Wall Street LAWYER
Securities in the Electronic Age

January 2019 ▪ Volume 23 ▪ Issue 1

A SECURITY IS A SECURITY: HOW INITIAL COIN OFFERINGS MAY TRIGGER SECURITIES ENFORCEMENT AND PENALTIES

By John D. Shire & James R. Billings-Kang

John D. Shire is a partner in the Corporate Department of Seyfarth Shaw's Washington D.C. office where he serves both as Chair of the Impact Investment Practice and as Co-Chair of the firm's Blockchain Technologies Team. James R. Billings-Kang is an associate in the Commercial Litigation Department of the firm's Washington D.C. office.
Contact: jshire@seyfarth.com.

With the advent of cryptocurrency and blockchain technology comes the government's response to regulate these emerging technologies. The U.S. Securities and Exchange Commission (SEC), seeking to stay ahead of these advancements, has already announced how securities regulations may apply in these nascent scenarios.[1] In conjunction with the U.S. Commodity Futures Trading Commission (CFTC), the SEC has expressed no reservation in regulating the crypto industry.[2] More than one year removed from the SEC's July 2017 investigative report offering insights on the interplay between securities regulations and the cryptocurrency industry,[3] lawsuits and penalties from SEC enforcement are on the rise, with no stoppage in sight.[4] Indeed, the SEC has cautioned investors who are considering participation in initial coin offerings (ICOs), fundraising efforts[5] by cryptocurrency startups utilizing blockchain technology to raise capital.[6]

SEC Regulation of Initial Coin Offerings and the Exchange of Tokens

The principles underlying securities regulations, although dating back to the 1930s, are equally applicable today as they were in years past. In other words, any veiled attempt to shroud a security offering with modern novelty won't serve as a defense even if the existing regulatory regime may not fit neatly with a disruptive technology. For instance, in

IN THIS ISSUE:

THOMSON REUTERS®

42481453

the case of ICOs, that much the SEC has made clear: "In these cases, calling the transaction an initial coin offering, or 'ICO,' or a sale of a 'token,' will not take it out of the purview of the U.S. securities laws."[7] In its July 25, 2017 investigative report, the SEC, in cautioning issuers of digital coins and tokens, concluded that "[w]hether or not a particular investment transaction involves the offer or sale of a security—regardless of the terminology or technology used—will depend on the facts and circumstances, including the economic realities of the transaction."[8] As further underscored by Stephanie Avakian, co-Director of the SEC's Enforcement Division, "The innovative technology behind these virtual transactions does not exempt securities offerings and trading platforms from the regulatory framework designed to protect investors and the integrity of the markets."[9]

To escape oversight, startups have attempted to tender digital tokens in exchange for cryptocurrency, rationalizing that these tokens do not represent investment contracts that qualify as securities. Conceptually, the tokens provide the purchasers with access to a product or service provided by the startups rather than serving as a vehicle of sale for investment purposes. This token model, shared by many entrepreneurs to pirouette around SEC enforcement, was endorsed by Victor Santos, the CEO of the Harvard-born startup CarrierEQ, Inc. d/b/a Airfax, who had explained that the Airfax ICO would escape regulatory scrutiny because the utility tokens offered would allow purchasers to access items within AirFox's system.[10]

This rationale notwithstanding, Airfox recently settled with the SEC and other regulators after raising $15 million through an ICO in October 2017 for purportedly failing to register its tokens as securities. It, along with Paragon Coin Inc. (both of whom disclaimed liability), paid a penalty of $250,000 each, with both agreeing to compensate harmed investors, register their tokens under Section 12(g) of the Exchange Act, and periodically file reports with the SEC.[11] These results are particularly notable in large part because the SEC, for the first time,

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

One Year Subscription ● 12 Issues ● $ 1,188.00
(ISSN#: 1095-2985)

did not pursue fraud claims against a token issuer. In addition, the public (including supporters of the cryptocurrency industry) has raised its eyebrows, as in the case of Ripple Labs, the parent company of the third largest cryptocurrency in the world, who has faced a barrage of lawsuits filed by its investors claiming, *inter alia*, that the company failed to register its token offering as a security.[12]

What is a Security?

