Wall Street LAWYER
Securities in the Electronic Age

August 2019 ▪ Volume 23 ▪ Issue 8

SEC DELIBERATES AND SEEKS INPUT TO EASE ACCESS TO UNREGISTERED OFFERINGS

By Teresa M. Goody & Michelle N. Tanney

Teresa M. Goody is a partner in the Washington, D.C. office of BakerHostetler. She has a broad-based securities and corporate practice that includes SEC investigations, securities litigation, assistance interacting with regulators and the government, and general securities and corporate advice. Michelle N. Tanney is an associate in the firm's New York office. Contact: tgoody@bakerlaw.com

On June 18, the Securities and Exchange Commission ("SEC") requested public comment on the "Harmonization of Securities Offerings Exemptions"—specifically, with regard to certain exemptions from registration under the Securities Act of 1933 ("Securities Act")[1]—with the goal of simplifying the exempt offering framework and expanding investment opportunities.[2]

The move comes following statements made by SEC Chairman Jay Clayton in April 2019 on the lack of investment opportunities for retail investors, particularly with growth companies.[3] With hundreds of companies targeting IPOs in the second half of 2019, U.S. capital markets would likely benefit from a comprehensive review of the framework to expand investment opportunities as the market continues to grow and provide varying ways to participate. Companies may benefit from more options to raise money through private offerings in lieu of public offerings. In addition, providing companies access to capital earlier in their life cycle through exempt offerings may give them the funds necessary to grow to be in a position to access the public markets, and thus may increase the number of IPOs.

The comment period ends on September 24, 2019.

Background

The Securities Act requires that every offer and sale of securities be registered with the SEC, unless an exemption is available. The purpose of registration is to provide investors full and fair disclosure of material information so they may make informed investment decisions.[4] In the past several years, however, Congress recognized that certain situations provide no practical need

IN THIS ISSUE:

THOMSON REUTERS®

42481474

for registration, and has passed legislation that allows for the scope of exempt offerings in an effort to raise capital in exempt offerings and to enhance capital formation.[5]

The Jumpstart Our Business Startups Act of 2012 ("JOBS Act"),[6] the Fixing America's Surface Transportation Act of 2015 ("FAST Act"),[7] and the Economic Growth, Regulatory Relief, and Consumer Protection Act of 2018 ("Economic Growth Act")[8] resulted in revisions to Securities Act registration exemptions. These revisions, however, exacerbated the complex patchwork of the varying, and sometimes overlapping, requirements and conditions. The resulting difficulties presented market participants, particularly smaller companies with more limited resources, with no road map to navigate the exempt offering framework.[9]

On June 18, the SEC provided a concept release to undertake a "broad review of available exemptions to the registration requirements of the federal securities laws that facilitate capital raising," seeking input to assess whether the exempt offering is accessible for both issuers and investors.[10] Specifically, the Commission seeks to: (*i*) determine whether overlapping exemptions create confusion for issuers seeking efficient ways to raise capital; (*ii*) identify gaps that make it difficult to rely on an exemption from registration to raise capital at key stages; and (*iii*) consider whether limitation on who can invest in certain exempt offerings, or the amount that can be invested, provide the appropriate level of investor protection.[11] In doing so, the SEC will determine the necessity to simplify, improve, or harmonize the exempt offering framework.[12]

The Current Framework

The Securities Act contains a number of exemptions to its registration requirements. For example, Section 3 of the Securities Act identifies certain classes of securities exempt from the registration requirements of the Securities Act.[13] While these exemptions are generally based on the characteristics of the securities, some exemptions are based on the transaction and characteristics of the investor, such as those identified in Section 4 of the Securities Act.[14] In *SEC v. Ralston Purina*, the Supreme Court held that the availability of the Section 4(a)(2) exemption, which exempts from registra-

Wall Street Lawyer
West LegalEdcenter
610 Opperman Drive
Eagan, MN 55123

One Year Subscription ● 12 Issues ● $ 1,296.00
(ISSN#: 1095-2985)

tion transactions by an issuer not involving any public offering (also referred to as a "private placement"), "should turn on whether the particular class of persons affected needs the protection of the Act.

An offering to those who are shown to be able to fend for themselves is a transaction 'not involving any public offering.' "[15] The Court's emphasis on the characteristics of the investors bleeds into today's current exempt offering framework, in which "the fewest conditions apply to an offering under an exemption where sales are restricted to accredited investors."[16]

The Request for Comment in Abstract

The amount raised in exempt offerings has increased relative to public registered offerings: in 2018, registered offerings accounted for $1.4 trillion of new capital compared with the nearly double $2.9 trillion raised through exempt offering channels.

Accordingly, the SEC asks a series of questions on the overall exempt offering framework, seeking to improve the regulatory structure. Generally, the Concept Release requests comment on seven topics:[17]

1. *The Exempt Offering Framework*: whether the SEC's exempt offering framework is "consistent, accessible, and effective for both companies and investors or whether the Commission should simplify, improve, or harmonize the exempt offering network."

2. *Capital Raising Exemptions Within the Framework*: whether changes should be made to "improve, harmonize, or streamline capital raising exemptions," such as the private placement exemption and Rule 506 of Regulation D, Regulation A, Rule 504 of Regulation D, the intrastate offering exemptions, and Regulation Crowdfunding.

3. *Potential Gaps in the Framework*: whether there are gaps in the exempt offering framework that may make it difficult—especially for smaller companies—"to rely on an exemption from registration to raise capital at key stages of their business cycle."

4. *Investor Limitations*: "whether limitations on who can invest in certain exempt offerings, or the amount they can invest, provide the appropriate level of investor protection" or pose obstacles to capital formation or investor access to investment opportunities.

5. *Integration*: whether the SEC can and should do more to allow companies to transition from one exempt offering to the next, and ultimately, to a registered public offering "without friction or delay."

6. *Pooled Investment Funds*: whether the SEC should "take steps to facilitate capital formation in exempt offerings through pooled investment funds, including interval funds and other closed-end funds, and whether retail investors should be allowed greater exposure to growth-stage companies through pooled investment funds in light of potential advantages and risks involved in investing through such funds."

7. *Secondary Trading*: whether the SEC should "revise its rules governing exemptions for resales of securities to facilitate capital formation and to promote investor protection by improving secondary market liquidity."

Request for Comment in Detail

Because the overall framework for exempt of-

ferings has changed significantly due to the expansion or revision of certain registration exemptions, the SEC is seeking public comment on whether there are ways to make the exemption framework more consistent and effective in its application. Although there are over 100 different areas the SEC identified for comment, the below highlights some of the more salient issues addressed in the Concept Release.

Accredited Investors

Many companies opt to raise capital through exempt offerings in which only accredited investors are eligible to participate; offerings that are unavailable to non-accredited investors. Generally, for offerings above $1.07 million per year, the disclosure requirements are much more onerous for offerings open to non-accredited investors than offerings limited to accredited investors. An accredited investor is primarily a wealthy individual or entity. Currently, an individual accredited investor is generally one who earns $200,000 per year individually or $300,000 as a married couple, or who has $1,000,000 in assets excluding the primary residence. But strong demand over the past several years to invest in exempt offerings that permit non-accredited investors to participate demonstrates that such investors are indeed very interested in participating in our capital markets. Accordingly, the SEC is requesting comment on whether revisions should be made to the accredited investor definition as it applies to pooled investment funds. Specifically, the SEC requested input on:[18]

- Whether the definition of accredited investor should change, including whether it should be revised to allow individuals to qualify based on measures other than sophistication.
- If the financial threshold requirements for natural persons to qualify as accredited investors should be revised.

This is no longer a market for just wealthy, sophisticated investors. With the rise of social media and other forms of communication, along with online trading platforms for unregistered securities, the information available about exempt securities is more tangible than ever, with investors and the public able to participate at a lower cost than at the time many of the exemptions were created.[19]

Although the SEC opines that there are many reasons why the amount of capital raised in exempt offerings exceeds the amount raised in registered offerings, it cautions that the focus of the concept release is on whether, in light of the increased activity in exempt markets, the current exempt framework is efficient in providing access to capital for a variety of issuers, including small issuers.[20] Historically, many retail investors have been relegated to registered offerings,[21] but many companies need to access capital by unregistered offerings to build their businesses.[22] Additionally, the increased amount raised in exempt offerings relative to registered offerings may leave certain investors with fewer opportunities if public markets were more frequently used.[23] While the current framework permits non-accredited investors limited access to unregistered offerings, in 2018, these investments accounted for less than 1% of investment in all exempt offerings.[24] The SEC asks significant questions that have been the subject of debate for years,[25] as to whether methods other than sophistication and wealth should be used to determine whether an investor can fend for themselves in our capital markets; and, if these are the suitable considerations, whether the levels required are appropriate.

