litigation, the U.S. District Court for the Eastern District of Virginia, and then the U.S. Court of Appeals for the Fourth Circuit, agreed with St. Paul. In so doing, the Fourth Circuit analogized the loss of use of software on a computer to a lock combination and the lock itself, noting that “when the combination to a combination lock is forgotten or changed, the lock becomes useless, but the lock is not physically damaged. With the retrieval or resetting of the combination—the idea—the lock can be used again.”⁵⁷ With this in mind, the court then explained that although AOL’s CGL policy “cover[ed] any damage that may have been caused to circuits, switches, drives, and any other physical components of the computer,” it did not cover “the loss of instructions to configure the switches or the loss of data stored magnetically.”⁵⁸ Because “[t]hese instructions, data and information are abstract and intangible,” the court held that damage to them “is not physical damage to tangible property.”⁵⁹

42. *Id.* at *3. 43. *Id.* 44. *Id.* at *5–*6. 45. *Id.* at *6. 46. *Id.* See also *Centennial Ins. Co. v. Applied Health Care Sys.*, 710 F.2d 1288, 1291 (7th Cir. 1983) (underlying complaint that alleged faulty controllers caused the loss of electronically stored data “clearly raise[d] the spectre that liability for property damage [might] ensue”); *Computer Corner, Inc. v. Fireman’s Fund Ins. Co.*, 46 P.3d 1264, 1266 (lower court had concluded data lost when policyholder reformatted a hard drive constituted tangible property, and the parties did not appeal that conclusion); *Retail Systems, Inc. v. CNA Ins. Cos.*, 469 N.W.2d 735, 737 (Minn. Ct. App. 1991) (data on a computer tape constituted tangible property). 47. 613 F.3d 797 (8th Cir. 2010). 48. *Id.* at 800. 49. *Id.* Eyeblaster had also purchased an Information and Network Technology Errors or Omissions policy from Federal and tendered the defense of Sefton’s claims under that policy as well. Federal also denied coverage under the Tech E&O policy, which covered “financial injury caused by a wrongful act that results in the failure of Eyeblaster’s product to perform its intended function or to serve its intended purpose,” because Eyeblaster’s conduct was allegedly intentionally wrongful. *Id.* at 803–84. However, the court concluded that Federal had not met its burden of proof with respect to that argument. *Id.* at 804–85. 50. *Id.* at 801. 51. *Id.* 52. *Id.* at 802.

53. 347 F.3d 89 (4th Cir. 2003). 54. *Id.* at 91–92. 55. *Id.* at 94. 56. *Id.* 57. *Id.* at 96. 58. *Id.* 59. *Id.*

UNLIKE THE RECENT DECISIONS CONSIDERING WHETHER BREACH-RELATED LOSSES
CONSTITUTE PROPERTY DAMAGE, COURTS HAVE REACHED DIFFERENT RESULTS
WHEN DECIDING WHETHER SUCH LOSSES QUALIFY AS ADVERTISING INJURY.

Other courts have followed *America Online* and similarly concluded that damage to electronic data is not covered property damage.⁶⁰

Coverage for Damages Resulting from the Unauthorized Access to Data under “Traditional” Liability Policies

Policyholders’ Approaches to Coverage

Coverage disputes relating to data breaches may also be instructive as courts begin to deal with IoT-related coverage disputes. Policyholders seeking coverage for such breaches generally argue that their resulting losses constitute property damage under Coverage Part A of their general liability policies or advertising injury under Coverage Part B of those policies.

Data Breaches as Covered Property Damage

As a general matter, courts that have considered whether breach-related losses constitute “damage to tangible property,” as required under CGL policies, have determined that they do not.

For example, in 2012, the U.S. District Court for the Western District of Wisconsin addressed whether electronic funds in an online bank account were tangible property under a commercial excess liability and “Bis-Pak” policy.⁶¹ In *Carlton*, the policyholder, DelaGet, had been hired by a restaurant group to manage its finances.⁶² The restaurant group’s accounts were allegedly exposed to a virus on DelaGet’s computer, and several hundred thousand dollars were stolen from the restaurant group’s bank account.⁶³

DelaGet argued that the term tangible property was reasonably susceptible to more than one meaning, and therefore, should be read to include electronic bank account funds.⁶⁴ The district court disagreed.⁶⁵ It concluded that the electronic funds at issue were not covered under the third-party liability coverage form because there was no required loss of use of tangible property.⁶⁶

More recently, a federal district court in Alabama reached a similar conclusion.⁶⁷ In that case, the policyholder, Camp’s Grocery, was sued by three credit unions after a breach of its computer network.⁶⁸ In the underlying suit, the credit unions alleged that the data breach

had compromised their customers’ credit card, debit card, and check card information.⁶⁹ Camp’s Grocery sought coverage under a business owners insurance policy, and when the insurer refused to provide coverage, Camp’s Grocery filed suit.⁷⁰ Among other things, Camp’s Grocery argued that the physical credit, debit, and check cards were tangible property and that the losses suffered by the credit unions in replacing these cards was “covered property damage.”⁷¹ Rejecting Camp’s Grocery’s argument, the U.S. District Court for the Northern District of Alabama concluded that the underlying claims were based on compromised intangible data contained on the cards that made the cards unusable.⁷²

Data Breaches as Advertising Injury

The term advertising injury is typically defined in CGL policies as

- a. Oral or written publication of material that slanders or libels a person or organization or disparages a person’s or organization’s goods, products or services;
- b. oral or written publication of material that violates a person’s right of privacy;
- c. misappropriation or advertising ideas or style of doing business;
- or d. infringement of copyright, title or slogan.

Unlike the recent decisions considering whether breach-related losses constitute property damage, courts have reached different results when deciding whether such losses qualify as advertising injury.

In April 2011, Sony Corporation suffered a massive data breach in its PlayStation video game online network, which led to the theft of millions of customers’ private information. Sony faced claims following the hack, and it sought coverage under its general liability policies. In *Zurich Am. Ins. Company v. Sony Corp. Of Am.*, a New York trial court was asked to decide whether the insurance companies were obligated to provide coverage for these claims.⁷³

In an oral opinion issued by Judge Jeffrey K. Oing, the court held that a publication took place when hackers breached Sony’s network even though the hackers did not actually make the stolen information public.⁷⁴ However, pursuant to the general liability

policies issued by Zurich, the publication had to be made by Sony itself.⁷⁵ Coverage could not be triggered by the actions of third parties.⁷⁶ Thus, Zurich’s policies did not cover Sony’s losses because the hackers, rather than Sony, were responsible for the publication.⁷⁷

On the other hand, in *Travelers Indem. Co. of Am. v. Portal Healthcare Solutions, L.L.C.*, the U.S. Court of Appeals for the Fourth Circuit held that the insurer was obligated to defend its policyholder in a class action lawsuit alleging that the policyholder had made private medical records available on the internet for several months.⁷⁸ In that case, confidential patient records kept by a medical records company were made available to unauthorized users.⁷⁹ The medical records company, Portal Healthcare, sought coverage under two commercial general liability policies for a class action lawsuit that had been filed against it.⁸⁰ The insurer argued that it was not obligated to provide coverage because Portal Healthcare’s conduct did not effect a publication, and no publicity occurred when Portal Healthcare posted the records online.⁸¹ The district court disagreed, concluding that making the records publicly available on the internet amounted to a publication that gave “unreasonable publicity” to and “disclose[d] information about patients’ private lives” under the commercial general liability policies even though no third party was alleged to have viewed the information and Portal Healthcare took no steps to attract public attention to the information.⁸²

On appeal, the Fourth Circuit affirmed the district court’s decision, holding that the insurer had a duty to defend Portal Healthcare in the underlying class action because the alleged conduct at least potentially constituted a publication of the patients’ confidential information.⁸³

Insurance Services Office Endorsements

Early Cyber-Related Endorsements

In response to coverage disputes under traditional policies involving the loss of ability to access data and the unauthorized access to data, the Insurance Services Office (ISO) has dealt with whether to exclude or limit coverage under traditional policies for cyber-related losses. For example, after some courts had determined that electronic data could constitute tangible property, in 2001 the ISO issued a CGL coverage form that explicitly provided that electronic data was not tangible property.⁸⁴ In 2004, the ISO then introduced an exclusion (p) in the CGL form for “Damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data.”⁸⁵ But that same year, the ISO also introduced an endorsement through which policyholders could buy back limited coverage for “‘property damage’ because of all loss

of ‘electronic data’ arising out of any one ‘occurrence.’” That same endorsement defined the term property damage for purposes of the endorsement to include the “[l]oss of, loss of use of, damage to, corruption of, inability to access, or inability to properly manipulate ‘electronic data,’ resulting from physical injury to tangible property”⁸⁶ Thus, this endorsement would apply where there has been a loss of or inability to access or manipulate electronic data only where there had otherwise been injury to tangible property.⁸⁷

ISO Endorsement CG 24 13 04 13

More recently, through endorsements that went into effect in April 2013, the ISO amended the definition of advertising injury to which Coverage Part B applies. Recall that CGL policies typically define advertising injury as follows:

- a. Oral or written publication of material that slanders or libels a person or organization or disparages a person’s or organization’s goods, products or services;
- b. oral or written publication of material that violates a person’s right of privacy;
- c. misappropriation or advertising ideas or style of doing business; or
- d. infringement of copyright, title or slogan.

Endorsement CG 24 13 04 13 removes subpart (b) of that definition—and in so doing (inasmuch as policyholders have relied on subpart (b) in seeking coverage for data breaches), this endorsement arguably defeats coverage in most cases for cyber liability claims as personal or advertising injury.

ISO Endorsement CG 21 06 05 14

Finally, the ISO endorsement CG 21 06 05 14, which went into effect in May 2014, impacts both Coverage Parts A and B by seeking further to limit recovery for cyber-related losses under traditional policies. With respect to Coverage Part A (bodily injury and property damage), the endorsement replaces exclusion (p) of CGL policies with the following:

This insurance does not apply to: . . . [d]amages arising out of: (1) Any access to or disclosure of any person’s or organization’s confidential or personal information, including . . . any other type of nonpublic information; or (2) The loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data.

Electronic data means “information, facts or programs stored as or on, created or used on, or transmitted to or from computer software.” This endorsement also provides that the exclusion applies even if “damages are claimed for notification costs, credit monitoring expenses, forensic expenses, public relations expenses or any other

60. See, e.g., *Ward General Ins. Services, Inc. v. Employers Fire Ins. Co.*, 114 Cal. App. 4th 548, 556 (2003) (the loss of a computer database was not a direct physical loss or damage to covered property under the first-party insurance policy at issue, as the court rejected the idea that “information, qua information, can be said to have a material existence, be formed out of tangible matter, or be perceptible to the sense of touch”); Recall Total Info. Mgmt, Inc. v. Fed. Ins. Co., 2012 Conn. Super. LEXIS 227, at *17 (Conn. Super. Ct. Jan. 17, 2012) (the theft or loss of use of data on tapes did not constitute damage to tangible property). 61. See *Carlton Co. v. DelaGet LLC*, 2012 U.S. Dist. LEXIS 70836 (W.D. Wis. May 21, 2012). 62. *Id.* at *3. 63. *Id.* 64. *Id.* at *14–*15. 65. *Id.* at *14. 66. *Id.* 67. See *Camp’s Grocery, Inc. v. State Farm Fire & Cas. Co.*, 2016 U.S. Dist. LEXIS 147361 (N.D. Ala. Oct. 25, 2016). 68. *Id.* at *2. 69. *Id.* 70. *Id.* at *1. 71. *Id.* at *21. 72. *Id.* 73. 2014 N.Y. Misc. LEXIS 5141 (N.Y. Sup. Ct. Feb. 21, 2014). 74. *Id.* at *70.