Section 2(a)(1) of the Securities Act of 1933 (the Securities Act), and Section 3(a)(10) of the Securities Exchange Act of 1934 (the Exchange Act) define what a "security" is.[13] While the definitions are "slightly different formulations," the U.S. Supreme Court has "treated [them] as essentially identical in meaning."[14]

In the watershed case of *SEC v. W.J. Howey Co.*,[15] the U.S. Supreme Court noted that a security included an investment contract, which is "a contract, transaction or scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party."[16] In other words, the *Howey* test, as it has become known, finds that there is a security with the satisfaction of three elements: (*i*) an investment of money, (*ii*) in a common enterprise, (*iii*) with a reasonable expectation of profits to be derived solely from the entrepreneurial or managerial efforts of others.[17] The Supreme Court recognized that the test "embodies a flexible rather than a static principle, *one that is capable of adaptation to meet the countless and variable schemes devised* by those who seek the use of the money of others on the promise of profits."[18]

The SEC and courts, relying on the flexibility of the *Howey* test, have placed ICOs under a careful microscope in determining whether the issued tokens should have been registered with the SEC prior to their offering.

Recent Applications of the *Howey* Test to ICOs

A recent application of the *Howey* test to digital tokens came from the Honorable Gonzalo P. Curiel in *SEC v. Blockvest, LLC*.[19] In *Blockvest, LLC*, the SEC accused Blockvest, LLC and its chairman and founder, Reginald Buddy Ringgold, III, of violating both the Securities Act and Exchange Act by offering and selling digital assets called BLVs without registering them as securities.[20] The SEC further alleged that the defendants engaged in fraud by cloaking the enterprise with improper legitimacy by falsely claiming that the BLV ICO was sanctioned by the SEC, CFTC, and National Futures Association; Deloitte Touche Tohmatsu Limited had partnered with and audited the defendants; and the Blockchain Exchange Commission, a fictitious regulatory agency created by the defendants, had approved the token offering.[21]

Already granted a temporary restraining order to freeze Ringgold's assets, prohibit the destruction of documents, and obtain expedited discovery, the SEC requested a preliminary injunction to continue these conditions.[22] As a government entity seeking injunctive relief, the SEC had the burden of showing a *prima facie* case of previous securities violation and a reasonable likelihood that the defendants will repeat the violation.[23] The Court could not provide any injunctive relief if there were "disputed questions of fact."[24]

To prove a previous securities violation, the

SEC had to show that the BLV tokens qualified as securities under the *Howey* test. Judge Curiel concluded that the government failed to meet the first and third prongs of the test.[25] In particular, the SEC could not demonstrate an investment of money, which required assessing the "promotional materials, information, economic inducements or oral representations at the seminars" relied upon by the investors before they purchased the test BLV tokens.[26]

To challenge the SEC's case, Ringgold swore that the investors were instead testers who, while they provided less than $10,000 in consideration, did not receive any tokens; instead, these were sophisticated investors who had a relationship with and were vetted by Ringgold and whom Ringgold retained exclusively to test the Blockvest, LLC platform, not to purchase any tokens.[27] Relatedly, and to challenge the satisfaction of the "expectation of profits" prong of the *Howey* test, Ringgold affirmed that the testers did not expect any profits.[28]

In response, the SEC also argued that Ringgold had 17 other investors who had remitted funds to Rosegold Investments LLP, purportedly the only investor of Blockvest, LLC, but Ringgold testified that these were mainly family and friends who did not rely on any representations related to Blockvest, LLC and simply did not care what the investments were for.[29] These affirmations were enough to create a dispute over the facts related to these two prongs of the *Howey* test, thereby preventing the Court from determining whether a security was offered.[30] As a result, the SEC could not demonstrate a *prima facie* showing of a previous securities violation and, therefore, no injunctive relief could follow.[31] The parties will likely engage in further discovery and, should dispositive motions fail, proceed to trial sometime next year.