Rule 506 of Regulation D

The intent of Regulation D ("Reg D") is to facilitate capital formation, while protecting investors.[26] Rule 506 of Reg D was adopted as a non-exclusive "safe harbor" under Section 4(a)(2), the private placement exemption.[27] In 2012, the JOBS Act required the SEC to eliminate the prohibition of general solicitation under Rule 506, provided that all purchasers of the securities offered are accredited investors, and the issuer takes steps to verify that the purchasers of securities are accredited investors.[28] Consequently, the SEC adopted Rule 506(c), and retained the safe harbor as Rule 506(b).

With its Concept Release, the SEC is seeking input on:[29]

- Whether changes should be made to Rule 506(b) or 506(c), including whether the requirements for each should be combined into one exemption.
- The importance of allowing non-accredited investors to participate in Rule 506(b) offerings.
- The appropriateness of the information requirements of Reg D, and whether they should be aligned with those of other exempt offerings.
- Whether the SEC should amend Reg D to clarify the meaning of "general solicitation" or "general advertising."
- Whether investment limits should be added for non-accredited investors.
- If non-accredited investors should be allowed to participate in an offering that involves general solicitation, and what information requirements would be appropriate.

Here again, the SEC's questions indicate that it is reevaluating the assumptions underlying the securities laws, with emphasis on the exemptive framework. The historical primary difference between Rules 506(b) and 506(c) is that Rule 506(b) permits up to 35 non-accredited investors to participate. Issuers are required to provide non-accredited investors with significantly more disclosure than nonaccredited investors.

In addition, since the passage of the JOBS Act, Rule 506(c) permits general solicitation. The distinction between these rules, again, seems to hinge on a differentiation between accredited and non-accredited investors, and the additional safeguards to protect non-accredited investors, as the definition of "accredited" evolves.

Rule 504 of Regulation D

According to the SEC, from 2009-2018, 2% of capital raised in Reg D offerings under $5 million was by non-investment companies under Rule 504.[30] Rule 504 provides an exemption from Securities Act registration for offerings of up to $5 million in any 12-month period, although certain issuers are not eligible to rely on this exemption.[31] Ineligible issuers include issuers who already file public reports under the Exchange Act, investment companies, or blank check companies.

The SEC is seeking input on:[32]

- Whether there should be changes, generally, to the Rule 504 exemption.
- Whether the $5 million offering limit should be increased.
- Whether the categories of eligible issuers should be expanded.
- If the offering exemption under Rule 504 is duplicative of Reg A, Tier 1.

Commentators have indicated that the lack of federal preemption of Rule 504 and Tier 1 Reg A offerings significantly limits their practicality, particularly given the complexity and costs associated with complying with all the differing state laws. The SEC would likely be interested in learning why investors choose one exemption over the other. The SEC would also likely appreciate commentators discussing the costs of complying with the regulatory requirements for both rules to understand whether the exemptions, in practice, are sufficiently meeting the capital raising and investor protection purposes of the exemption.

Regulation A

In 2015, the SEC amended Regulation A (Reg A) to provide two tiers of exempt offerings up to $50 million, and in 2018, expanded the eligibility to use Reg A to include issuers subject to ongoing reporting requirements of the Securities Exchange Act of 1934 (the Exchange Act).[33] The SEC is required to review the $50 million limit every two years.

Topics the SEC is seeking input on include, among other things:[34]

- Whether the requirements of Reg A address capital formation and investor protection considerations.
- If the $50 million Tier 2 offering limit should be increased.
- Whether the types of eligible securities issued under Reg A should be expanded.

Tier 2 Reg A offerings are far more common than Tier 1 Reg A offerings. A notable issue with Tier 1 Reg A offerings, as indicated above, is the lack of federal preemption. With regard to Tier 2 offerings, questions about the increase in the $50 million raise limit also suggests whether the $75 million float cap should likewise be considered contemporaneously.

A significant issue has arisen with respect to offerings of digital assets, which are deemed investment contracts (but neither debt nor equity *per se*) and whether those securities are eligible securities for Reg A offerings. The SEC has qualified digital asset token Reg A offerings that were claimed to be neither debt nor equity, but it was not explicit as to how these securities are classified as eligible securities pursuant to Rule 261.[35] In addition, the SEC may be interested in the amount of legal and accounting fees that Reg A issuers pay to qualify this exempt offering, and whether the costs of complying with the regulatory requirements meet the capital raising and investor protection purposes of the exemption.

Intrastate Offerings

Section 3(a)(11) of the Securities Act, or the "intrastate offering exemption," allows for an exemption if the issuer is (1) organized in the state where it is offering securities (2) carries out a significant portion of their business in that state and (3) makes offers and sales only to residents of that state.[36] If an issuer meets this standard, then the offering is not limited in size or the number of investors so long as the entire issue of securities is sold exclusively to residents of the state in question.

The SEC adopted Rule 147 as a "safe harbor" under Section 3(a)(11) to provide objective standards that an issuer can rely on to meet the exemption. The Rule 147 safe harbor is intended to provide assurances that the offering exemption would be used for the purpose of local financing of issuers by investors within the issuer's state or territory.[37] This allows for the Rule to track Congress' intent in enacting Section 3(a)(11).

However, Rule 147A, adopted in 2016, provides alternative means for smaller issuers to raise capital, including through intrastate crowdfunding.[38] The Rule was adopted noting the Commission's exemptive authority under Section 28 of the Securities Act, and is therefore not subject to the statutory limitations of Section 3(a)(11).[39] As a consequence, Rule 147A does not restrict offers, but requires that *sales* be made to residents of the issuer's state. This allows for the Rule to maintain the spirit—but not precise intent—of Rule 3(a)(11) in that residents located in the issuer's state are able to take advantage of the exemption.[40] Additionally, Rule 147A does not require issuers to be incorporated or organized in the same state where the offering occurs, as long as they can demonstrate the "in-state nature" of their business.[41] Accordingly, Rule 147A focuses on sales rather than offers and on where the issuer does business, rather than where it is organized.

The SEC seeks input on:[42]

- The extent to which the intrastate exemptions are being used.
- If Rule 147 and Rule 504 should be eliminated as duplicative of Reg A Tier 1.
- Whether the wording the exemption captures the spirit of Congress' intention when enacting the rules.

The intrastate offering exemption is likely one of the easiest Rules to offend. Offering securities out-of-state is enough to eliminate the ability to rely on an exemption, even if the offering was a good faith mistake. Indeed, because there is no *de minimis* exception to the Rule, issuers may be subject to damages levied by investors. Rule 147A certainly modernized the Rule and made it easier for startups and growth companies to determine the best way to structure their financing.

Regardless of whether the issuer seeks an exemption under 3(a)(11) or seeks refuge under Rule 147A, they must be cognizant of the numerous securities laws still at play. In other words, the exemption does not simplify the entire process. For example, offers transmitted through electronic means (e.g., phone, Internet) must be registered under the Securities Act and, depending on the number of shareholders, may be required to register under the Exchange Act. Additional complexities arise in understanding the resale and transfer limitations of the securities, as the rules applicable to resales depend on the underlying federal exemption of the original sale.

For example, if the intrastate offering is conducted pursuant to Section 3(a)(11), the securities will have to "come to rest" in the state under Rule 147 before the securities may be transferred out of state. But, an intrastate offering that relies on Rule 504 renders the securities "restricted," and subject to the restrictions on transfer provided in the Securities Act.

Regulation Crowdfunding

Title III of the JOBS Act added Section 4(a)(6) to the Securities Act to provide exemption from registration for certain crowdfunding transactions. Generally, crowdfunding is a method of capital raising in which an "entity or individual raises funds via the Internet from a large number of people typically making small individual contributions."[43] Eligible issuers are permitted to raise a maximum aggregate amount of $1.07 million in a 12-month period.[44]

The SEC is seeking comment on:[45]

- If Regulation Crowdfunding should be retained, as is.
- Whether Regulation Crowdfunding's re-

quirements appropriate address capital formation and investor protection considerations.

- If the $1.07 million offering limit should be increased, and if so, would Regulation Crowdfunding overlap with Rule 504 of Reg D?

- If the eligibility requirements for Regulation Crowdfunding should be modified.