75. *Id.* 76. *Id.* 77. *Id.* Other courts have similarly concluded that a data breach did not amount to advertising injury under the policies at issue in those cases. See, e.g., *Santos v. Peerless Ins. Co.*, 2009 Cal. App. Unpub. LEXIS 3415 (Cal. Ct. App. Apr. 30, 2009) (breach of a company’s network did not constitute an advertising injury because Apple, plaintiff in an underlying suit, “had not alleged that Santos violated Apple’s privacy rights”). 78. 35 F. Supp. 3d 765 (E.D. Va. 2014). 79. *Id.* at 768. 80. *Id.* 81. *Id.* at 770–72. 82. *Id.* 83. 644 Fed. Appx. 245 (4th Cir. 2016). 84. ISO Policy Forms, Form Number CG 00 01 10 01. That amendment defined electronic data as “information, facts or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and applications software, hard or floppy disks, CD-ROMs, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment.” 85. ISO Policy Forms, Form Number CG 00 01 12 04. 86. ISO Policy Forms, Form Number CG 04 37 12 04 at D.17. 87. ISO Policy Forms, Form Number CG 04 37 12 04. That same year, the ISO also introduced a claims-made coverage for liability due to the loss of data, where computer hardware has not also been damaged. ISO Policy Forms, Form Number CG 00 65 12 04.

loss, cost or expense incurred by [the named insured] or others arising out of” that which is the subject of the exclusion.

Notably, there are two versions of this endorsement. Both versions have the language quoted above, but the second version also expressly excepts bodily injury from the exclusion by providing that “[u]nless Paragraph (1) above applies, this exclusion does not apply to damages because of ‘bodily injury.’” This version of the endorsement thus indicates that damages due to bodily injury that arise out of “[t]he loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data” may not be excluded from coverage, as long as the bodily injury did not arise from access to or disclosure of a person or organization’s nonpublic information. This variation of endorsement CG 24 13 04 13 will likely be front and center in future coverage disputes, where policyholders are liable for bodily injury due to the hacking or other malfunctions of IoT devices.

Finally, with respect to Coverage Part B (personal and advertising injury), CG 21 06 05 14 also states:

This insurance does not apply to: . . . “[p]ersonal and advertising injury” arising out of any access to or disclosure of any person’s or organization’s confidential or personal information. . . . [t]his exclusion applies even if damages are claimed for notification costs, credit monitoring expenses, forensic expenses, public relations expenses or any other loss, cost or expense incurred

by you or others arising out of any access to or disclosure of any person’s or organization’s confidential or personal information.

An ISO executive explained the rationale for endorsement CG 21 06 05 14 at the time that it was introduced:

At the time the ISO Commercial General Policies (CGL) were developed, certain hacking activities or data breaches were not prevalent and, therefore coverages related to the access to or disclosure of personal or confidential information and associated with such events were not necessarily contemplated under the policy.

As the exposures to data breaches increased over time standalone policies started to become available in the marketplace to provide certain coverage with respect to data breach and access to or disclosure of confidential or personal information.⁸⁸

Thus, the intent of CG 21 06 05 14 seems to be to direct policyholders to standalone policies for coverage for cyber-related claims, with the notable exception of claims for bodily injury, where policyholders have purchased coverage with that version of the endorsement.

Coverage for Data Breaches under Standalone Cyber Policies

At the same time that courts have reached mixed results (at best) as to whether coverage is available for cyber-related incidents under traditional policies, and against the backdrop of the ISO’s

TO DATE, COURTS DECIDING COVERAGE DISPUTES FOLLOWING A DATA BREACH HAVE CONSIDERED WHETHER THE LOSS OF ELECTRONIC DATA CONSTITUTES PROPERTY DAMAGE. BUT WITH IoT PRODUCTS, A CYBER-RELATED LOSS COULD FALL UNDER THE MORE TRADITIONAL DEFINITION OF COVERED PROPERTY DAMAGE.

exclusionary endorsements, the market for standalone cyber policies has grown. Unlike traditional policies, which often have standard wording, there is no standard wording for cyber-related policies. Cyber policies typically present coverages for discrete types of cyber-related losses, such as first- and third-party losses arising from data breaches, network interruption, and extortion.

Although specialized policies have gained popularity in recent years, so far there have been only a few reported court decisions regarding the scope of coverage under these policies. Although the case law is thus less well-developed, a few key cases underscore the importance of paying attention to policy terms and understanding the scope of coverage even when purchasing a specialized policy.

One of the first litigated disputes involving a stand-alone cyber insurance policy was *Columbia Cas. Co. v. Cottage Health Sys.*⁸⁹ In that case, Cottage Health suffered a data breach that released private health care information on approximately 32,500 patients that was stored on its servers.⁹⁰ Columbia Casualty had issued a standalone NetProtect360 cyber insurance policy to Cottage Health, and following the data breach, Columbia Casualty sought a declaration in the U.S. District Court for the Central District of California that it was not obligated to provide coverage for Cottage Health’s losses. More specifically, Columbia Casualty alleged that (1) the breach occurred because Cottage Health and/or its third-party vendor stored the patient information on a system that was internet-accessible and without the proper security measures, and (2) Cottage Health violated non-delegable duties under California law to maintain the security of confidential medical records and to detect and prevent data breaches on its systems.⁹¹

Another early case was *Travelers Prop. Cas. Co. of Am. v. Fed. Recovery Servs.*⁹² Federal Recovery was in the business of processing, storing, transmitting, and handling electronic data for other companies.⁹³ Federal Recovery entered into a Servicing Retail Installment Agreement with Global Fitness, pursuant to which Federal Recovery agreed to process member accounts and transfer member fees to

Global Fitness.⁹⁴ A dispute erupted between the companies, and Global Fitness sued Federal Recovery, alleging that Federal Recovery had retained possession of member data and interfered with Global Fitness’ business dealings.⁹⁵ Federal Recovery tendered defense of the suit to Travelers, which had issued a CyberFirst Technology Errors and Omissions Liability Form Policy to Federal Recovery.⁹⁶

Pursuant to the CyberFirst policy, Federal Recovery was entitled to coverage for losses caused by an “errors and omissions wrongful act,” which was defined as “any error, omission or negligent act.”⁹⁷ But in its complaint, Global Fitness alleged Federal Recovery “knowingly withheld [data from Global Fitness] and refused to turn it over until Global [Fitness] met certain demands.”⁹⁸ Thus, “[i]nstead of alleging errors, omissions, or negligence, Global [Fitness] allege[d] knowledge, willfulness, and malice.”⁹⁹ Accordingly, the U.S. District Court for the District of Utah concluded that Travelers did not have a duty to defend Federal Recovery in the Global Fitness suit.¹⁰⁰

Additionally, just last year, in *P.F. Chang’s China Bistro, Inc. v. Fed. Ins. Co.*, the U.S. District Court for the District of Arizona was asked to weigh in on the scope of coverage under a standalone cyber insurance policy.¹⁰¹ P.F. Chang’s, like many merchants, was unable to process credit card transactions itself.¹⁰² As a result, it entered into an agreement with a third party, Bank of America Merchant Services (BAMS), to facilitate the processing of credit card transactions with the banks who issue credit cards.¹⁰³ Pursuant to the agreement, P.F. Chang’s agreed to pay any fines, fees, or penalties imposed on BAMS by credit card associations, based on P.F. Chang’s acts or omissions.¹⁰⁴

In June 2014, P.F. Chang’s learned that computer hackers had obtained about 60,000 credit card numbers belonging to P.F. Chang’s customers and posted these numbers to the internet.¹⁰⁵ After the cyber incident, credit card associations imposed fees on BAMS and, in accordance with their agreement, BAMS passed along the fees to P.F. Chang’s.¹⁰⁶ P.F. Chang’s then sought coverage for cyber-related losses from Federal Insurance under a Cybersecurity

88. ISO Comments on CGL Endorsements for Data Breach Liability Exclusions, Ins. J., July 18, 2014, available at <http://www.insurancejournal.com/news/east/2014/07/18/332655.htm>.

89. No. 2:15-cv-03432 (C.D. Cal. filed May 5, 2015). 90. *Id.* at ¶¶16-91. *Id.* at ¶¶17–18. Ultimately, this case was not decided on the merits. A few months later, the U.S. district court judge dismissed the suit to allow the parties to pursue alternative dispute resolution as provided for in the NetProtect360 cyber insurance policy. 92. 103 F. Supp. 3d 1297 (D. Utah 2015). 93. *Id.* at 1298. 94. *Id.* at 1299. 95. *Id.* at 1300. 96. *Id.* at 1301. 97. *Id.* at 1302. 98. *Id.* 99. *Id.* 100. *Id.* 101. 2016 U.S. Dist. LEXIS 70749 (D. Ariz. May 31, 2016). 102. *Id.* at *3. 103. *Id.* 104. *Id.* at *4. 105. *Id.* 106. *Id.* at *6.



by Chubb Policy.¹⁰⁷ Federal Insurance reimbursed P.F. Chang's for \$1.7 million in costs incurred by P.F. Chang's as a result of the data breach, but it refused to reimburse P.F. Chang's for the fees assessed by BAMS.¹⁰⁸

P.F. Chang's filed suit against Federal Insurance, and Federal Insurance moved for summary judgment.¹⁰⁹ In support of its motion, Federal Insurance argued that the BAMS fees did not constitute a loss as it was defined under the policy and, even if it did, coverage was eliminated by two exclusions that precluded coverage for liabilities assumed by P.F. Chang's without Federal Insurance's consent.¹¹⁰ The Arizona federal district court agreed with Federal Insurance, concluding that the BAMS fees did not fall under the policy's definition of loss and, in any event, these fees fell within the policy's exclusions concerning assumed liabilities.¹¹¹

Unique Insurance Issues Implicated by the IoT

When the Unauthorized Access to Data Causes Bodily Injury or Property Damage

To date, courts deciding coverage disputes following a data breach have considered whether the loss of electronic data constitutes property damage. But with IoT products, a cyber-related loss could fall under the more traditional definition of covered property damage.

For example, the 2008 hack of a Polish train system discussed above resulted in a train derailment that injured at least 12 passengers and may very well have caused damage to the passengers' personal property and the property in the vicinity of the incident. In a situation like that one, the train company might, in the first instance, seek coverage for any third-party claims under traditional general liability policies. If those general liability policies exclude coverage based on the unauthorized access of the train's electronic systems, there might well not be coverage. As discussed above, ISO endorsement CG 21 06 05 14 excludes "[d]amages arising out of: . . . (2) [t]he loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data." This would arguably exclude property damage (and, unless the adopted endorsement contains the limited exception, bodily injury) resulting from the hack if the train derailment were considered as damage "arising out of . . . the] corruption of . . . electronic data." Having said this, policyholders like the train company might argue (especially as to policies that have not incorporated the more recent ISO endorsements, or that have adopted the variant of CG 21 06 05 14 that excepts bodily injury) that the focus should be on the resulting injury (not the cause) and that bodily injury and/or property damage emanating from the unauthorized access to data therefore should be covered.

The train company might also look to its cyber insurance policy for coverage. But unlike general liability policies, those policies tend to focus coverage for costs of more typical post-breach losses such as customer notification, credit monitoring, legal fees, and fines. By contrast, those policies typically do not provide coverage for bodily injury or property damage.

Recently, however, certain carriers have started to offer insurance policies that include broader coverage for the types of losses that might occur after a cyber incident. For example, some cyber insurance policies now cover bodily injury, property damage, business interruption, and product liability related to a data breach. Even still, cyber policies offering coverage for a wider array of damages are not as commonplace right now; most cyber insurance policies do not provide such coverage. As a result, even if a company, like the train company, had purchased traditional insurance coverage and a standalone cyber insurance policy, that company might face complex insurance-related issues when property damage and/or bodily injury occurs after a cyber-attack, as in the example just discussed.

Other Complications Raised by Connected Devices

Beyond coverage for bodily injury and property damage, the interconnectedness of a widespread number of devices presents other issues. Information stored on one IoT device is only as protected as the least secure device connected to the same network. Regardless of how secure a particular device is on its own, if it is connected to a network, the security of that device could be vulnerable due to lack of security of a completely different device connected to that network. This has the potential to compromise a policyholder's ability to seek coverage under its stand-alone cyber policy.

As mentioned above., in the case of *Columbia Cas. Co. v. Cottage Health Sys.*, Columbia Casualty sought a declaration that it was not obligated to provide coverage for its policyholder, Cottage Health, under a NetProtect360 cyber insurance policy after a data breach released tens of thousands of patient medical records stored electronically on Cottage Health's servers.¹¹² Columbia Casualty alleged, in part, that the cyber incident occurred because Cottage Health and/or its third-party vendor had stored the patient files on a system that lacked the proper security measures contrary to the representations Cottage Health made on its insurance application.¹¹³

Such representations are commonly required in cyber insurance policy applications. Where the security of one connected device depends on all other devices connected to the same network (potentially including devices outside of the policyholder's control), this could complicate a policyholder's ability to make representations



regarding the security measures in place and/or comply with a cyber insurance policy requirement to maintain certain security measures.

Conclusion

The explosion of the IoT brings many opportunities. But it also comes with a wealth of unique risks. Controlled demonstrations and actual cyber incidents have shown IoT products to be susceptible to attacks. The next wave of insurance coverage litigation may very well involve these products as manufacturers derive new and creative ways to connect everyday objects to the internet. As more disastrous losses occur with the mainstream use of these products, courts will be faced with complicated insurance coverage questions regarding the interplay between various insurance policies. As a result, it will be all the more important for insurance carriers and policyholders to pay careful attention to the specific terms of their insurance policies to make sure that the available coverage satisfies both parties' expectations. **L**

Ellen MacDonald Farrell is a senior counsel in Crowell & Moring's Washington, D.C. office and a member of the Insurance/Reinsurance Group, focusing on the litigation, arbitration, and negotiated resolutions of insurance and reinsurance disputes, as well as counseling on policy language and privacy and security issues. For more than 15 years, Ellen has represented some of the nation's

*largest insurers in high-stakes disputes involving the insurance industry. Ellen has helped insurers negotiate cost-share and buy-back agreements, and she has advised insurers on a wide range of issues including the classification and allocation of long-tail claims, number of occurrences, equitable contribution between insurers, trigger, allocation, multi-year policy issues, alleged/missing policy issues, late notice, and issues presented by Bermuda Form policies. Ellen also counsels insurers with respect to the development of policy wording and emerging insurance issues and has spoken frequently on insurance issues implicated by cyber risks. **Rachel P. Raphael** is an associate in Crowell & Moring's Washington, D.C. office and a member of the Insurance/Reinsurance Group. Rachel's practice involves litigation, arbitration, and counseling on a wide variety of insurance and reinsurance issues and includes pre-dispute advice as well as insurer/reinsurer representation in complex disputes. Rachel previously worked as a law clerk for the Office of the Assistant General Counsel for International Affairs of the U.S. Department of the Treasury and as an investment banking analyst at Houlihan Lokey.*



RESEARCH PATH : [Commercial Transactions > Insurance > Understanding Business Insurance > Articles](#)

108. *Id.* at *5–*7. 109. *Id.* at *1. 110. *Id.* at *11–*23. 111. *Id.* at *14–*15, *24–*25. 112. No. 2:15-cv-03432. 113. *Id.* at ¶¶ 17–18.

This article is presented with permission from Appleman: Current Critical Issues in Insurance Law, Copyright 2017, Matthew Bender & Company, Inc., a member of the LexisNexis Group.

REIGN MAKER

RULE NEW BUSINESS WITH
COURTLINK®

Request a demo

WWW.LEXISNEXIS.COM/REIGNMAKER
OR CALL 888.253.3901



Comparison of legal research providers, November 2016
LexisNexis and the Knowledge Burst logo are registered trademarks of RELX, Group, used under license. CourtLink is a registered trademark of Reed Elsevier Inc.
© 2017 LexisNexis. All rights reserved. BRCL2015-02 0317



Kristine Di Bacco and Doug Sharp FENWICK & WEST LLP

Start-up Seed Financing

Start-up companies use seed financings primarily to raise the capital required to build a minimum viable product and test their product-market fit. This article provides guidance to company counsel and founders on how to identify a seed investor and choose the financing method that best fits the company's needs. The article assumes that the company is a Delaware C corporation, which is the market standard for venture-backed companies.

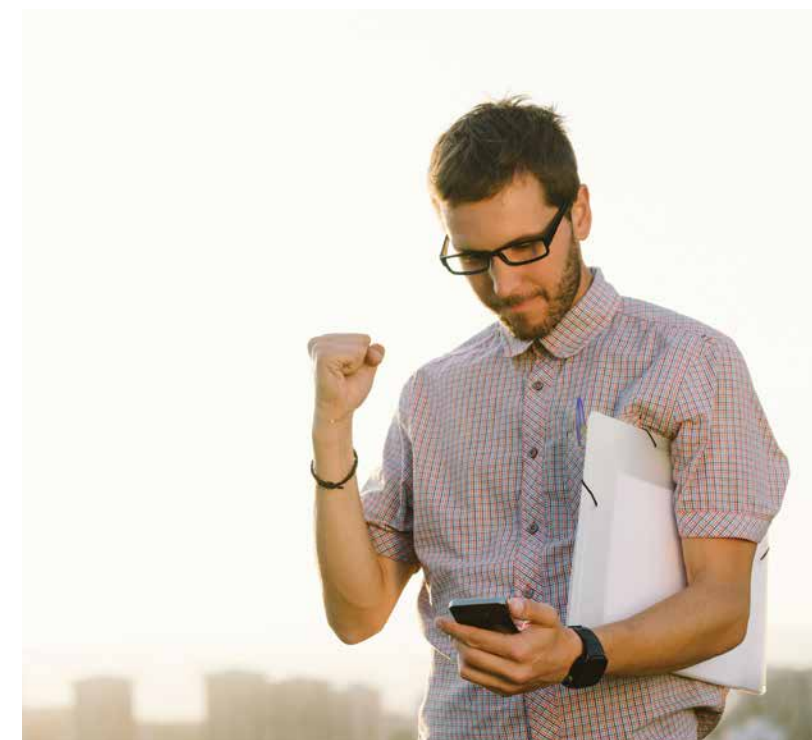
Understanding the Goals of Various Types of Investors

A typical seed financing features a founding team (and perhaps up to a handful of employees) raising between \$500,000 and \$2 million to allow for 12 to 24 months of operational capital. During this time, the founders will attempt to prove out their idea and develop the traction required for raising the next round of financing (known as a Series A financing) from a professional venture capitalist.

A seed investor's purpose is typically to test an investment hypothesis (either on a founding team, idea, or market) by providing capital to a company that will test the hypothesis. Investors at this stage will often make a large number of small investments in a variety of companies on the theory that, while many of them will fail, the few that are successful will generate significant returns for the investor. At the seed stage, investors are deciding to make their investment primarily on their assessment of the quality of the founding team and the market opportunity presented by the business model.

A few traits of founders that are seen as positive signals to investors include, but are not limited to:

- Technical/domain expertise in the planned business
- Prior successful entrepreneurial forays
- Strong introductions from people in their network
- Promising early traction
- Strong educational background (e.g., engineers from Stanford)



To decide whether to invest in a seed round, an investor will likely meet with the founding team, who will give the investor a pitch on their product/idea, market, team, and business model. Often the company's existing contacts (e.g., advisors, former co-workers, or lawyers) set up these pitch meetings (known as a warm introduction).

Types of Investors

There are a variety of typical investors in such financings:

- **Later-stage professional venture capitalists (VCs).** Many blue-chip firms (e.g., Sequoia, Andreessen Horowitz, and NEA) have separate funds for seed-stage investments. They often will invest \$200,000 to \$1 million and will be the only lead investor in a seed financing. VCs are sophisticated and often represented by outside legal counsel for seed financing transactions. They often use their seed funds as a mechanism for ensuring access to competitive Series A and Series B investments, which are the first and second rounds of financing after seed financing has been provided.
- **Seed funds.** These funds (e.g., SV Angel, First Round Capital, Slow Ventures, and BoxGroup) base their investment thesis on investing small amounts of capital in a large number of companies. They are well versed in this type of transaction and are able to quickly decide whether to invest and then move to close the transaction. They often invest between \$50,000 and \$500,000.
- **Incubators/accelerators.** These organizations (e.g., Y Combinator, TechStars, and 500 Startups) provide small amounts of capital (such as \$100,000) and a formal educational program in exchange for a fixed percentage of a company (often 6–8%). They also separately invest in their companies through seed financings without companies going through their formal education program.
- **Professional angels.** These are individuals (e.g., Ron Conway) who invest as their primary occupation. They are often extremely well-connected within their community and able to introduce founders to other investors and provide advice to early-stage founders. They often invest between \$25,000 and \$100,000.
- **Seed funding platforms/syndicates.** On these platforms (e.g., AngelList) individual investors come together to pool their money and follow the lead of an angel investor they trust to invest on their behalf or otherwise discover companies in which to invest. Typical investments for each individual can range from \$2,500 to \$50,000.
- **Serial entrepreneurs.** These are individuals who have accumulated wealth due to prior successes. They tend to invest in order to pay it forward and to mentor other founders as they start their companies. These individuals typically invest between \$25,000 and \$100,000.
- **Industry experts/advisors.** These individuals have expertise in the field in which the start-up is interested and can deliver mentorship and guidance as the company begins its journey. Investing gives these advisors the opportunity to have skin in the game and see upside for their time

spent advising the company. These experts typically invest \$10,000 to \$25,000.

- **Wealthy individuals (including friends and family).** These are individuals with a broad range of sophistication, which can often be as little as having watched an episode of Shark Tank. They have money to deploy, want to feel connected to the energy of a technology company, may see tech investing as a risky asset class within their broader portfolio, or want to help out a founder who is a friend/family member. These individuals may invest as little as \$2,500 and as much as \$250,000.

Most rounds of seed financing consist of a blend of the above investors, as each brings its own value to the table (beyond just capital). One balancing act to consider is whether to include a professional VC in the seed round. While it can be seen as a positive signal initially, it can be a double-edged sword in that the VC’s decision to either lead, participate in, or elect not to participate in the subsequent preferred stock financing will be a very strong signal in the market (and often the VC will elect not to participate or lead the round, which reduces potential new investors’ confidence).

Overview of Seed Financing Legal Instruments

The three most common types of series seed financing instruments are convertible notes, simple agreements for future equity, and preferred stock. These three instruments cover virtually all seed financing transactions in Silicon Valley and with start-ups across the country. The company almost always determines which instrument to use, unless there is a significant (lead) investor that negotiates the terms of the entire financing round on behalf of all other investors and feels strongly about the form the seed financing takes.

You should note that sales of common stock are not typically used for seed financing for two primary reasons. First, common stock does not come with the various investor-friendly terms (described below) that other instruments include, so it is less appealing to investors. Second, it places a price on the outstanding common stock, which then will set the price for grants of options and restricted stock to employees. Typically, a valuation firm using 409A methodology (i.e., performing a valuation before a liquidity event such as an initial public offering in accordance with Section 409A of the Internal Revenue Code) will value common stock in an early stage start-up at around 20–25% of the preferred stock. Thus, a priced common round with investors would eliminate this lower price benefit, which is one of the key recruiting tools for early employees.

CONVERTIBLE NOTES ARE THE DEFAULT METHOD FOR RAISING SEED CAPITAL AND DEFINITELY FOR SEED ROUNDS RAISING LESS THAN \$2 MILLION. IN TERMS OF PROCESS, CONVERTIBLE NOTE FINANCINGS MAY OR MAY NOT BEGIN WITH A FORMAL TERM SHEET.

Convertible Notes

Convertible notes are loans (i.e., debt) by an investor that convert into an equity interest in the company upon a priced preferred stock financing meeting certain conditions. Convertible notes are by far the most common instrument used to complete seed rounds.