Crowdfunding is one of the most innovative recent capital formation tools for small companies and has been particularly instrumental for companies in need bridge capital in their make-or-break moments. Crowdfunding can be used in a variety of ways—whether it allows for requisite inventory in a moment of growth, enables salaries to be paid to make it through a growth period, or some other small, but life-changing period for a company. A frequent concern among crowdfunding issuers is that their capitalization table can become unwieldy and less attractive for larger investors. In addition, while some have requested an increase in the annual offering limit, others have expressed concern of fraud, particularly given the limited disclosure requirements. It is a careful balance between disclosure requirements to protect investors and enabling companies to access capital without it being cost-prohibitive to do so.

Pooled Investment Funds

Pooled investment funds include registered investment companies, business development companies ("BDCs"), and private funds. The SEC has noted that there may be a number of advantages for retail investors investing through a pooled investment fund such as "a diversified portfolio that can reduce risk relative to the risk holding a security of a single issuer."[46] Although registered investment companies and BDCs are deemed accredited investors regardless of the fund's assets, private funds, such as venture capital funds, are not accredited investors unless they qualify under a provision of Rule 501(a).[47] Accordingly, it would be difficult for a non-accredited retail investor to gain access to these exempt offerings.

The SEC has accordingly requested comment on whether, among other things:[48]

- Pooled investment funds are an important source of capital for exempt offerings.

- Recent market trends have affected retail investor access to growth-stage issuers that do not seek to raise capital in the public markets.

- Regulatory provisions or practices, including those promulgated by the SEC, discourage participation by registered investment companies and BDCs in exempt offerings.

- All types of pooled funds should qualify as accredited investors without satisfying quantitative criteria, such as a total assets or investments threshold.

The assessment of pooled investment funds is particularly complex given that it involves regulatory inquiries involving the Securities Act, the Exchange Act, the Investment Company Act of 1940, and the Investment Advisors Act of 1940. This makes clear the SEC's intent of a comprehensive approach to evaluate whether the current framework best meets the capital formation needs of all issuers, and particularly smaller issuers, as well as whether retail investors have adequate investment opportunities in addition to sufficient protections.

Impact

The Concept Release is the first step toward

what will likely be a long journey in changing the rules governing exempt offerings, and who can invest in them. However, the SEC has long been laying the groundwork for this release. For example, in an August 2018 speech, Chairman Clayton discussed private capital raising, acknowledging that there has not yet been a comprehensive review of the exemptive framework "to ensure that the system, as a whole, is rational, accessible, and effective."[49] Referring to the exemption landscape as "elaborate patchwork," Chairman Clayton went on further to note that certain considerations need be made regarding whether current rules that limit who can invest in certain offerings "should be expanded to focus on the sophistication of the investor, the amount of the investment, or other criteria rather than just the wealth of the investor."[50]

Moreover, in this reassessment of, and analysis of assumptions underlying, the exemptions from registration, commentators would be wise to suggest that the SEC expand its scope to include modernization and principle-based rules that are nimble, to accommodate various technological advancements in our financial markets—from blockchain and digital assets to the next innovative technology.

ENDNOTES:

[1]15 U.S.C.A. 77a *et seq.*

[2]U.S. Sec. & Exch. Comm'n, *SEC Seeks Public Comment on Ways to Harmonize Private Securities Offering Exemptions* (June 18, 2019), Press Rel. No. 2019-97, *available at*: https://www.sec.gov/news/press-release/2019-97 (Press Release).

[3]Michelle Fox, CNBC, *SEC Chair Jay Clayton wants big firms to go public earlier so retail investors can get in on the growth* (April 26, 2019), *available at*: https://www.cnbc.com/2019/04/26/sec-chair-jay-clayton-wants-big-companies-to-go-public-earlier.html.

[4]U.S. Sec. & Exch. Comm'n, *Concept Release on Harmonization of Securities Offering Exemptions*, Rel. Nos. 33-10649; 34-86129; IA-5256; IC 33512, at p. 5, *available at*: https://www.sec.gov/rules/concept/2019/33-10649.pdf (Concept Release).

[5]Concept Release at p. 5.

[6]Pub. L. No. 112-106, 126 Stat. 306 (2012) (JOBS Act).

[7]Pub. L. No. 114-94, 129 Stat. 1312 (2015) (FAST Act).

[8]Pub. L. No. 115-174, 132 Stat. 1296 (2018) (Economic Growth Act).

[9]Concept Release at p. 6.

[10]Concept Release at p. 7.

[11]Concept Release at p. 7.

[12]Concept Release at p. 7.

[13]*See* 15 U.S.C.A. 77c.

[14]*See* 15 U.S.C.A. 77d.

[15]346 U.S. 119, 125 (1953).

[16]Concept Release at p. 12.

[17]Press Release.

[18]Concept Release at pp. 54-56.

[19]Concept Release at p. 16.

[20]Concept Release at p. 21.

[21]This remains a priority of the SEC per recent rule changes and guidance. *See, e.g.,* Rel. No. 33-10607 (Feb. 19, 2019); Rel. No. 33-10532 (Aug. 17, 2018).

[22]Concept Release at pp. 21-22. According to the Concept Release, approximately only 13% of households qualify as accredited investors. Concept Release at p. 36.

[23]Concept Release at p. 22.

[24]Concept Release at p. 22.

[25]For example, just last year, a bill was introduced, but not passed by the Senate, to amend the definition of an accredited investor. H.R.1585 Fair Investment Opportunities for Professional Experts Act, *available at*: https://www.congress.gov/bill/115th-congress/house-bill/1585.

[26]Concept Release at p. 63.

[27]*See* U.S. Sec. & Exch. Comm'n, *Revision of*

Certain Exemption From Registration for Transactions Involving Limited Offers and Sales, Rel. No. 33-6389 (Mar. 8, 1982) (the Regulation D Adopting Release).

[28]JOBS Act § 201(a).

[29]Concept Release at pp. 82-83.

[30]Concept Release at p. 116.

[31]Sec. & Exch. Comm'n, *Rule 504 of Regulation D*, *available at*: https://www.sec.gov/fast-answers/answers-rule504.html.

[32]Concept Release at p. 118.

[33]Concept Release at pp. 86-87.

[34]Concept Release at pp. 107-108.

[35]Eligible security for Reg A purposes is defined as "[e]quity securities, debt securities, and securities convertible or exchangeable to equity interests, including any guarantees of such securities, but not including asset-backed securities as such term is defined in Item 1101(c) of Regulation AB." 17 C.F.R. § 230.261(c).

[36]15 U.S.C.A. 77c(a)(11).

[37]Concept Release at p. 121.

[38]Concept Release at p. 121.

[39]Concept Release at p. 121.

[40]Concept Release at p. 122.

[41]Concept Release at p. 122.

[42]Concept Release at pp. 125-126.

[43]Concept Release at p. 127, n. 400.

[44]17 C.F.R. § 227.100(a)(1).

[45]Concept Release at pp. 150-151.

[46]Concept Release at p. 173.

[47]Concept Release at p. 182. Examples are whether the private fund holds total assets in excess of $5 million and is a corporation, and is corporation Massachusetts or similar business trust, or partnership, not formed for the purpose of acquiring the securities offered.

[48]Concept Release at pp. 187-193.

[49]Chairman Jay Clayton, Sec. & Exch. Comm'n, *Remarks on Capital Formation at the Nashville 36|86 Entrepreneurship Festival* (Aug. 29, 2018), *available at*: https://www.sec.gov/news/speech/speech-clayton-082918.

[50]Chairman Jay Clayton Remarks.

WHY COMPLIANCE (STILL) MATTERS

By John F. Savarese, Ralph M. Levene, David B. Anders & Marshall L. Miller

John F. Savarese, Ralph M. Levene, and David B. Anders are all partners in the Litigation Department of Wachtell, Lipton, Rosen & Katz. Marshall L. Miller is of counsel in the firm's Litigation Department. Mr. Savarese is also a member of the Editorial Advisory Board of "Wall Street Lawyer." Contact: JFSavarese@wlrk.com, RMLevene@wlrk.com, or DBAnders@wlrk.com.

We and many other observers have noted the significant drop over the past two years in both the number of white-collar prosecutions and the scale of corporate fines and penalties. In such an environment, companies might be tempted to think that having an effective compliance program is less urgent and less important than in the past. Our experience suggests that succumbing to such temptation would be a mistake. In fact, now is arguably the best time for corporations to continue investing in their compliance programs to ensure they have in place an effective and comprehensive set of compliance policies, procedures, and internal controls.

Four important developments support this view:

First, the Department of Justice ("DOJ") and other law enforcement authorities—through various policy pronouncements and speeches over the past 18 months—have made their white-collar decision-making process more transparent. Law enforcement authorities have clarified what they expect to see in a well-maintained corporate compliance regime and how the presence (or absence) of those elements will be weighed when determin-

ing critical components of corporate resolutions, such as the type of disposition they will seek, the scale and nature of financial penalties, and other remedial measures, including monitors, that may be imposed. Indeed, just last week, DOJ's Antitrust Division announced a new policy that empowers prosecutors, when making charging decisions, to give credit to companies for having effective antitrust compliance programs, noting that the Division "is committed to rewarding corporate efforts to invest in and instill a culture of compliance." Put simply, the "carrot" being offered by law enforcement to encourage compliance and cooperation is bigger than ever, but so is the "stick" used when companies fall short of these governmental expectations.

Second, the record of corporate dispositions over the past two years illustrates the dramatic differences in how the government rewards on the one hand, and punishes on the other, the range of corporate responses to underlying misconduct. For example, in *Cognizant Technology Solutions Corp.* (Feb. 13, 2019), the DOJ declined to take any criminal enforcement action against the company "notwithstanding that the [FCPA] misconduct reached the highest levels of the company," because the company "voluntarily self-disclosed the conduct within two weeks of when the board learned of it," and, as a result, DOJ was able to develop criminal cases against individual executives. Similarly, in *Walmart Inc.* (June 20, 2019), despite an extensive record of wrongdoing and a failure to initially self-report misconduct in a Mexican subsidiary, the Walmart parent was able to secure a non-prosecution agreement.

This result was due in large part to the company's extensive and proactive cooperation, and its adoption of substantial remedial measures, including the hiring of a global chief ethics and compliance officer, with direct reporting to the board's Audit Committee, a wide array of anti-corruption monitoring measures, enhanced internal controls, expanded training and the termination of relationships with third parties involved in corrupt activities.

Conversely, in *Rabobank N.A.* (Feb. 7, 2018), the DOJ insisted upon a corporate guilty plea for Bank Secrecy Act ("BSA") and anti-money laundering ("AML") violations because the bank had implemented a flawed BSA/AML program that precluded appropriate investigation of suspicious transactions, and senior executives actively obstructed an initial Office of the Comptroller of the Currency ("OCC") examination of the bank, submitted false and misleading information about its BSA/AML program, and demoted or terminated employees who were raising questions about the adequacy of the bank's compliance program.

Similarly, though somewhat less dramatically than in the *Rabobank* case, in *HSBC Holding plc* (Jan. 18, 2018), DOJ required a deferred prosecution agreement principally because the bank's initial efforts to cooperate were deficient in several respects and it did not voluntarily and timely disclose the underlying misconduct. And according to recent media reports, the Federal Trade Commission has approved a $5 billion penalty against Facebook for violating a 2012 consent decree that required, among other things, implementation of a comprehensive consumer privacy compliance program.

Third, the DOJ recently issued an extensive memorandum providing guidance regarding its specific expectations concerning corporate compliance programs, cooperation, remediation, and restitution. The guidance highlights that prosecutors may "reward" efforts to improve compliance through a more favorable form of resolution or a

reduced penalty. And in a speech announcing the guidance, the Assistant Attorney General for DOJ's Criminal Division emphasized that implementation of an effective compliance program is a precondition to eligibility for a declination under DOJ's Foreign Corrupt Practices Act ("FCPA") Corporate Enforcement Policy.

The DOJ guidance runs to 18 pages, and we will not try here to summarize all of what it covers. However, in our view, the central takeaways include:

- developing a comprehensive inventory of the legal, regulatory and reputational risks entailed in running the company's various business lines;
- periodically refreshing and updating this inventory as the company's businesses, sales/marketing practices, markets, geographic scope and customer base evolve over time;
- designing a compliance program that is dynamic and carefully tailored to address these evolving risks and that is periodically reassessed and enhanced as necessary, based on up-to-date metrics and data, to take account of material changes in the company's legal, regulatory, and reputational risk profile;
- taking steps to ensure that the company's compliance program is properly "operationalized" at the level of day-to-day business activities where issues often arise, including by making sure that the right "tone at the top" translates into the right "tone on the ground," and instituting well-considered training and educational programs aimed at the right audiences and using the right tools; and
- ensuring adequate board and senior management involvement, both in terms of assuring they are appropriately informed about risks entailed in the enterprise and mitigation measures being deployed to address those risks, and also that the board is given adequate opportunities to pressure test those measures through periodic updates and time for follow-up inquiry.

Fourth, a final reason for continued focus on compliance is that, in recent years, both foreign governments and state attorneys general have become far more active than in the past and now seek more aggressively to bring cases, either alongside U.S. authorities or even in situations where federal authorities have chosen not to act. At the same time, as we explained earlier this year, foreign governments are increasingly adopting corporate dispositions modelled on U.S. Non-Prosecution Agreements ("NPAs") and Deferred-Prosecution Agreements ("DPAs"), and expressly recognize that credit is being given for companies having effective compliance regimes, adopting appropriate remedial measures, and providing substantial, valuable cooperation. Some foreign countries also have enacted affirmative defenses that would exonerate companies able to demonstrate they had a well-designed compliance program at the time of the alleged wrongdoing. Likewise, having put in place a comprehensive and well-designed compliance program will redound to any company's benefit when responding to a state attorney general investigation.

For all of these reasons, it is wise to invest in designing, implementing, and periodically refreshing and reorienting a robust compliance program. In our experience, effective compliance programs provide a real opportunity to prevent misconduct from arising in the first place or nipping potential legal and compliance issues in the bud before they

blossom into a full-blown corporate crisis. And should misconduct occur, an effective compliance program that enables early detection and timely remediation of misconduct will best position a company to achieve a more favorable resolution at the close of any resulting investigation.

DIGITIZED SECURITIES AND THE PROMISE OF AUTOMATED COMPLIANCE

By David J. Kappos, D. Scott Bennett, Michael E. Mariani, Jeffrey M. Amico, Christopher Pallotta, Vincent Molinari, Annemarie Tierney & Peter Chiaro

David J. Kappos, one of the foremost leaders in the field of intellectual property, is a corporate partner at Cravath. D. Scott Bennett, a corporate partner at Cravath, focuses on representing issuers and investment banking firms in connection with securities offerings. Michael E. Mariani is a corporate partner at Cravath whose practice focuses on representing companies and investment banks. Jeffrey M. Amico is Legal Counsel at Fluidity Factora and was formerly a corporate associate at Cravath. Christopher Pallotta is the Co-founder and CEO of Templum and the Managing Director at Raptor Group overseeing a portfolio of investments in technology, financial services, media, and sports sectors. Vincent Molinari is the Co-founder of Templum, Inc., and the CEO of its subsidiary, Templum Markets. Annemarie Tierney is the Head of Strategy and General Counsel of Templum Inc. Peter Chiaro is a Senior Associate with Templum.

[This article is based on a larger white paper, available at https://tmsnrt.rs/2LSGlCC.]

A digitized security is a digital representation of a security that can be programmed to automate certain functions and whose ownership is traced in real time using a distributed ledger.[1] The first generation of digitized securities being issued today are effectively traditional securities enveloped in a digital wrapper. That should not suggest that their potential impact is limited, however. As in the shift from "snail mail" to email, the content of the underlying information does not change. However, like email, digitization offers significant advantages over the legacy paper-based system.

Among the most promising of these advantages is the potential to use smart contracts to automate compliance with certain aspects of securities law. Using a digitized security, an issuer could write certain transfer restrictions directly into the code of the smart contract, effectively enshrining certain key securities law requirements like holding periods or shareholder caps directly into the security itself. Done properly, this could provide both issuers and regulators with assurance that applicable laws were being complied with, while also eliminating certain transactional frictions that make it difficult for investors to trade on secondary markets.

In the near term, this technology likely offers the greatest value to secondary markets for securities of private companies, as many of the applicable registration exemptions that are administratively burdensome to comply with could be rendered in code and enforced automatically.[2] The value of a digitized security in this context over the status quo is that these compliance checks would be enforced *automatically* upon any transfer, and without requiring any post-trade intervention or reconciliation to ensure compliance and track ownership. This is possible because distributed ledgers allow the various entities necessary to effect a securities transaction (e.g., brokers, exchanges, custodians) to all share a common, programmable data layer. This marks a step-function change over the status quo in the markets for private securities, where there is currently a significant lack of infrastructure to facilitate legally compliant secondary trading at

scale. Over the longer term, distributed ledgers may also gain adoption in public capital markets as well, streamlining not only settlement processes but other heavily intermediated functions like distributing cash flows and managing shareholder voting as well. Ultimately, digitized securities may not be the panacea for private market liquidity issues that some advocates claim. However, they can offer real benefits to private market issuers and investors, as the status quo simply remains too inefficient and cumbersome as we move into the digital age of financial markets.