Key Terms

In drafting convertible notes, you should include the following key terms:

- Conversion events, which usually consist of a qualified subsequent financing (usually a preferred stock financing raising new money above a certain threshold (typically \$2 million)), a company acquisition, or (sometimes) the maturity date
- Automatic or voluntary conversion feature
- Conversion price, which is typically the lower of (a) an agreed cap on the valuation of the company prior to further investment (pre-money) at the time of conversion, and/or (b) a discount (typically 15–25%) of price per share of the shares issued in the qualifying financing
 - Almost all notes are capped, as the cap establishes an approximate valuation for the company and sets the general bounds for what percentage of the company the investor is purchasing when the notes convert.
- Change of control premium, which is usually a premium payment (50–100% of the principal and interest outstanding) or conversion to common stock at the valuation cap
- Interest rate, which is nominal and can be as low as the applicable federal rate
- Maturity date (e.g., 12–24 months)
- Events of default
- Protective provisions (i.e., consent from the noteholder(s) is required to take certain actions, such as creating an equity incentive plan or selling the company) (unusual)
- Security interest (unusual)

Advantages

The advantages of convertible notes include:

- **Well-established and understood.** Companies, investors, and their lawyers understand the mechanics. This results in a short timetable to complete (e.g., 1–2 weeks in their simplest form) and relatively low legal fees.
- **Operating flexibility.** For a company, convertible notes give founders more freedom to make decisions as they do not contain the typical controls on a company that a preferred stock investor would require.
- **Valuation.** The company can put off negotiating a valuation until the priced preferred stock round (though the cap and/or discount function as a maximum approximate valuation).
- **Amendment.** A note facility (i.e., many investors investing under one note purchase agreement) means that all notes can usually be amended by a majority of dollars invested in the note round. This can sometimes be necessary if, for example, the maturity date needs to be extended or other terms changed before or in connection with a priced preferred stock financing. For this reason, you should structure a convertible note round as a facility whenever possible, rather than as a series of individual independent notes.
- **Unsecured.** In the event of a liquidation of the company, the notes will receive payment prior to any payments flowing to other types of investors, but the note investors cannot foreclose on the company’s assets since the notes are typically unsecured.

Disadvantages

The disadvantages of convertible notes include:

- **Repayment.** Notes need to be repaid upon maturity or in event of default, and the company may not have the funds to do so. However, if the maturity date passes and the company has not yet raised a priced preferred stock round (so the notes have not converted), then investors usually will agree to extend the maturity date so that the company has additional time to raise the Series A round.



- **Dilution to founders.** Typically, outstanding convertible notes are included in the pre-money capitalization in the next financing, so these notes are dilutive to the existing stockholders (e.g., the founders and early employees) but not to the new preferred stock investors.
- **Liquidation preference windfall.** If not drafted to convert to a shadow preferred (which is a different series of preferred with liquidation preference equal to the price at which the applicable note(s) convert) or partial preferred/common blend, they can create extra liquidation preference above all common equity (i.e., for the discounted portion of the note due to the discount or cap).

Process

Convertible notes are the default method for raising seed capital (and definitely for seed rounds raising less than \$2 million). In terms of process, convertible note financings may or may not begin with a formal term sheet. Because the terms are relatively straightforward, it is often customary for you, the company counsel, to simply draft the convertible note documentation based on rough parameters agreed to by the company and its initial lead seed investor. Often there is little to no negotiation outside the key terms listed above, as they are legally straightforward to implement (which is another benefit of using a convertible note structure).

Simple Agreements for Future Equity

In December 2013, Y Combinator (a leading start-up accelerator) introduced its alternative to convertible notes—Simple Agreement for Future Equity (SAFE), <https://www.ycombinator.com/documents/#safe>. It provides four types of SAFEs, each of which is freely accessible on the Y Combinator’s website:

- The first SAFE includes a cap but with no discount.
- The second does not include a cap but does include a discount.
- The third contains both a cap and a discount.
- The fourth contains a most-favored nation clause, but neither a cap nor a discount.

Key Terms

In drafting SAFEs, you should be familiar with the following key terms:

- **Valuation cap.** The valuation cap is a maximum value ascribed to the company, such that in a qualified financing, the SAFE converts as the lower of the price per share calculated using the valuation cap and the actual price per share of preferred stock sold in such financing.
- **Conversion discount.** The conversion discount (e.g., 15–25%) is the amount the price per share in a qualified financing is discounted for determining the price per share at which the SAFE converts.
- **Most-favored nation status.** The holder of the SAFE may be entitled to receive the benefit of any preferential terms received by any subsequent purchaser of convertible securities of the company.
- **Pro rata rights.** SAFEs by default provide that the investor will receive pro rata rights to purchase more shares in all future financings by the company excluding the financing in which the SAFE converts, without limiting this right to those investing above a certain amount (as is typical during a financing).

Note that SAFEs include neither an interest component nor an obligation to repay absent a conversion.

Advantages

The advantages of SAFEs include:

- **Quick and Simple.** Like convertible notes, they are relatively quick and inexpensive to negotiate and draft.
- **Stand-alone agreements.** By default, SAFEs are structured as stand-alone agreements. This allows for a company to sell them to investors individually as the investors are ready to close, avoiding the need to coordinate a simultaneous closing with many investors.

Disadvantages

The disadvantages of SAFEs include:

- **Stand-alone agreements.** As discussed above, SAFEs are structured as stand-alone agreements. A company could issue a different type of SAFE to each of its investors, creating disclosure issues and potentially massive coordination challenges when the SAFEs convert in an equity financing if there are multiple varieties of SAFEs outstanding. In addition, amending each SAFE requires the consent of each holder, making changing terms in connection with a financing much more difficult.
- **Multiple valuation caps.** By default, SAFEs convert into a series of shadow preferred stock in order to provide the correct liquidation preference (i.e., only the amount of capital actually invested by the investor). If a company issues SAFEs with different caps, multiple series of shadow preferred stock will be required, causing great administrative complexity at the time the SAFEs convert to preferred stock.
- **Pro rata rights.** Pro rata rights are extremely atypical and not customary for small seed investors to receive. You should either remove pro rata rights from the SAFE before it is presented to investors or limit them by incorporating an investment threshold.
- **Some ambiguity regarding proper tax and accounting treatment.** While Y Combinator has asserted that SAFEs are equity instruments, not debt (and thus no minimum applicable federal rate is required for interest, and they are not subject to various other debt legal requirements), the sentiment among Silicon Valley lawyers and accountants is that this is not a settled question. There is not complete agreement in the tech community about whether these instruments are properly characterized as debt or equity. This can lead to confusion and complexity for the company’s (and investors’) tax and accounting records.

Process

SAFEs are becoming more and more common as the market becomes more accustomed to them. Since they have very few inputs and, if used as provided by Y Combinator, require few changes to the provisions, founders tend to use them without consulting outside legal counsel first, who will often explain the above issues and either tweak the documents to resolve them or guide the company to use a more traditional convertible note structure. In general, closing a seed financing with SAFEs is straightforward once the company and investors agree to the key terms.

Preferred Stock

There are two types of preferred stock documents used in seed financings: the lightweight version www.seriesseed.com and a full Series Seed set of documents.

Full Series A Documentation

Some professional VCs have interpreted Series Seed to mean full-blown Series A documentation (with all the related rights and privileges) as per the National Venture Capital Association’s model legal documentation, <http://nvca.org/resources/model-legal-documents/>. This includes five major transaction documents:

- Stock purchase agreement
- Certificate of incorporation
- Investors’ rights agreement
- Voting agreement and right of first refusal
- Co-sale agreement

There are also additional ancillary documents like a legal opinion and closing certificates.

The full Series A documentation is typically significantly more expensive in legal fees and requires the negotiation of all the terms and documents that will be used in a later Series A financing. This can be difficult since the seed round often does not include traditional lead investors with which the company can negotiate the documents. This structure of transaction can typically take 4–6 weeks to complete (from finalization of the term sheet to closing of the investment).

Series Seed Preferred Documentation

There is also a set of Series Seed preferred stock documents (<http://www.seriesseed.com/>) that take into account various perspectives from the broader Silicon Valley community, including VCs and entrepreneurs. These documents greatly simplify the transaction and defer the detailed negotiation of a fulsome set of investor rights until the Series A financing.

The Seriesseed.com approach includes most of the key terms included in a traditional full Series A round, including:

- Liquidation preference
- Limited protective provisions (i.e., prohibiting the company from taking certain actions without the consent of the preferred stockholders; such actions may include changing rights of preferred stock, increasing authorized capitalization, creating senior series/class of preferred stock, redeeming stock (subject to customary exceptions), declaring dividends, changing board size, or selling or liquidating the company)
- Board seat
- Preemptive rights
- A drag-along (i.e., the ability to compel an investor to participate in certain sales)

On the other hand, it does not include:

- Typical price-based anti-dilution protection
- Registration rights
- Full right of first refusal and co-sale rights for investors over founder shares

The investors will receive the same rights as the future investors in the Series A financing. Importantly, the Seriesseed.com approach only requires two documents:

- Investment agreement
- Certificate of incorporation

No ancillary documents like a legal opinion and closing certificate are required, so the process is significantly streamlined and therefore less expensive. Using the Seriesseed.com documents is straightforward. All the key terms are defined in a definitions section in the beginning of the investment agreement and the certificate of incorporation.

Securities Laws Considerations


Federal Exemptions

Regardless of how the seed investment is structured, it’s critical that the company has a valid federal securities law exemption from registration under the Securities Act of 1933, as amended (Securities Act), for the issuances. The two most commonly used federal exemptions for seed financings are:


- The private placement exemption provided by Section 4(a)(2) (15 U.S.C.S. § 77d) of the Securities Act, which exempts “transactions by an issuer not involving any public offering”
- Rule 506(b) (17 C.F.R. § 230.506) of Regulation D, which provides a safe harbor under Section 4(a)(2) of the Securities Act

Related Content

For a detailed examination of venture capitalists and private equity firms, see

> [PRIVATE EQUITY INDUSTRY PRACTICE GUIDE](#)
 **RESEARCH PATH:** [Capital Markets & Corporate Governance](#) > [Industry Practice Guides](#) > [Private Equity](#) > [Practice Notes](#)

For additional information on convertible notes, see

> [UNDERSTANDING CONVERTIBLE DEBT SECURITIES](#)
 **RESEARCH PATH:** [Capital Markets & Corporate Governance](#) > [Debt Securities Offerings](#) > [Rule 144A/Regulation S Debt Offerings](#) > [Practice Notes](#)

For an explanation on the use of Simple Agreement for Future Equity (SAFEs) securities in the crowdfunding context, see

> [MARKET TRENDS: CROWDFUNDING – OTHER KEY MARKET TRENDS](#)
 **RESEARCH PATH:** [Capital Markets & Corporate Governance](#) > [Market Trends](#) > [Equity](#) > [Practice Notes](#)

For an overview on convertible notes, see

> [UNDERSTANDING ANTI-DILUTION ADJUSTMENT FORMULAS IN CONVERTIBLE BONDS](#)
 **RESEARCH PATH:** [Capital Markets & Corporate Governance](#) > [Debt Securities Offerings](#) > [Rule 144A/Regulation S Debt Offerings](#) > [Practice Notes](#)

For guidance on managing a private offering, see

> [MANAGING THE PRIVATE OFFERING](#)
 **RESEARCH PATH:** [Capital Markets & Corporate Governance](#) > [Private Offerings](#) > [Private Placements](#) > [Practice Notes](#)

For a sample convertible note to be used in connection with a pre-seed or seed financing transaction for a start-up company, see

> [CONVERTIBLE PROMISSORY NOTE](#)
 **RESEARCH PATH:** [Corporate Counsel](#) > [Financing and Venture Capital](#) > [Venture Capital Financing](#) > [Forms](#)




Historically, the private placement exemption was the traditional exemption relied upon for federal securities exemptions, but Regulation D has now become more common and most companies rely on this exemption because its parameters are more certain than Section 4(a)(2) alone. Rule 506(b) allows for the company to sell securities to an unlimited number of accredited investors (defined in Rule 501(a)) (17 C.F.R. § 230.501) and up to 35 other purchasers. If those other purchasers are unaccredited, they must be sophisticated (i.e., have sufficient knowledge and experience in financial and business matters to make them capable of evaluating the merits and risks of the prospective investment). However, it’s generally advisable for companies using this exemption to sell only to accredited investors. This is because including non-accredited investors requires a company to deliver exhaustive disclosure and offering documents, which can be prohibitively expensive and time-consuming from a legal and accounting perspective for a young company to prepare. It’s also worth noting that if you want to take advantage of the new provisions in Rule 506(c) that allow general solicitation, all investors must be accredited.

A company that makes an offering under Regulation D is required to file a Form D with the Securities and Exchange Commission (SEC) within 15 days of the first sale of securities. Once filed, the Form D is available to the public on the SEC website, and various news organizations will trawl the SEC website and report on start-ups’ fundraising activities. Thus, you should advise the company to prepare a press release on a parallel path to the Form D filing in order to manage its public narrative.