This paper proceeds as follows. First, it provides an overview of distributed ledger systems at a high level, including their potential benefits as compared to existing technologies. Second, it summarizes the basic framework that governs securities offerings in the United States, as well as the administrative burdens that smaller private companies must bear in order to comply with this regime. Third, it examines specifically how and where smart contracts could be used to automate compliance with certain of these securities law requirements, thereby reducing a major barrier to secondary liquidity in private markets. Finally, it concludes by analyzing certain obstacles that must be overcome in order for this technology to gain widespread adoption and considers which existing solutions are most likely to generate widespread adoption.

An Overview of Distributed Ledger Systems

Key Concepts

A digitized security is a digital representation of a security that exists on a distributed ledger. A distributed ledger is a system that enables independent participants to reach consensus on the validity of a set of shared data in the absence of a central coordinator.[3] The product of this consensus is a shared, append-only "ledger" (resembling a computer log file) that is constantly updated to reflect the addition of new data. Distributed ledgers can either be public or private, depending on which participants are permitted to execute and validate transactions.

A blockchain is a particular type of distributed ledger in which data (e.g., transactions) is grouped into blocks and then chained together in chronological order using a cryptographic mechanism known as a hash function. The process of chaining one block to the next creates a virtually irreversible record of all transactions that can be referenced in the future to prevent users from double-spending their digital assets.

While the original and most common vision of blockchain is of a fully public, decentralized, permissionless network, there are a wide variety of blockchain solutions, many of which are, in fact, either fully or partly private and/or require permission to join.[4] In contrast with public, permissionless networks, private, permissioned blockchains employ various processes to approve new participants, including to ensure all new participants subscribe to a set of rules that govern their use of the network. One significant difference between public and private blockchains is the existence of a central intermediary. In a public blockchain—i.e., a true distributed ledger—there is no central authority and the decision on whether a new block should be added to the chain is vested with the consensus of the blockchain community, whereas in a private blockchain, central intermediaries may be necessary. Therefore, in a true private blockchain with only one central participant, the technology becomes more similar to a traditional private database. There are also hybrid solutions where the right to read the chain might be public but the

transaction/data authorization process is controlled by a pre-selected set of nodes; for example, a consortium of 15 exchange institutions, each of which operates a node, where 10 of them must sign every block in order for the block to be valid.

Because anyone can join and add a new block to a public, permissionless blockchain, it is impossible to ensure participants agree to a set of rules, except to the extent the rules are built into the code of the blockchain. However, in a private, permissioned blockchain or a hybrid solution, it is possible to limit the parties who can transact on the blockchain according to certain rules implemented within the protocol. Another distinction between public and private blockchains is that a public blockchain is immutable, whereas private blockchains may have more flexibility for risk depending on the perspective for changes in the blockchain.

Certain distributed ledgers also allow users to embed computer scripts into the ledger that will be executed automatically by the nodes running the ledger if the conditions specified in the script are satisfied. These scripts are known as smart contracts.

Smart contracts can be designed to create digitized securities (which are digital representations of value) and enable their transfer between users. As noted, smart contracts are effectively computer programs that will be run by the network if and when the embedded conditional logic is satisfied. After the contract has been deployed by the creator, other users may interact with it to achieve a desired outcome. For example, a basic "multi-signature" smart contract would allow a transfer from one individual to another only if a requisite number of participants sign and approve the transaction. Other basic examples could include smart contracts that only allow transfers up to a spending cap, or only within certain time periods, or only to pre-approved persons, such as accredited or institutional investor accounts.

The Capital Markets Use Case

At its core, a public blockchain is a record-keeping system with no central administrator. In a private, permissioned blockchain, however, the degree of decentralization is based on how the members running the private blockchain choose to structure their business relationships; there can be a central administrator, or a consortium of members who administer the blockchain. Though blockchains can be used to store other forms of data (e.g., identity-based information), their primary use case to date has been to track ownership of assets and facilitate their transfer between users. Public blockchains of this variety (e.g., Bitcoin) can be thought of as peer-to-peer asset registries. Public blockchains with more advanced scripting languages (e.g., Ethereum) as well as certain private blockchain solutions (e.g., Symbiont) take on a more active role, serving as both the asset registry *and* the computer that actually executes the transactions.

As noted, the unique innovation of public blockchains over existing database technologies is that a blockchain is designed to serve these functions without a central administrator. If we think of blockchains as open-source record-keeping systems that can be programmed like computers, it becomes possible to envision an entire ecosystem of applications being built on and sharing a common data layer. For example, imagine that the various entities necessary to effect a securities transaction today (e.g., exchanges, brokers, custodians) could all share a single set of records, instead of maintaining (and reconciling) their own respective ledgers on a daily basis. Imagine further that this shared settlement layer could be programmed by

an issuer to automate certain functions like regulatory compliance or cash flow distributions, and that these functions would execute automatically as programmed. The same example can also be implemented on a private, permissioned or hybrid blockchain protocol, where the governance rules implemented by exchanges or custodians serving as nodes can ensure more structured and efficient transfer of information and recording of transactions.

This notion of a shared data layer is significant in the capital markets context because it produces an agreed-upon record of who owns a particular security at any moment, updated in real time, *regardless* of the particular venue or medium through which a transaction occurred. In other words, in theory, it becomes irrelevant if the buyer and seller connect via a regulated (e.g., a traditional public exchange or an alternative trading system) or unregulated (e.g., a message board or even in person) trading venue. As long as the seller sends the token from her blockchain address to the buyer's blockchain address, that transfer will ping the digitized security's smart contract (ensuring the trade complies with any transfer restrictions) and will be logged into the ledger, updating the ownership records instantly. This technology could potentially eliminate the need for certain existing intermediaries (e.g., transfer agents, custodians) whose job it is to store securities on others' behalf and enable their transfer between holders. Indeed, blockchains could enable a more direct, straight-through relationship between the issuer and its security holders throughout the life cycle of the security. However, the implementation of this functionality for public blockchain-based digitized securities, as well as the related regulatory environment, is still developing.

To understand why this vision is important, it is helpful to draw a contrast with the settlement infrastructure in today's capital markets. In the United States public markets, the Depository Trust Company ("DTC") provides this "asset registry" service, keeping what is effectively the master record of who owns which securities on a daily basis. However, where the system described above is automated, programmable, instantaneous and—in trades with a discrete buyer and seller—peer-to-peer, today's process is manual and heavily intermediated. Most trades today are not settled near-instantaneously, but rather take two or more business days before ownership is officially transferred. This is, in part, due to the fact that (unlike the system described above), brokerages must affirmatively report all of their clients' trades to DTC, which in turn must manually update its ledger. Even further complicating the process is the fact that DTC does not track the *actual* beneficial owners of the securities it processes. Instead, it tracks ownership as between its "participants" (which include brokerages and other financial intermediaries), who in turn keep track of the beneficial owners (e.g., their clients). The brokerages then need to manually reconcile their individual records with each other to ensure their respective ledgers match.

As complex and inefficient as this system is, it is still superior to the status quo in the private markets, where no such recordation infrastructure exists at all. While some private placement trading platforms do exist, secondary trading in securities of private issuers generally relies on an ad hoc system in which issuers maintain spreadsheets tracking their security holders. Notwithstanding that today there are certain market participants who help issuers manage their capitalization tables in a digitized framework, given that issuers must keep the list current, they will usually require holders to seek their permission prior to any secondary

trading. Suffice it to say, this system is not built to handle legally compliant secondary trading on any significant scale. It is slow, error-prone, and lacks any programmable functionality. While there are many reasons why most private securities are illiquid, the transactional frictions inherent to this system are likely a contributing factor. Blockchains may offer a way to reduce certain of these frictions. Not only can they provide a real-time audit trail of a security's ownership, they can be programmed to automate key functions necessary to facilitate secondary trading, including complying with securities laws.

Automated Compliance

Virtually any asset in the world can be represented as a digitized security and traded on a distributed ledger, including a traditional security. As mentioned, the process of digitizing a security makes it "programmable," meaning it can interact with smart contracts to automatically execute certain key functions. One of the most promising near-term applications of this technology involves coding transfer restrictions directly into the smart contract to automate compliance with certain key securities laws and an issuer's specific transfer restrictions. Done properly, this would ensure that any attempted secondary transfer of the digitized security that does not comply with the applicable rule set will not execute.

There are various open-source protocols being designed today to allow issuers to implement this vision. One option is a private, permissioned blockchain for unregistered securities transactions. Like open-source protocols, private blockchains can establish a standardized digitized security framework to allow more sophisticated transfer restrictions to be built directly into a smart contract. However, unlike public, open-source protocols, private blockchains provide issuers and investors, as well as regulators, with more certainty that transactions will occur securely, and that all participants are authorized to conduct the transaction due to their ability to decide on the rules of the blockchain protocol. Another option is public decentralized protocols (ERC including ERC-1400 and ERC-1404 for tokens issued on the Ethereum blockchain) that have a wider adoption rate due to their public nature and straightforward coding language.

Although public and private blockchains have their differences, both of these solutions aim to provide uniform standards to allow more complex regulatory restrictions in smart contracts. Prior to launch, an issuer would follow one of these protocols to write the security's smart contract in a way that imported the applicable regulatory requirements. Once the digitized security was issued, any subsequent transfer attempts would ping the digitized security's smart contract. If the necessary conditions were satisfied, the digitized security would be automatically transferred. If not, the transfer would be blocked, and a message would be delivered explaining which condition was not satisfied. Using this technology, issuers can ensure they remain in compliance with certain key rules while also removing certain costly barriers that impede investors' ability to trade.

Overview of Key U.S. Securities Laws

Basic Framework Governing Primary Offerings of Securities

To understand specifically how and where this technology may add value, it is necessary to first provide a basic understanding of the laws governing securities offerings in the United States. The Securities Act of 1933 (the Securities Act) and the Securities Exchange Act of 1934 (the Exchange Act) together serve as the foundation of U.S. secu-

rities law. At a high level, the Securities Act requires an issuer of securities to either file a registration statement with the Securities and Exchange Commission ("SEC") (including a prospectus that describes the issuer's business and the securities being offered) or conduct the offering in a way that qualifies for a specific exemption from registration. If the offering is registered, the issuer will generally then become subject to the ongoing reporting requirements and other disclosure obligations set forth in the Exchange Act. These obligations include filing annual, quarterly, and current reports with the SEC and delivering annual proxy statements to investors that disclose, among other things, audited and unaudited financial statements and executive compensation. While recent amendments under the JOBS Act have scaled down certain of the reporting obligations for "emerging growth companies," the compliance burden can still be onerous. Companies who want to avoid these obligations but still want access to the financing options offered by capital markets can conduct their offering in a way that qualifies for a registration exemption.

Costs of Compliance (and Non-Compliance) in Secondary Markets

While qualifying for a registration exemption can be fairly straightforward at the time of issuance, remaining in compliance while also facilitating secondary trading imposes a significant administrative burden on issuers (and particularly smaller issuers). It requires them to track certain information regarding their security holders at all times, including quantity, location, accreditation status, and holding periods. For many companies, this is done in one of two ways: (*i*) in a manual, error-prone fashion, often via internal spreadsheets and paper contracts; or (*ii*) not at all. However, the cost of violating these rules can be severe for non-reporting issuers. For example, if (in the course of secondary trading) the number of security holders of a class of an issuer's equity securities rises above 500 non-accredited or 2,000 total investors (and the issuer has more than $10 million in assets), the issuer will be forced to begin reporting as a public company.

To avoid this fate, most issuers of private securities will actively take precautions that impede secondary liquidity, such as requiring a transfer agent to remove restrictive legends, or legal counsel to provide opinions affirming compliance, or even contractually forbidding secondary sales altogether. And even where issuers take these precautions, it is still possible for the securities to be traded (in contravention of the restrictive legend) without the issuer's knowledge. These barriers combine with other market forces to collectively render most private securities illiquid, which is impounded into their price via an "illiquidity discount."[5] Many issuers view this discount as a necessary cost to ensure regulatory compliance.

Conclusion

The digitized security space is undoubtedly in its infancy. There are significant layers of infrastructure that still need to be built out before the vision articulated in this paper can be realized. Neither issuers nor institutional investors will embrace digitized securities unless the technology adds tangible value over the status quo. In the public capital markets, the settlement infrastructure that facilitates secondary trading is convoluted and slow by the standards of today's technology age. However, it is still a mostly reliable system, and is therefore likely to persist until blockchains see significant improvements in transaction throughput and security. The status quo in the private capital markets, on the other hand, is one with virtually no infrastructure to facilitate legally compliant sec-

ondary trading on any significant scale. Blockchains can therefore add real, near-term value on the private market side, serving as the "smart" settlement system that tracks ownership in real time and automates functions like compliance across trading venues.

Indeed, despite the industry's nascent stage, several companies have already begun experimenting with and implementing this vision.[6] This first generation of digitized securities have been launched by private issuers (primarily in the real estate space) looking for an efficient way to raise low-cost capital from a potentially global base of investors. On the investor side, these offerings provide access to assets (e.g., commercial real estate projects) that many smaller investors have traditionally been priced out of, while also enabling secondary liquidity on the back end. As the industry continues to mature, more established market participants may begin to notice this emerging technology and the potential it has to transform today's capital markets.

ENDNOTES:

[1]The lexicon of distributed ledger technology is in flux as the technology itself, and the terminology in the space, continues to evolve. We refer to "digitized securities" for consistency; "smart securities" and "security tokens" are alternative phrases used to describe the same, or similar, applications of this technology.

[2]This technology is especially apt for asset classes that have traditionally experienced low liquidity levels, such as private real estate investment trusts or limited partnership interests.

[3]Rauchs, et al., *Distributed Ledger Technology Systems: A Conceptual Framework* (2018), https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2018-08-20-conceptualising-dlt-systems.pdf.

[4]The public-private distinction refers to who can access the blockchain in any capacity, as public blockchains are open to all, while private blockchains are open only to pre-approved members. The permissioned/permissionless distinction refers to who can add data (commonly in the form of submitting transactions and executing smart contracts) to the blockchain, as permissioned blockchains restrict this right to approved members, while permissionless blockchains allow all members to add data.

[5]Damodoran, *The Cost of Illiquidity*, http://people.stern.nyu.edu/adamodar/pdfiles/country/ illiquidity.pdf.

[6]See for example, *Templum Markets Launches Digital Security Offering of St. Regis Aspen Resort*, BUSINESS WIRE (Aug. 8, 2018, 12:00 PM), https://www.businesswire.com/news/home/20180808005549/en/Templum-Markets-Launches-Digital-Security-Offering-St; Alois, *tZero Distributes Security Token to Investors, Plans Secondary Trading*, CROWDFUND INSIDER (Oct. 16, 2018, 10:20 AM), https://www.crowdfundinsider.com/2018/10/140167-tzero-distributes-security-token-to-investors-plans-secondary-trading; Fries, *Real Estate Security Token "Factor-805" Released, Brings DAI To Digital Securities*, THE TOKENIST (Feb. 25, 2019), https://thetokenist.io/real-estate-security-token-factor-805-released-brings-dai-to-digital-securities; Baydakova, *French Lender Societe Generale Issues $112 Million Bond on Ethereum*, COINDESK (Apr. 23, 2019, 8:53 PM), https://www.coindesk.com/french-lender-societe-generale-issues-112-million-bond-on-ethereum.

NEW YORK PASSES EXPANSIVE NEW CYBERSECURITY LAW

By Jonathan S. Kolodner, Rahul Mukhi & Russell A. Mawn, Jr.

Jonathan S. Kolodner is a partner at Cleary Gottlieb Steen & Hamilton and his practice focuses on white-collar criminal enforcement and regulatory matters as well as complex commercial litigation. Rahul Mukhi is also a partner and his practice focuses on criminal, securities, and other enforce-

ment and regulatory matters as well as on complex commercial litigation. Russell A. Mawn, Jr. is an associate at the firm Contact: jkolodner@cgsh.com or rmukhi@cgsh.com.

On July 25, 2019, New York Governor Andrew Cuomo signed into law the Stop Hacks and Improve Electronic Data Security Act (the "SHIELD Act" or the "Act"), which expands data breach notification obligations under New York law and for the first time imposes affirmative cybersecurity obligations on covered entities.

The Act makes five principal changes to existing New York law:

1. Expanding the law's jurisdiction to entities that maintain private information of New York residents, regardless of whether or not such entities actually conduct business within the State;

2. Broadening the scope of "private information" triggering notification obligations in the event of a breach, including to biometric data;

3. Expanding the definition of a "breach" to include unauthorized "access" to private information, in addition to unauthorized "acquisition" of such information;

4. Increasing civil penalties for violations of notification obligations; and

5. For the first time, affirmatively requiring covered businesses to develop, implement, and maintain "reasonable" data security safeguards, which include, among other things, conducting risk assessments and addressing identified risks.

The first four provisions go into effect on October 23, 2019, while the fifth provision requiring companies to adopt and maintain a cybersecurity compliance program becomes effective on March 21, 2020.