Blue Sky

In addition to the federal securities law exemption, the company also needs to comply with state securities laws (blue

sky laws) in the state in which it is located and the states in which each of its investors is located. Compliance regimes vary from state to state, but most often there is either a notice filing if using Section 4(a)(2) or an electronic filing if using Regulation D. For example, if the company relies on the 4(a)(2) private placement exemption in California (and does not file a Form D), it should file a 25102(f) notice (http://www.dbo.ca.gov/forms/doc/DBO-25102f_Packet.pdf) with the California Department of Business Oversight. Some states require the filing to be made in advance of the sale of securities, so you should be careful to check the blue sky regime in each applicable state before the securities are sold. 

Kristine Di Bacco represents emerging technology companies primarily in the consumer internet, e-commerce, FinTech, digital health, and consumer hardware and software sectors at Fenwick & West. Her practice includes a broad range of corporate transactional matters, including the formation of new start-up companies, venture capital financings, mergers & acquisitions, and public offerings. Kristine provides clients with practical and thoughtful advice to help solve their business and legal issues and assists clients in structuring, negotiating, and closing business transactions quickly and effectively. Kristine also represents and advises leading incubators, angel investors, and venture capitalists investing in technology companies. Doug Sharp focuses his practice at Fenwick & West on a variety of corporate matters to support clients in the technology industry. While attending law school, Doug was the Financial Director & Member Editor for the Stanford Technology Law Review.

 **RESEARCH PATH:** [Capital Markets & Corporate Governance](#) > [Industry Practice Guides](#) > [Technology](#) > [Practice Notes](#)



Trevor S. Norwitz, Sebastian V. Niles,
Avi A. Sutton and Anna S. Greig WACHTELL, LIPTON, ROSEN & KATZ

Market Trends: Shareholder Proposals

Shareholder proposals are a popular and effective mechanism enabling shareholders to recommend or require that a company and/or its board of directors take a specified action.

TO BE ELIGIBLE TO SUBMIT A PROPOSAL FOR CONSIDERATION at a meeting of the company’s shareholders and have such proposal included in the company’s proxy statement and proxy card under federal law, a shareholder must have held company shares with a market value of at least \$2,000 (or at least 1% of the company’s securities entitled to vote on the proposal at the shareholder meeting) for at least one year and comply with additional substantive and procedural rules set forth in Rule 14a-8 (17 C.F.R. § 240.14a-8) under the Securities Exchange Act of 1934, as amended (the Exchange Act). There has been criticism that the dollar threshold in Rule 14a-8, which was adopted decades ago in 1998, is too low. See e.g., Comment Letter of The Business Roundtable, File No. S7-25-97 (Dec. 9, 1997). It is possible that this threshold may be raised in the future and that other reforms may be made to the shareholder proposal process. Alternatively, albeit infrequently used, a shareholder may submit a proposal under state law, without regard to the requirements of Rule 14a-8, but must bear the cost of preparing and mailing its own proxy statement to the company’s shareholders.

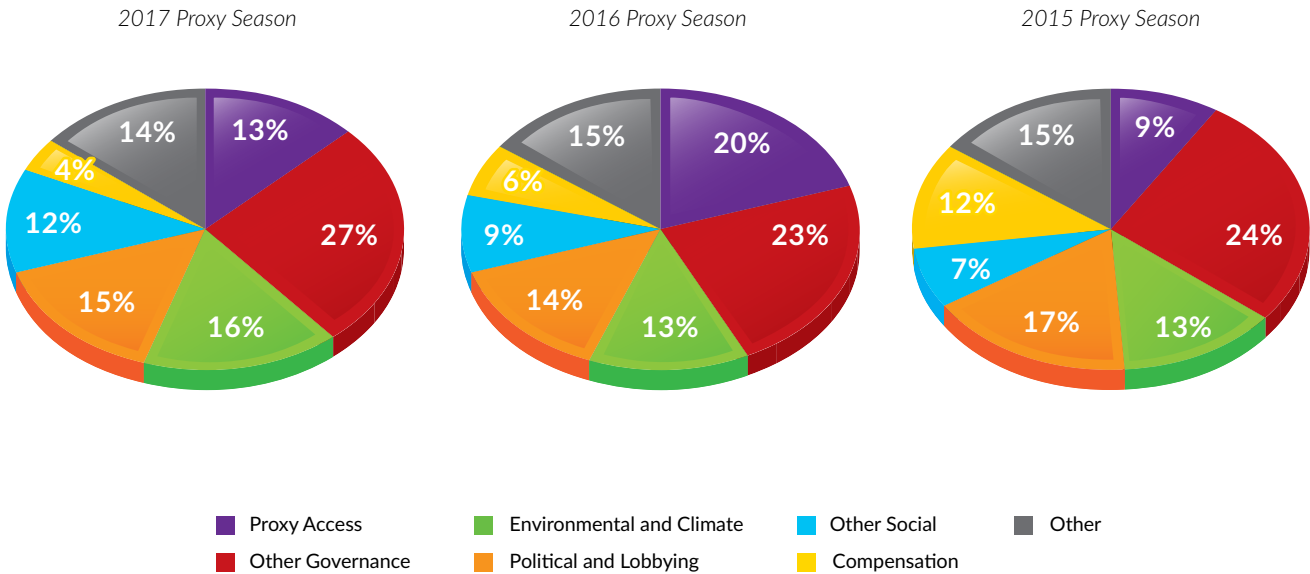
After a significant increase in the frequency of shareholder proposals in the 2015 proxy season—due in large part to the prevalence of proxy access proposals described below—the number of shareholder proposals submitted to U.S. public companies has been decreasing somewhat (from 943 in 2015, to 916 in 2016, down to 861 in 2017), though the number of proposals still exceeds the 2013 level (820), according to the Institutional Shareholder Services (ISS) Voting Analytics database and other privately sourced data. (All 2017 data herein

is as of July 1, 2017.) As the number of shareholder proposals submitted has increased since 2013, however, the average investor support for shareholder proposals has actually been declining over the past five years, down from 34.4% in 2013 to 29.8% in 2016 and 25% in 2017.

As discussed in detail below, prior trends are expected to continue. In particular, it is expected that:

- The pressure to adopt proxy access bylaws will continue to increase at large-cap companies and begin spreading to mid-cap companies.
- Proponents of proxy access will attempt to refine proxy access bylaws by proposing amendments to existing proxy access bylaws.
- Other governance-related proposals will decline at large-cap companies but increase at mid-cap companies.
- Specific compensation-related proposals will reappear in light of high-profile controversies and legislative uncertainty.
- Shareholder support for environmental and social topics and board diversity—gender diversity in particular—will increase.
- While less common, shareholder proposals may continue to address economic/business issues and be put forward by economic-oriented activists / hedge funds (e.g., Greenlight’s Spring 2017 proposal at General Motors, which ultimately failed).

Common Types of Proposals



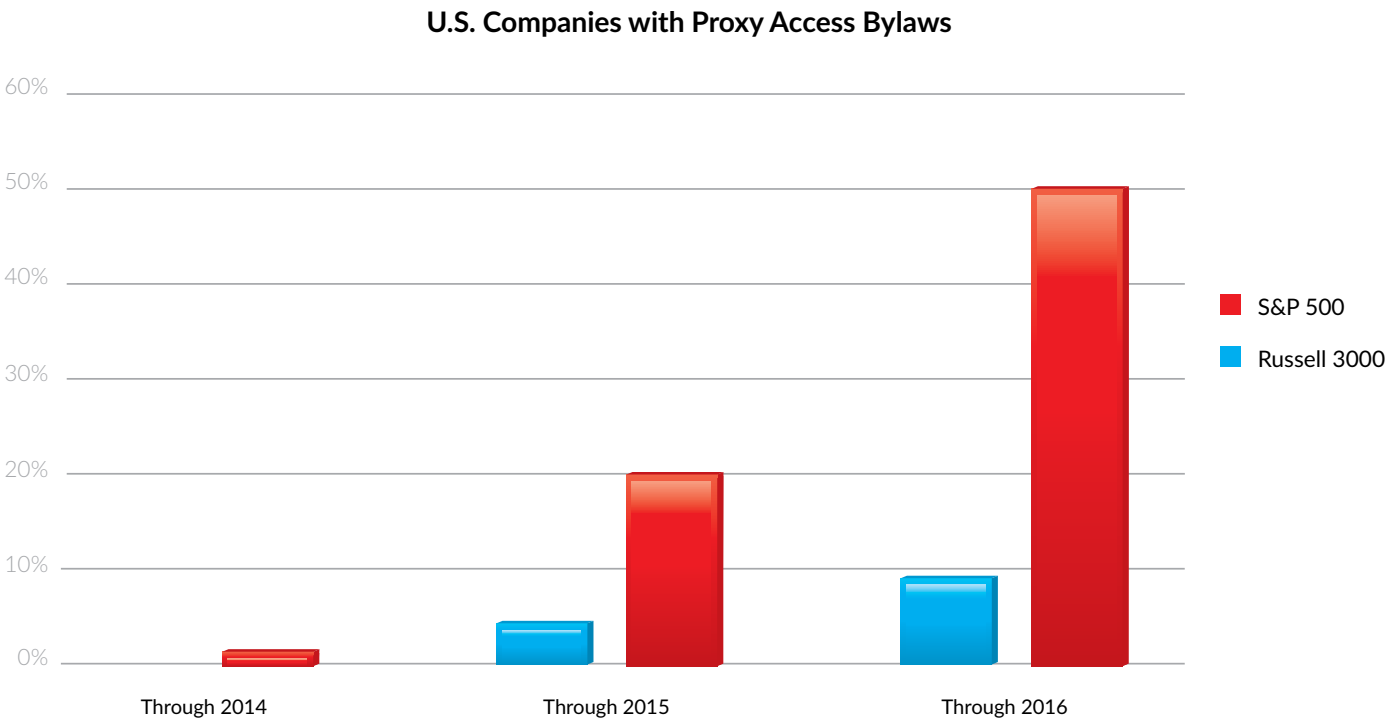


Governance

Proxy Access

Proxy access gives shareholders who meet specified conditions the right to include one or more shareholder-nominated candidates for election to the board of directors in the company’s proxy statement and on its proxy card. Since 2015, proxy access has been one of the more dominant shareholder proposals at large-cap companies and the most likely type of shareholder proposal to obtain majority shareholder support. This has resulted in a majority of S&P 500 companies adopting some form of proxy access, either as a result of a successful shareholder proposal or due to voluntary adoption of a proxy access bylaw with terms consistent with market practice.

Given this widespread adoption, pressure to adopt proxy access at remaining large-cap companies is likely to increase, but the focus of proponents of shareholder proposals may begin shifting to the amendment or refinement of existing proxy access bylaws. However, unless they target real outliers, fix-it proposals that make it to a vote will likely fare poorly—during the 2016 and 2017 seasons, all proposals for bylaw amendments failed at every company that had already adopted proxy access with market standard terms (i.e., those that permit a shareholder, or group of up to 20 shareholders, owning 3% or more of the company’s common stock continuously for at least three years, to nominate up to 20% of the company’s board).