Expanded Definition of Covered Entities

The SHIELD Act[1] removes the requirement that in order to be covered by the law a person or business must do business in New York. The law currently in effect applies to a person or business "which (*i*) conducts business in New York state, and (*ii*) which owns or licenses computerized data which includes private information." By eliminating the first requirement, the law will now apply to all persons or companies that "own or license" the private information of New York residents, regardless of the location of the company's business activities.

Consistent with the exterritorial trend in data security and privacy laws exemplified by the European Union's General Data Protection Regulation ("GDPR") and California's Consumer Privacy Act ("CCPA"), the Act will cover businesses that operate outside of New York (or even outside of the United States), if such entities maintain private information of New York consumers, employees, or other residents.

Expanded Definition of "Private Information"

Since 2005, New York has required entities that suffer a breach of "private information" of New York residents to notify affected individuals, New York authorities, and, where the breach affects more than 5,000 people, consumer reporting agencies. Prior to the passage of the Act, "private information" has been defined as "personal information"—"any information concerning a natural person which, because of name, number, and personal mark, or other identifier, can be used to identify such natural person"—in combination with one of the following: (*i*) social security num-

ber; (*ii*) driver's license number or non-driver identification number; or (*iii*) account number or credit or debit card number, with a password or code that would allow access to a financial account.

The SHIELD Act adds fourth and fifth data elements that trigger notification obligations in combination with "personal information": (*iv*) an account number or credit or debit card number if it provides access to a financial account without a password or access code and (*v*) biometric information.[2] In addition, the Act adds notification obligations upon a breach where the information obtained includes "a username or e-mail address in combination with a password or security question and answer that would permit access to an online account." Notification of a breach of this type involving email/username information is triggered *whether or not in combination with "personal information."*

In expanding the categories of information triggering data breach notification obligations to include email/username information alone, New York is now in line with certain other states that have included the same protections in their own breach notification laws such as California, Florida, and Illinois, among others.

Expanded Definition of a Breach

In further broadening the scope of the law, the Act amends the definition of a "breach of the security of the system," from "unauthorized acquisition" to "unauthorized access to or acquisition of" private information. Cybersecurity incidents can often involve unauthorized actors only gaining access to systems and private information, without actually acquiring such information, either because a company's defenses prevent such acquisition, or the hacker does not seek to acquire the information at that time. Under the Act's new definition of breach, evidence of exfiltration is no longer needed to trigger notification obligations. The Act elaborates that, in "determining whether information has been accessed," a company may consider "indications that the information was viewed, communicated with, used, or altered."[3]

Increased Civil Monetary Penalties for Violation of Notification Obligations

Previously, New York law provided for civil penalties of the greater of $5,000 for a violation of the notification obligations, or $10 per instance of failed notification, with the latter amount being capped at $150,000. The Act retains the $5,000 minimum penalty, but doubles the penalty per failed notification to $20, with a correspondingly greater cap of $250,000.

As before, these penalties apply to a person or business that violates the law "knowingly or recklessly."

Additionally, the Act increases the statute of limitations for violations, giving the Attorney General three years, rather than two, to bring an enforcement action against the company, measured from the date of discovery by the Attorney General or notification by the company, whichever is earlier. The Act includes a statute of repose prohibiting any action six years "from the date of discovery of the breach by the company unless the company took steps to hide the breach."

Affirmative Data Security Requirements

Perhaps most notably, the SHIELD Act for the first time imposes an affirmative duty on companies to develop, implement, and maintain "reasonable safeguards" for computerized data which includes private information of New York residents.

The Act elaborates the data security measures that "shall" deem a company in compliance with

the "reasonable safeguards" requirement, which include "administrative safeguards," "technical safeguards," and "physical safeguards." The Act identifies risk assessments, training, and selecting appropriate service providers as among the reasonable safeguards to ensure compliance with the Act:

Administrative Safeguards	(1) designates one or more employees to coordinate the security program; (2) identifies reasonably foreseeable internal and external risks; (3) assesses the sufficiency of safeguards in place to control the identified risks; (4) trains and manages employees in the security program practices and procedures; (5) selects service providers capable of maintaining appropriate safeguards, and requires those safeguards by contract; and (6) adjusts the security program in light of business changes or new circumstances.
Technical Safeguards	(1) assesses risks in network and software design; (2) assesses risks in information processing, transmission and storage; (3) detects, prevents and responds to attacks or system failures; and (4) regularly tests and monitors the effectiveness of key controls, systems and procedures.
Physical Safeguards	(1) assesses risks of information storage and disposal; (2) detects, prevents and responds to intrusions; (3) protects against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information; and (4) disposes of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed.

The Act's apparent intention is to provide the above-listed measures as examples of the respective safeguards to ensure compliance with the Act, but there is potential uncertainty over the amount of flexibility that New York regulators will provide to companies in deviating from the specific compliance provisions set forth in the statute.

For violations, the New York Attorney General is empowered to enforce the Act's reasonable safeguards provisions with penalties not to exceed $5,000 "for each violation," although the law does not clarify what constitutes a "violation" for purposes of imposition of a fine. The law is explicit in stating that "[n]othing in this section shall create a private right of action."

The "reasonable safeguards" requirements exempts certain businesses from compliance: (*i*) "small businesses," defined as those with fewer than 50 employees, less than $3 million in gross annual revenue for three fiscal years, or less than $5 million in year-end assets;[4] and (*ii*) businesses in the financial and healthcare industries that are regulated by and compliant with the Gramm-Leach-Bliley Act, New York DFS' cybersecurity regulations (23 NYCRR 500), the HIPAA Act, or the HITECH Act. The Act also includes a catchall exemption for companies regulated by and compliant with "any other data security rules and regulations" at the federal or New York state level. All other companies that own or license private information of New York residents will need to be compliant with the law by March 21, 2020.

Conclusion

Taken as a whole, the SHIELD Act represents a major step in expanding New York data breach

obligations and security requirements for companies that obtain or license the data of New York residents. Most importantly, companies that collect private information of New York consumers, employees, or other residents must now develop, implement, and maintain reasonable safeguards to protect such information.

The law is specific in identifying certain measures to ensure compliance, many of which are in line with current best practices for mitigating cybersecurity risk, including, among others:

- designating responsible personnel;
- conducting risk assessments;
- training employees;
- conducting due diligence and imposing contractual safeguards requirements on vendors;
- deleting data no longer needed for business purposes, and
- regularly testing key processes and controls.

Time will tell how aggressive New York authorities will be in enforcing these obligations in the absence of a breach. However, given that for almost every company it is only a matter of time before the next breach occurs, businesses should expect that there will be ample opportunity for vigorous enforcement and plan accordingly.

ENDNOTES:

[1]The new law is available here: https://legislation.nysenate.gov/pdf/bills/2019/S5575B.

[2]Biometric information is defined as "data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity."

[3]In another new provision, the Act provides that individuals do not have to be notified if their data was exposed unintentionally to someone authorized to access their private information, as long as the information is not expected to be misused by that person or cause financial or emotional harm to the individual. Companies will still have to document such an event and keep records of it for five years. If such an incident involves the information of more than 500 residents in New York, the person or company will be required to provide a written determination to the state Attorney General's Office within 10 days of determining whether notification is necessary or not.

[4]Small businesses are required to implement "safeguards that are appropriate for the size and complexity of the small business, the nature and scope of the small business's activities, and the sensitivity of the personal information the small business collects from or about consumers."

SEC/SRO UPDATE:

SEC ANNOUNCES SEVERAL CHANGES IN CHAIRMAN'S EXECUTIVE STAFF; ALLISON HERREN LEE SWORN IN AS SEC COMMISSIONER; SEC STAFF PUBLISHES STATEMENT ON MANAGING TRANSITION AWAY FROM LIBOR

By Peter H. Schwartz & Laura Pflumm Cerezo

Peter H. Schwartz is a partner and Laura Pflumm Cerezo is an associate in the law firm of Davis Graham & Stubbs LLP in Denver, Colo. The authors thank Sandra Wainer, a paralegal at Davis Graham, for her assistance in preparing this article. Contact: peter.schwartz@dgslaw.com or laura.cerezo@dgslaw.com.

SEC Announces Several Changes in Chairman's Executive Staff

On June 26, the Securities and Exchange Commission ("SEC") announced several changes in the executive staff of Chairman Jay Clayton, including:

- the departure of Chief of Staff Lucas Moskowitz;[1]
- the appointment of Sean Memon as the new Chief of Staff;[2] and
- the appointment of Bryan Wood as the new Deputy Chief of Staff.[3]

The SEC also released a full roster of the executive staff as of June 2019.[4]

Moskowitz will leave the agency in early August after serving in various roles in the federal government for nearly a decade, including more than five years at the SEC. He was named Chief of Staff by Chairman Clayton in May 2017. In that role, Moskowitz served as Chairman Clayton's lead advisor and worked together with Commission staff on a broad range of matters including rulemaking and policy, enforcement, strategy, personnel, management, operations, communications, legislative affairs, and coordination with state and federal regulatory agencies. Moskowitz will return to the private sector.

Prior to his appointment as Chief of Staff, Memon served as the SEC's Deputy Chief of Staff since May 2017. In that capacity, Memon served as a senior advisor to Chairman Clayton on legal, policy and management matters affecting all aspects of the agency's mission, including rulemaking, enforcement, examinations, and internal agency operations. He also worked with cross-divisional teams within the SEC, and with other state and federal agencies, to coordinate policy responses to market and legal developments.

Wood, before being appointed at Deputy Chief of Staff, served as the Director of the Office of Legislative and Intergovernmental Affairs ("OLIA") since June 2017, where he served as the agency's primary congressional liaison and provided advice to the Chairman, Commissioners, and SEC staff on legislative, policy, strategic, and operational matters. During his tenure as OLIA Director, Wood managed the agency's congressional engagement, including the appropriations process, legislative amendments to the federal securities laws, and congressional testimony, advised on rulemakings implementing congressional mandates, and aided four Commissioner nominees in Senate confirmations. Wood also coordinated interactions with other government agencies and serves as the Chairman's deputy on the Federal Housing Finance Oversight Board and the Financial Stability Oversight Board.

Allison Herren Lee Sworn in as SEC Commissioner

On July 9, Allison Herren Lee was sworn into office as a Commissioner of the SEC.[5] Commissioner Lee was nominated by President Donald J. Trump and, as a Democrat, fills a commissioner seat left open by the departure of Commissioner Kara Stein in January 2019. Commissioner Lee's addition brings the SEC back to a full five-member Commission as she joins fellow Commissioners Robert Jackson, Hester Peirce, Elad Roisman, and Chairman Jay Clayton.

Commissioner Lee has more than two decades of experience as a securities law practitioner, serving in the SEC from 2005-2018 in various roles, including senior counsel in the Complex Financial Instruments Unit and as counsel to former Commissioner Kara Stein.[6] Most recently, Lee wrote, lectured, and taught courses internationally in Spain and Italy on financial regulation and corpo-

rate law. Prior to her government service, Lee spent seven years in private practice focusing on antitrust, securities, and commercial litigation. Commissioner Lee's term expires in June 2022.

SEC Staff Publishes Statement on Managing Transition Away From LIBOR

On July 12, the SEC announced that its Staff had published a statement encouraging market participants to proactively manage the transition away from London Interbank Offered Rate ("LIBOR") and outlined several potential areas that may warrant increased attention during that time.[7] According to the press release, it is expected that parties reporting information used to set LIBOR will stop doing so after 2021.

The Staff's statement encourages market participants to:

- identify existing contracts that extend past 2021 to determine their exposure to LIBOR; and
- consider whether contracts entered into in the future should reference an alternative rate to LIBOR or include effective fallback language.

The statement also contains specific guidance for how registrants might respond to risks associated with the discontinuation of LIBOR.

According to the press release, because "LIBOR is used extensively in the U.S. and globally as a benchmark rate to set interest rates for various commercial and financial contracts, the discontinuation of LIBOR could have a significant impact on financial markets and may present a material risk for market participants, including public companies, investment advisers, investment companies, and broker-dealers." The press release also asserted that these risks will be exacerbated if the work necessary to effect an orderly transition to an alternative reference rate is not completed in a timely manner.

The Staff has stated that it will continue to actively monitor the extent to which market participants are identifying and addressing risks associated with the expected discontinuation of LIBOR, and that it welcomes discussion on the transition and encourages members of the public to share information about the potential impact of the expected discontinuation of LIBOR.

ENDNOTES:

[1]*See* SEC Press Rel. No. 2019-108 (June 26, 2019), *available at* https://www.sec.gov/news/press-release/2019-108.

[2]*See* SEC Press Rel. No. 2019-109 (June 26, 2019), *available at* https://www.sec.gov/news/press-release/2019-109.

[3]*See* SEC Press Rel. No. 2019-110 (June 26, 2019), *available at* https://www.sec.gov/news/press-release/2019-110.

[4]*See* SEC Press Rel. No. 2019-112 (June 26, 2019), *available at* https://www.sec.gov/news/press-release/2019-112.

[5]*See* Press SEC Rel. No. 2019-121 (July 9, 2019), *available at* https://www.sec.gov/news/press-release/2019-121.

[6]*See* Allison Herren Lee Biography, *available at* https://www.sec.gov/biography/allison-herren-lee.

[7]*See* SEC Press Rel. No. 2019-129 (July 12, 2019), *available at* https://www.sec.gov/news/press-release/2019-129. *See also Staff Statement on LIBOR Transition* (July 12, 2019), *available at* https://www.sec.gov/news/public-statement/libor-transition.

FROM THE EDITORS

Congress Celebrates "National Whistleblower Day" as SEC Hits Milestone

As members of Congress, regulatory officials, and federal employees celebrated "National Whistleblower Day" on July 30, the Securities and Exchange Commission announced a whistleblower award to an anonymous overseas foreign national of half a million dollars.

National Whistleblower Day was designed to honor those employees that blow the whistle to stop waste, fraud, and abuse in their respective government agencies. And as part of the celebration, one government oversight council announced it was expanding its resources to ensure that whistleblowers are heard and not retaliated against.

The Council of the Inspectors General on Integrity and Efficiency ("CIGIE") released its new whistleblower resource page, which gives potential whistleblowers the ability to report possible violations or to find out more information about whistleblower rights and what is appropriate to report. The new website was made possible with support from both the Senate and House Appropriations Subcommittees on Financial Services and General Government, according to a CIGIE press release.

The whistleblower site and other planned enhancements were part of the CIGIE's request to Congress for funding in fiscal year 2019. CIGIE was appropriated $2 million, and the House appropriations bill for 2020 plans to give the agency an additional $1 million.

Federal whistleblowers have been behind important inspector general investigations into the Department of Veterans Affairs, the Federal Aviation Administration, and many more, according to the CIGIE.

For its part, the SEC has reported more than $2 billion in monetary sanctions from recent actions brought by whistleblowers and has paid out more than $300 million in rewards.

And now, the SEC is harnessing an even more powerful tool. Under the Foreign Corrupt Practices Act ("FCPA"), the SEC can pay out whistleblower awards to foreign nationals who report bribes they may have witnessed. Indeed, since the establishment of the SEC's whistleblower office by the Dodd-Frank Act, more than $40 million has been paid to overseas whistleblowers.

Under the Act, whistleblowers may be eligible for an award when they voluntarily provide the SEC with original, timely, and credible information that leads to a successful enforcement action. Whistleblower awards can range from 10% to 30% of the money collected when the monetary sanctions are more than $1 million.

In a press release about the SEC's whistleblower award to a foreign national, Stephen Kohn, a leading whistleblower attorney praised the action. "Whistleblowers are now the backbone of the international anti-bribery laws," said Kohn, noting that more than 3,000 foreign whistleblowers have already entered the SEC's confidential whistleblower program.

"For the first time, non-U.S. citizens have an effective way to report bribery in their home-countries and qualify for compensation under effective laws," Kohn explained. "The FCPA is a game-changer in the fight against international corruption."

John F. Olson & Gregg Wirth

EDITORIAL BOARD

Wall Street LAWYER

West LegalEdcenter
610 Opperman Drive
Eagan, MN 55123

FIRST CLASS
MAIL
U.S.POSTAGE
PAID
WEST

Wall Street LAWYER

West LegalEdcenter
610 Opperman Drive, Eagan, MN 55123
Phone: 1-800-344-5009 or 1-800-328-4880
Fax: 1-800-340-9378
Web: http://westlegaledcenter.com

THOMSON REUTERS

YES! Rush me ***Wall Street Lawyer*** and enter my one-year trial subscription (12 issues) at the price of $1,092.00. After 30 days, I will honor your invoice or cancel without obligation.

Name _____

Company _____

Street Address _____

City/State/Zip _____

Phone _____

Fax _____

E-mail _____

METHOD OF PAYMENT

❑ BILL ME

❑ VISA ❑ MASTERCARD ❑ AMEX

Account # _____

Exp. Date _____

Signature _____

Postage charged separately. All prices are subject to sales tax where applicable.