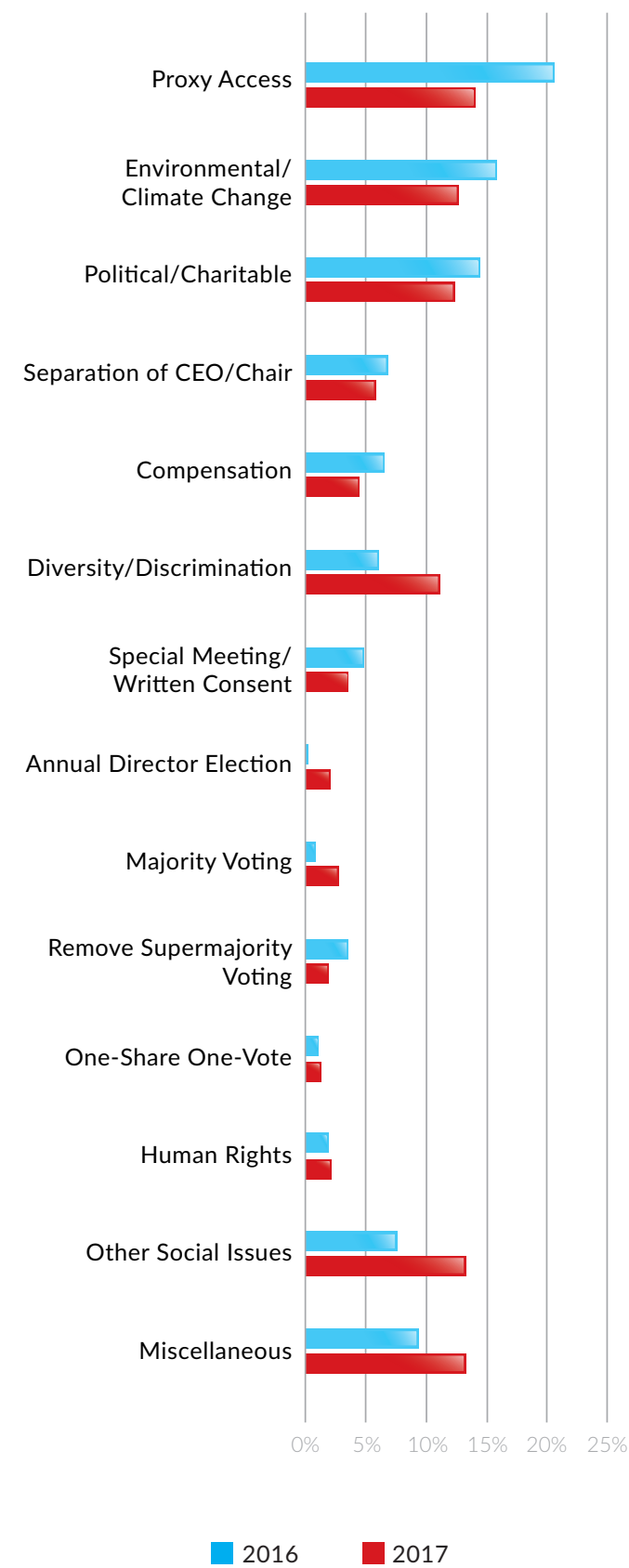
While during the 2015 season and much of the 2016 season companies often excluded proxy access proposals on the basis of a conflicting management proposal on the same topic, recent guidance issued by the Securities and Exchange Commission (SEC) has narrowed the ability of companies to exclude shareholder proposals. See SEC Staff Legal Bulletin No. 14H (October 22, 2015), <https://www.sec.gov/interps/legal/cfslb14h.htm>, and Legal and Regulatory Trends below. As a result, proxy access proposals that were excluded in 2017 were primarily excluded on the basis of substantial implementation by the company, rather than a conflicting management proposal.

Separate Chairman and CEO

Shareholder proposals regarding the separation of the chairman and chief executive officer (CEO) positions are common, as they have been for a number of years. While still popular, the total number of these proposals decreased in 2016 and 2017 at S&P 500 companies (41 and 36, respectively) as compared to 2015 (55), due in large part to their low success rate in 2015 (average 3.6% of support, and none achieved majority support in 2016). This decline in proposals has also been seen in the subset of independent chair proposals that were actually submitted for a shareholder vote, rather than withdrawn by the proposing shareholder or omitted by the company; however, the proposals that ultimately make it to a vote have seen modest increases in support.

INDEPENDENT CHAIR PROPOSALS SUBMITTED TO A VOTE (Excludes withdrawn or omitted proposals)								
# of Proposals Voted On			Average % Support			Proposals Passed		
2017	2016	2015	2017	2016	2015	2017	2016	2015
31	35	44	33.5%	27.0%	30.1%	0	0	2

Shareholder Proposals by Category



Although proxy advisory firms such as ISS and Glass Lewis generally support these proposals, investors are increasingly of the view that a lead independent director with broad powers and responsibilities is an acceptable alternative to separation of the chairman and CEO roles.

Due to the low overall success rate of these proposals over the past few years, whether due to a withdrawal, omission, or failed vote, shareholder proponents may be more selective going forward about the companies targeted with this type of proposal. Instead, shareholder proponents may focus on companies with more significant or pervasive performance or governance concerns in order to garner higher support.

Shareholder Off-Cycle Action Rights

Proposals regarding shareholders’ right to call a special meeting or to act by written consent are also relatively common.

A significant majority of large-cap companies already grant shareholders the right to call special meetings, so most new shareholder proposals on the topic call for a reduction in the ownership threshold of existing special meeting rights.

Additionally, proposals requesting that companies permit shareholders to act by written consent have dropped significantly since 2015. The shift of focus to proxy access is partially responsible for this decrease, but many investors have also come to believe that special meeting rights are a sufficient (and more appropriate) mechanism to allow shareholder action outside of the annual shareholder meeting.

Other Governance Topics

Traditional governance proposals, such as board de-staggering, majority voting, and elimination of supermajority voting, have become less common as most large-cap companies have already adopted these measures. Rather than turning their attention to the same issues at smaller companies, proponents of shareholder proposals have typically moved on to new causes, the most notable being proxy access. Nevertheless, in 2016 the Council of Institutional Investors announced a campaign to target close to 200 Russell 3000 companies that still have a plurality standard in director elections, and such proposals typically pass when submitted. See Council of Institutional Investors, Majority Voting for Directors, http://www.cii.org/majority_voting_directors.

Compensation

The 2016 proxy season marked a five-year low for the number of compensation-related shareholder proposals voted upon—and none received majority support. This is due in large part to the required say-on-pay votes, which provide investors an alternative mechanism to express their approval or disapproval of a company’s executive compensation program.



However, a number of proposals on new compensation topics surfaced in 2016, including calls to adjust incentive metrics to account for share buybacks and the prohibition of government service golden parachutes. Although none received majority support, one proposal at Xerox to adjust incentive metrics to account for share buybacks did receive 45.6% support. See Sydney Carlock, et al., 2016: Proxy Season Review – Compensation, ISS Report Center (Sept. 22, 2016).

While compensation-related proposals had been on the decline because of recent high-profile controversies and uncertainties surrounding legislative solutions, the 2017 season actually saw an increase in the number of proposals on compensation, in particular compensation clawbacks. Additionally, due to investors’ heightened focus on climate change, shareholder proponents submitted eight proposals relating to the linking of executive pay to sustainability or climate metrics. More of these may be on the horizon.

Environmental and Social

Proposals relating to environmental and social issues were the most common proposal type at S&P 500 companies for each of the last five years (up to 354 in 2017). This figure includes all topics in the broad environmental and social category, including climate change and climate regulation; environmental health and safety; political, lobbying, and charitable disclosure; human rights; diversity, gender, and discrimination topics; and other miscellaneous social topics. Specifically, proposals requesting increased climate risk

disclosure had greater support in 2017 (33.7%) and 2016 (34.5%) as compared with 2015 (23.2%). Although the 2016 proxy season did not see majority support for environmental and social proposals, the increasing support culminated in the passage of climate-related proposals at four S&P 500 companies in 2017, most notably the support by 62% of ExxonMobil shareholders for a proposal that requires ExxonMobil to report on the impact of climate change on its business. In 2016, only 38% of ExxonMobil shareholders supported a substantially identical proposal, indicating the rapid pace at which shareholder support for climate-related proposals is increasing year over year.

Support from large institutional investors for shareholder resolutions on climate change is also increasing. For example, State Street backed 51% of such resolutions in 2016, compared with only 14% in 2015. See Shirley Westcott, Proxy Advisors and Investors Prep for 2017 Proxy Season, Harvard Law School Forum on Corporate Governance and Financial Regulation (Dec. 22, 2016), <https://corpgov.law.harvard.edu/2016/12/22/proxy-advisors-and-investors-prep-for-2017-proxy-season/>. Additionally, a number of significant institutional investors have recently committed to supporting enhanced climate risk disclosure. BlackRock, which holds a stake in most major U.S. public corporations, identified climate risk as one of its top engagement priorities for 2017. See Annual Letter to CEOs from Larry Fink, Chairman and Chief Executive Officer of BlackRock (Jan. 24, 2017), <https://www.blackrock.com/corporate/en-no/investor-relations/larry-fink-ceo-letter>.

FIX-IT CAMPAIGNS TO AMEND EXISTING PROXY ACCESS BYLAWS ARE EXPECTED TO CONTINUE AND, AS MORE COMPANIES ADOPT PROXY ACCESS, INCREASE IN FREQUENCY.

In addition to climate and sustainability proposals, shareholder proposals relating to political expenditures and lobbying are common, though decreasing. Notably, conservative shareholder groups have joined their progressive counterparts in putting forth shareholder proposals on social issues. However, shareholder support for proposals on these topics is generally quite low, with only two proposals out of 61 voted on in 2016 receiving majority support. See Glass Lewis, 2016 Season Review: United States and Canada Governance Lessons from January to June 2016 (Aug. 31, 2016). In 2017, none of the 50 political/lobbying proposals that went to a vote received majority support.

Finally, gender pay equity garnered increasing attention in the 2016 and 2017 proxy seasons, highlighted by the increased shareholder support for a proposal at eBay to sponsor a gender equality study that was submitted in each of the 2015 and 2016 proxy seasons. The proposal received only 8.5% support in 2015, followed by 51.2% support in 2016 to pass.

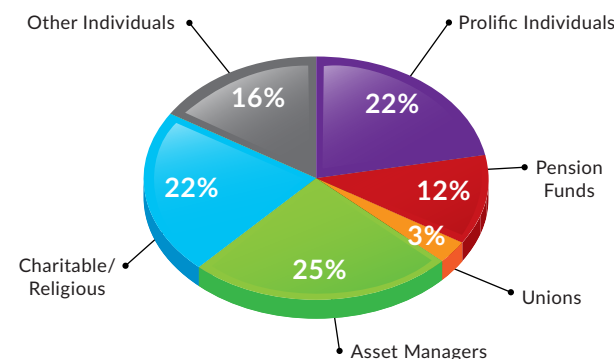
Proponents

The most prolific proponents of shareholder proposals are individual investors John Chevedden, James McRitchie, William and Kenneth Steiner, and Jing Zhao. Chevedden alone accounts for approximately 14% of all shareholder proposals submitted in the 2017 season. Individuals of this ilk are sometimes referred to as “gadfly investors,” as their interests are generally not those of typical investors but are instead meant to instigate and bring about change.

The New York City Comptroller submitted a large number of shareholder proposals on behalf of five New York City pension funds in 2015 and 2016, primarily focused on proxy access as part of the Comptroller’s “Boardroom Accountability Project.” The initiative targets companies where three priority issues generate concerns: (1) climate change risk, (2) board diversity, and (3) excessive executive compensation. In 2017, the Comptroller was less active in submitting proposals related to proxy access. Instead, the Comptroller focused its attention in 2017 on proposals requesting enhanced sustainability disclosure.

Other proponents of shareholder proposals include:

- Public pension funds, which focus their proposals mainly on governance issues related to board diversity and social proposals relating to employee diversity, political contribution disclosure, and environmental issues
- Labor unions, which focus primarily on governance and compensation-related issues
- Asset management or advisory institutions, which focus on environmental and social issues



Legal and Regulatory Trends

The 2017 proxy season has unfolded during a time of considerable legal and regulatory uncertainty across a broad range of topics. In particular, the regulation of proxy advisors may gain traction with the new U.S. administration, giving proxy advisors reason to actively engage with companies as they shape their voting recommendations. Both ISS and Glass Lewis have new staff members in critical roles, and therefore institutional knowledge and precedent may not carry the same weight as in prior years.

In addition, the regulatory framework addressing no-action relief for the exclusion of shareholder proposals from proxy materials is evolving. Generally, a company may exclude a shareholder proposal from its proxy materials if the proposal fails to meet any of the procedural and substantive requirements of Rule 14a-8 (17 C.F.R. § 240.14a-8). A company may seek no-action relief from the SEC to exclude a proposal from its proxy materials on a number of additional grounds, most usually because of a direct conflict with a management proposal (Rule 14a-8(i)(9)) or because there has already been substantial implementation of the proposal (Rule 14a-8(i)(10)).

In the fall of 2015, the SEC issued Staff Legal Bulletin No. 14H, <https://www.sec.gov/interps/legal/cfslb14h.htm>, making it more difficult to obtain no-action relief on the direct conflict ground. After initially granting no-action relief to Whole Foods for a shareholder proposal seeking to amend the company’s existing proxy access bylaw, the SEC reversed course and refused to grant no-action relief on the basis of a direct conflict. The SEC stated that it would permit a company to exclude a shareholder proposal on the basis that it directly conflicts with a management proposal only “if a reasonable shareholder could not logically vote in favor of both proposals, i.e., a vote for one proposal is tantamount to a vote against the other proposal.”


As a result, proposals with similar objectives on different terms will not be considered to directly conflict with one another. In light of this development, the number of ballots containing competing proposals increased in the 2016 and 2017 seasons. The board of directors in such a circumstance may have to consider the effects of both proposals, and any company that includes a shareholder proposal and a management proposal on the same topic may have to include a proxy statement disclosure explaining the differences between the proposals and how the company expects to consider the voting results.

Following the issuance of Staff Legal Bulletin No. 14H, a higher proportion of no-action requests were made on the basis of substantial implementation. The substantial implementation ground permits exclusion if a company has satisfied the essential objective of the proposal. While this basis for exclusion remains viable in many cases, in July 2016 the SEC denied no-action relief on the basis of substantial implementation in the case of a proxy access bylaw when the provision already implemented by the company was very similar to that proposed. The denial suggests that companies may not easily be able to rely on substantial implementation as a basis to exclude shareholder proposals calling for revisions to proxy access bylaws, though it is likely still a basis for exclusion of proxy access adoption proposals. In certain cases, proposals to revise existing proxy access bylaws will still be excludable.

Related Content


For a complete discussion on the shareholder proposal process, see

> [EXCLUDING SHAREHOLDER PROPOSALS AND SEEKING NO-ACTION LETTERS](#)

 **RESEARCH PATH:** [Capital Markets & Corporate Governance > Proxy Statement and Annual Meeting > Shareholder Activism > Practice Notes](#)

For a summary on how publicly traded companies can prepare for proxy voting recommendations by Institutional Shareholder Services (ISS), see

> [PREPARING FOR ISS PROXY VOTING RECOMMENDATIONS CHECKLIST](#)

 **RESEARCH PATH:** [Capital Markets & Corporate Governance > Proxy Statement and Annual Meeting > Shareholder Activism > Checklists](#)

For guidance on the practice and effectiveness of responding to negative vote recommendations from proxy advisory firms, see

> [MARKET TRENDS: ADDITIONAL PROXY SOLICITING MATERIALS RESPONDING TO NEGATIVE VOTING RECOMMENDATIONS](#)

 **RESEARCH PATH:** [Capital Markets & Corporate Governance > Market Trends > Corporate Governance & Continuous Disclosure > Practice Notes](#)

Market Outlook

Overall, the rate of shareholder proposals across all topics should remain relatively stable, with individual investors such as John Chevedden continuing to submit a large number of proposals at an array of companies.

Fix-it campaigns to amend existing proxy access bylaws are expected to continue and, as more companies adopt proxy access, increase in frequency. Proposals targeted at companies with primary proxy access provisions that already conform to the market standard are not likely to generate significant shareholder support, but proposals at companies that significantly deviate will likely attract more support.

As noted above, while traditional governance-related proposals have focused on large-cap companies, now that the majority of such companies have adopted the proposed measures, investors may begin to shift focus to small- and mid-cap companies.




Companies should also expect a high number of proposed resolutions on climate change, requests for lobbying and political expenditure disclosure, and workplace diversity. Climate-related proposals will likely see increasing support, and companies should be attentive to changes in their investors' voting policies and practices to best prepare and predict the outcome of proposals that go to a vote.

Related Content

For an overview on the proxy and annual meeting process in general, see

> [PROXY STATEMENT AND ANNUAL MEETING RESOURCE KIT](#)

 **RESEARCH PATH:** [Capital Markets & Corporate Governance > Proxy Statement and Annual Meeting > Resource Kits > Practice Notes](#)

For a description of the frameworks adopted by companies for sustainability reporting and the recent trends in sustainability disclosure, see

> [INTRODUCTION TO CORPORATE SUSTAINABILITY](#)

 **RESEARCH PATH:** [Capital Markets & Corporate Governance > Corporate Governance and Compliance Requirements for Public Companies > Corporate Governance > Practice Notes](#)

For an introduction to proxy advisory firms, see


> [UNDERSTANDING THE ROLE OF PROXY ADVISORY FIRMS](#)

 **RESEARCH PATH:** [Capital Markets & Corporate Governance > Proxy Statement and Annual Meeting > Mailing and Delivery of the Proxy Statement > Practice Notes](#)

As in past years, boards that are seen as insufficiently responsive to shareholder votes may suffer from a negative ISS or Glass Lewis recommendation. With the uncertainty surrounding the legal and regulatory framework for the exclusion of shareholder proposals, companies should be prepared to include shareholder proposals and provide thoughtful and well-reasoned recommendations for or against such proposals.

Approaches to Proxy Season

Given the change in leadership at both ISS and Glass Lewis, companies should refresh and update their proxy advisor outreach plans to ensure a clear narrative, in addition to their plans for shareholder engagement. Companies should develop a keen understanding of shareholder perspectives on the company and foster long-term relationships with major shareholders, including by appropriately handling shareholder requests to discuss governance; the business portfolio, capital allocation, and operating strategy; environmental and social and governance matters; and for greater transparency into the board's practices and priorities. Companies should also integrate business-relevant environmental and social governance considerations into long-term strategy and be prepared to respond to increasing investor attention on the topic.

Boards should evaluate every shareholder proposal thoughtfully and resist changes that the board believes will not be constructive, while addressing any modifications that in the board's judgment will result in transparent, good governance, and promote the long-term interests of shareholders. 

Trevor Norwitz is a partner in the Corporate Department at Wachtell, Lipton, Rosen & Katz where he focuses primarily on mergers and acquisitions and corporate governance matters. He has advised public and private entities across many industries in connection with mergers, acquisitions, divestitures, hostile takeover bids and defenses, proxy contests, joint ventures, financing transactions and corporate governance and crisis management situations. Sebastian V. Niles is a Partner at Wachtell, Lipton, Rosen & Katz where he focuses on rapid response shareholder activism and preparedness; takeover defense and corporate governance; risk oversight, including as to cybersecurity and crisis situations; U.S. and cross-border mergers, acquisitions, buyouts, investments, divestitures, and strategic partnerships; and other corporate and securities law matters and special situations. Avi A. Sutton and Anna S. Greig are associates at Wachtell, Lipton, Rosen & Katz.

 **RESEARCH PATH:** [Capital Markets & Corporate Governance > Market Trends > Corporate Governance & Continuous Disclosure > Practice Notes](#)



Patrick Yingling and Aleksandra Kopec KING & SPALDING

Market Trends: Middle Market Loans

What is the “middle market” of the U.S. leveraged loan market? While there is no checklist for what constitutes the middle market, the two basic parameters are that the borrower has between \$10 million and \$100 million of annual earnings before interest, taxes, depreciation, and amortization (EBITDA) and the aggregate loan size is in the range of \$30 million to \$500 million. As a general matter, there are common characteristics of credit facilities in the middle market: secured by collateral, small lender groups and other club-type deals, and financial covenant and negative covenant packages that are more robust than those for large corporate borrowers.

THERE HAS BEEN A CONTINUED INCREASE IN ACTIVITY THIS year in the middle market. There has also been a loosening of terms and a move toward more borrower-friendly provisions in credit facilities similar to what have historically been present in bond facilities or large-cap loans. This move is most apparent in the provisions that govern mandatory prepayments, incremental facilities, and negative covenants. Additionally, limited condition acquisition provisions have become commonplace in the middle market, unitranche structures have been increasingly featured in middle market deals, and a new LIBOR issue has created uncertainty throughout the financial markets.

Mandatory Prepayments

There is a distinct move this year toward more borrower-friendly provisions relating to mandatory prepayments resulting from excess cash flow (ECF), asset sales, and extraordinary receipts (i.e., any cash received by or paid to or for the account of any person not in the ordinary course of business). With respect to ECF mandatory prepayments, thresholds are becoming more commonplace in an increasing number of middle market deals. If there is an ECF threshold in an



IT IS COMMON IN MIDDLE MARKET LOAN AGREEMENTS TO GIVE THE BORROWER THE OPTION OF REINVESTING PROCEEDS FROM ASSET SALES IN NEW ASSETS INSTEAD OF REQUIRING THOSE PROCEEDS TO BE USED TO PREPAY THE LOANS.

agreement, a prepayment would be required only after the borrower accumulates a certain dollar amount of ECF in any given fiscal year. In addition, the calculation of ECF continues to be watered down by giving the borrower a dollar-for-dollar reduction for prepayments of certain debt. Historically such dollar-for-dollar reductions were limited to optional prepayments of the term loans plus, more recently, voluntary prepayments of revolving loans (if the revolving commitment is also reduced). But that reduction has increasingly been expanded to include incremental loans, incremental equivalent debt, refinancing facilities, and second lien debt. In addition, the time period for when this debt has to have been prepaid in order to benefit from the ECF reduction is often expanded to include not only the prior fiscal year, but also the period from the end of the prior fiscal year to the ECF calculation date and, in some cases, the borrower can still get the benefit of the reduction even if it has not made the prepayment so long as it has committed to make the payment during the succeeding fiscal year.

Asset sale and insurance condemnation prepayments have also been watered down recently. Both are typically now subject to a certain dollar threshold (both for a single transaction and for all transactions in any given fiscal year). Furthermore, with respect to asset sales, the mandatory prepayment requirements are sometimes being tied to leverage ratios (with step downs) similar to ECF payments.

It is common in middle market loan agreements to give the borrower the option of reinvesting proceeds from asset sales in new assets instead of requiring those proceeds to be used to prepay the loans. Now, the same is becoming true for extraordinary receipts. And with respect to both asset sales and extraordinary receipts, such reinvestment right periods are becoming longer in duration. It is now not unusual for a borrower to have 12 or even 18 months to reinvest the net cash proceeds received from extraordinary receipts or asset sales in other assets useful for its business before the mandatory prepayment requirement is triggered, and that reinvestment

period can be extended for an additional period of time (up to six months) if the borrower commits to reinvesting the proceeds during the reinvestment period.

Incremental Facilities

The incremental facilities section has also evolved toward more borrower-friendly provisions as well. In the past, incremental facilities were available up to a fixed dollar amount. It is becoming increasingly prevalent in the middle market to set the amount available under incremental facilities equal to the sum of:

- A starter basket (i.e., a free and clear basket), which can be the greater of a fixed dollar amount and a multiple of EBITDA, plus
- The amount of any voluntary prepayments of term loans (and, in some facilities, certain other debt), plus
- An unlimited amount subject to a leverage ratio test.

The free and clear basket typically does not have a leverage test associated with it. Many middle market deals permit the borrower to choose which basket they are utilizing at the time of the incremental loan, and some even permit the borrower conveniently to reallocate the amount of the incremental loan between the free and clear basket and the leverage based incurrence basket after the fact.

Most deals set a cap on the amount by which the all-in yield with respect to an incremental term loan can exceed the all-in yield with respect to the existing term loan (called a most favored nation provision). The cap is typically set at 50 basis points, though some very aggressive sponsors have begun asking for that cap to be increased to 75 basis points. Sponsors sometimes request a sunset, or a period of time after the closing date (usually 12 or 18 months, though it may be as long as 24 months or as short as six months in some cases), upon which the most favored nation provision terminates. The sunset provision is clearing the market more often, but it is still fairly uncommon in a true middle market transaction. The majority of deals that have a sunset provision also give the lead arranger the ability to remove the sunset provision if necessary to successfully syndicate the loan.

There has also been an increase in middle market transactions that include the concept of incremental equivalent debt, or sidecar facilities. This is a large cap concept that has worked its way into middle market deals for aggressive sponsors. If a deal has an incremental equivalent debt concept, the borrower can use incremental debt capacity to raise additional pari passu or subordinated secured or unsecured loans outside of the credit agreement. The conditions applicable to incremental loans would also apply to incremental equivalent debt.

A similar large-cap feature—refinancing facilities—has also become more prevalent in large middle market deals. These facilities allow the borrower to refinance all or a portion of its existing loans with new debt issued under the existing credit agreement or with additional debt issued outside of the credit agreement. This concept is attractive to borrowers because it allows them to seek out lower priced debt that would be permitted to share pari passu in the collateral and guarantees of the senior credit facility.

Negative Covenants

The trend toward borrower-friendly provisions in the negative covenants section is most notable in context of the restricted payments and investments covenants (including permitted acquisition flexibility). In the restricted payments and investments covenant, it has become common to have an available amount or builder basket for the borrower. When the concept of an available amount first made its way into middle market transactions, it was usually defined as the amount of ECF that was not required to prepay the loans (i.e., retained ECF). But the available amount definition has slowly picked up additional components, including some or all of the

following: (1) a hard dollar starter amount (typically based on a percentage (usually less than 25%) of the borrower's EBITDA), (2) qualified equity contributions made to the borrower (excluding amounts received in connection with equity cures), and (3) amounts received from gains on investments utilizing the available amount.

The available amount basket can be used by the borrower for acquisitions and other investments and, in some deals, for restricted payments as well. Some aggressive middle market deals contain:

- No leverage ratio test or event of default qualifier on using the available amount for investments –and–
- A closing leverage (or slightly inside closing leverage) ratio condition only on using the available amount for restricted payments

Also, for the benefit of the borrower, it is becoming commonplace in the restricted payments and investments covenants to have an additional basket that is unlimited but subject to a leverage ratio test. Such basket is in addition to the available amount basket (but usually with a de-levering requirement prior to availability).



NONTRADITIONAL DIRECT LENDERS ARE EXPECTED TO CONTINUE GAINING MARKET SHARE IN THE MIDDLE MARKET BECAUSE THEY ARE NOT SUBJECT TO THE SAME REGULATORY REGIME AS BANK LENDERS.

The relaxation of the restricted payments and investments provisions, which allow cash to be siphoned out of the credit party group, should be viewed in conjunction with the other potential value leaks in the credit facility. This year, J. Crew famously used a trap-door provision in its credit facility to transfer millions of dollars in intellectual property to an unrestricted subsidiary, effectively moving a substantial portion of the collateral that secured such facility away from J. Crew’s lenders. This “J. Crew Trap Door,” as the provision has been dubbed, may be viewed as a cautionary tale toward the borrower-friendly shift in credit agreement provisions.

Furthermore, in the negative covenant provisions, the ability to consummate permitted acquisitions, consistently based on various conditions the borrower must satisfy before consummating any such acquisition, has seen a loosening in the middle market as well. There has been a move away from a general cap on acquisition consideration in larger middle market deals, with the typical approach now being to cap only the consideration with respect to the acquisition of noncredit party subsidiaries (typically comprised of foreign subsidiaries) or, in some deals, doing away with caps altogether and instead relying on a leverage ratio condition.

Also, many of the limitations that previously existed with respect to permitted acquisitions have almost entirely fallen away (including caps on earnouts and a requirement that the target have positive EBITDA). There has also been a continuation of the development of the limited condition acquisition concept.

Limited Condition Acquisition

The limited condition acquisition (LCA) concept has become commonplace in the middle market. The LCA is a permitted acquisition or investment not conditioned on obtaining third-party financing. The concept is tied to incremental loans and whether a permitted acquisition can be consummated. This provision allows the borrower, to the extent it has committed to an acquisition without a financing condition, to elect the date of the acquisition agreement as the relevant date (i.e., the test date) for testing whether the incurrence of debt (including pursuant to the incremental facility) and liens and the taking

of certain other actions (such as investments, restricted payments, asset sales, or fundamental changes) are permitted.

If the borrower makes an LCA election, the measurement of ratios and baskets relating to debt or lien incurrence or the taking of other actions (including consummation of the acquisition), as well as the existence of any default or event of default, until consummation of the acquisition or termination of the acquisition agreement, is determined as of the test date. This concept is akin to the funds certain concept contained in underwritten commitment letters for acquisition financings, and it provides the borrower with certainty when committing to an acquisition that an EBITDA decrease, default, or other adverse event occurring between the date of the acquisition agreement and consummation of the deal will not impair its ability to raise debt under the incremental facility or take other actions if conditions are met on the date of the acquisition agreement. With this concept, the borrower can bid successfully in competitive sale processes with other potential buyers who may be coming to a deal with traditional stand-alone “SunGard” style commitment papers or other offers not subject to a financing condition.

Unitranche Structure


Unitranche facilities have become more common in the middle market and are typically offered by less traditional lenders such as specialty finance companies. The unitranche concept combines first lien and second lien debt (or senior/subordinated debt) into one credit facility that has a blended rate of interest for the borrower. The lien (and payment) priorities between the first lien/second lien or senior/



Related Content

For additional information on all segments of the loan market, see

> [SEGMENTS OF THE LOAN MARKET: INVESTMENT GRADE, LARGE CAP, MIDDLE MARKET AND LEVERAGED FINANCE](#)

 **RESEARCH PATH:** [Finance > Fundamentals of Financing Transactions > Credit Facility Basics > Practice Notes](#)


For more on asset-based lending and leveraged finance, see

> [COMPARING AND CONTRASTING ASSET-BASED LENDING AND LEVERAGED FINANCE](#)

 **RESEARCH PATH:** [Finance > Asset-Based Lending > Introduction to Asset-Based Lending > Practice Notes](#)


For additional details on covenant obligations, see

> [RECENT TRENDS IN COVENANT OBLIGATIONS](#)

 **RESEARCH PATH:** [Finance > The Credit Agreement > Representations, Warranties and Covenants > Practice Notes](#)

For more about financial covenants generally, see

> [FINANCIAL COVENANTS \(CREDIT AGREEMENT\)](#)

 **RESEARCH PATH:** [Finance > The Credit Agreement > Representations, Warranties and Covenants > Practice Notes](#)

subordinated debt are addressed in an agreement among lenders, which the borrower usually acknowledges in writing (but in certain situations may not know exists).

This structure simplifies the financing process by reducing the number of loan documents and therefore may reduce transaction costs for the borrower. However, due to some bankruptcy concerns (e.g., the structure is largely untested in bankruptcy and the first out portion of the unitranche financing may not be entitled to receive post-petition interest if the financing is treated as one class and it is undersecured) and familiarity with the traditional structure, the unitranche concept has some hurdles to clear before it becomes more prevalent in the middle market for traditional bank lenders.

LIBOR Issue

The UK Financial Conduct Authority announced that it will phase out LIBOR by the end of 2021. LIBOR is featured in almost

every credit facility in the middle market. Unfortunately, there is no indication that a replacement rate will be agreed to in the near future.

This uncertainty has caused much debate in the middle market (and other loan markets) on how credit facilities should protect against the possibility that LIBOR cannot be ascertained in the future. The Loan Syndications & Trading Association (LSTA) has suggested an approach in which the agent bank and the borrower would negotiate a new rate, and after determining the new rate, the required (majority) lenders would have a five-business day period in which they could object to the new rate selection.

One alternative to the LSTA approach would be to have the agent bank, the borrower, and the required lenders approve an alternate rate, and during the negotiation period, either all loans convert to base rate or the agent bank could implement a rate that they determine accurately reflects the lenders’ costs of funds. The market has not yet adopted a preferred approach, and it will be interesting to see how lenders adapt to the LIBOR rate uncertainty.

Summary

Lending activity in the middle market is likely to remain strong into 2018. Nontraditional direct lenders are expected to continue gaining market share in the middle market because they are not subject to the same regulatory regime as bank lenders. The flexibility afforded to direct lenders will likely continue the trend of loosening terms, resulting in an even more borrower favorable environment. 

Patrick Yingling is a partner in the Charlotte office of King & Spalding, where he is a member of the firm’s Finance Practice Group. Mr. Yingling’s practice focuses primarily on the representation of lead arrangers and agent banks in connection with the structuring and documentation of syndicated credit facilities, including merger and acquisition-related financings, first and second lien credit facilities, investment grade financings, cross-border facilities, financial sponsor leveraged acquisitions, and asset-based lending. Mr. Yingling has experience with a broad range of industry types including business services, healthcare, media/communications, sports and entertainment, defense, real estate investment trusts, and manufacturing. Aleksandra Kopec is a senior associate in King & Spalding’s Global Finance practice group resident in the Charlotte office. Ms. Kopec is active in King & Spalding’s leveraged finance practice.

 **RESEARCH PATH:** [Finance > Market Trends & Insights > Market Trends > Practice Notes](#)



LexisNexis White Paper Addresses Need for Ethical Sourcing in Electronics Industry

The global electronics industry and the supply chains that support it come under scrutiny in “Ethical Sourcing and Everyday Electronics,” a white paper released by LexisNexis.

“THE GLOBAL ELECTRONICS INDUSTRY THAT PRODUCES our mobile phones, laptops, tablets and many more items we use daily is one of the largest industrial sectors in the global economy, generating more revenue than any other goods-producing sector,” author Jantine Wedermuller von Elgg says. “A part of that revenue is made at the expense of people that are part of the complex electronics supply chains that can comprise multiple tiers, hundreds of supplier locations and thousands of individuals.”

The paper identifies two countries—the Democratic Republic of the Congo (DRC) and Malaysia—as targets by third parties who seek to exploit workers for financial gain, citing the DRC’s “abundance of raw materials,” particularly minerals and metals, and the presence in Malaysia of “more than 5,000 international businesses from 40 countries” that rely on subcontractors and third-party employment agencies for manpower.

The paper notes that the U.S. Department of State’s 2017 Trafficking in Persons Report stated that men, women and children in the DRC are forced to work in artisanal mines and to smuggle materials and are subject to debt bondage, long working hours and abuse. In Malaysia, the paper says, research has shown that “at least a third of migrant workers” in the electronics sector are in forced labor situations.

To combat forced labor and foster ethical sourcing, a number of countries, including the United States, France and the United Kingdom, have adopted guidelines and enacted legislation. In addition, investors and consumers have begun to show awareness and to apply pressure on businesses to mitigate human rights risks.

Furthermore, the paper says, the United Nations Guiding Principles on Business and Human Rights (UNGPs) “provide an authoritative global standard for preventing and addressing the risk of adverse human rights impacts linked to business activity.”

“Ethical sourcing starts with commitment and strong due diligence,” the paper says. “But with more than 50 percent of organizations discovering issues with third parties after their initial due diligence investigations, ongoing risk monitoring is required. A proactive and reactive approach within a business, at the highest level and across departments, and throughout supply chains, will help to comply with regulatory measures as well as to go beyond and improve the situation of people working in supply chains across the world.”

LexisNexis supports the rule of law around the world by:

- Providing products and services that enable customers to excel in the practice and business of law and help justice systems, governments and businesses to function more effectively, efficiently and transparently
- Documenting local, national and international laws and making them accessible in print and online to individuals and professionals in the public and private sectors
- Partnering with governments and non-profit organizations to help make justice systems more efficient and transparent
- Supporting corporate citizenship initiatives that strengthen civil society and the rule of law across the globe

For a copy of the white paper and more information on LexisNexis’ role in supporting the rule of law, visit <http://bis.lexisnexis.com/Everyday-Electronics>.



LexisNexis®

Lexis® for Microsoft® Office

DELIVER BULLETPROOF CONTRACTS

TRUSTED PRACTICAL GUIDANCE AND
PRECISE PROOFREADING TOOLS
RIGHT WITHIN YOUR DOCUMENT

Start your free trial today

LEXISNEXIS.COM/BULLETPROOF
OR CALL 888.285.3947

20

LEGAL DRAFTING
TOOLS



INTEGRATED INTO
WORD & OUTLOOK®

850+

ATTORNEY
AUTHORS

17

PRACTICE AREAS
WITH EXPERT GUIDANCE



LexisNexis®

Lexis Practice Advisor®

START HERE TO GET IT RIGHT

Get off on the right foot in your matters with
effortless navigation to expert guidance.

Try Lexis Practice Advisor® today

[LEXISNEXIS.COM/PRACTICE-ADVISOR](https://www.lexisnexis.com/practice-advisor)

800.628.3612

850+

ATTORNEY
AUTHORS

93%

ATTORNEY AUTHORS
CURRENTLY PRACTICING

320

CONTRIBUTING
LAW FIRMS

*As compared to Thomson Reuters Practical Law network. Comparison data based on information available as of December 2017.

LexisNexis, Lexis Practice Advisor and the Knowledge Burst logo are registered trademarks of RELX Inc. Westlaw is a registered trademark of West Publishing Corporation. © 2017 LexisNexis. PA00211-0 0817