Two weeks after the *Blockvest* decision, the Honorable Susan D. Wigenton of the U.S. District Court for the District of New Jersey, in the putative class action *Solis v. Latium Network, Inc.*, came down with the opposite conclusion. In considering the defendants' motion to dismiss, the Court held that the Complaint passed muster by sufficiently alleging that the sale of Latium tokens could constitute a violation of the Securities Act because they were unregistered with the SEC.[32] In particular, the Court concluded that Latium tokens—which were sold to investors such as the lead plaintiff through an ICO as a means to utilize Latium's blockchain-based tasking platform—appeared to be securities under the *Howey* test.[33] Conceding the first prong of the test, the defendants disputed that there was a common enterprise and a reasonable expectation of profits derived solely from the efforts of others.[34]

The Court disagreed. First, a common enterprise was present through "horizontal commonality," meaning the allegations, taken as true for purposes of considering the motion, showed that there was a "pooling of investors' contributions and distribution of profits and losses on a pro-rata basis among investors."[35] Second, *Howey*'s third prong was met by averments that the defendants' promotional materials and public statements galvanized people, such as the lead plaintiff who purchased over 200,000 tokens, to participate in the ICOs with the promise of "better financial returns."[36] Further showing that the tokens were meant to generate profit as

opposed to a means to use the tasking platform was Latium's white paper, which described how the tokens would generate compensation for its executives.[37] In line with Courts that do not require that the profits be derived *exclusively* by others, the New Jersey federal court found that, because the investors were completely dependent on the defendants to ensure the success of Latium and its platform, the Complaint adequately showed that any profits "primarily resulted from Defendants' efforts."[38] With the *Howey* test met, the Court concluded that "[b]ecause the [Latium] tokens were never registered with the [SEC], Plaintiff may maintain a cause of action against Latium under Section 12 of the Act."[39]

Further Guidance

Needless to say, while the regulatory landscape is less murky than before, questions remain. To the extent digital tokens qualify as securities, for example, this finding will have a lasting impact on secondary markets and exchanges that trade such tokens, exposing many to legal risks. Inescapably, when tokens satisfy the *Howey* test, issuers must decide on whether to register the tokens with the SEC and issue them in a public offering or rely on a number of exemptions, including, among others, Regulation Crowdfunding, Rule 506(c) of Regulation D, and Regulation A+, the three exemptions that permit general solicitation without any territorial limitations on sales within the United States. By the same token, ICO offerors will inexorably need to consider the implications of the Investment Company Act, U.S. Bank Secrecy Act, Commodity Exchange Act, Internal Revenue Code, and state securities laws.

Oversight by the CFTC, moreover, warrants examination. On September 26, 2018, Judge Rya W. Zobel of the U.S. District Court for the District of Massachusetts entered an order holding that the CFTC has the power to prosecute fraud involving virtual currency.[40] Judge Zobel's order reaffirmed the CFTC's anti-fraud and anti-manipulation authority over "any. . . contract of sale of any commodity in interstate commerce,"[41] and so in addition to the regulatory authority of the SEC, the CFTC has regulatory power to monitor, ban and penalize "any manipulative device, scheme, or artifice to defraud" in connection with the sale of a commodity.[42] The CFTC successfully litigated in 2018 challenges to its jurisdiction to regulate virtual currencies under the Commodity Exchange Act and its implementing regulations.[43]

To crystallize the SEC's regulatory umbrella overseeing ICOs, William Hinman, director of the SEC's Division of Corporation Finance, has promised that a "plain English" guide is currently in the works to apprise the public on how any potential token offering may qualify as a security: "We also will be putting out more guidance, the idea is a plain English instrument that people can look at and they'll bring together sort of my *Howey*-meets-*Gary* speech, and that analysis. . . . We'll elaborate on that in a very plain English way. . . ."[44] Relatedly, the SEC has developed the Strategic Hub for Innovation and Financial Technology, or FinHub (https://www.sec.gov/finhub), a new division devoted to assisting fintech startups navigate the contours of securities regulation.[45]

In the alternative, token issuers may wish to consider a number of options to permissibly

escape regulatory oversight. For instance, they could provide prospective purchasers with the necessary disclosures to definitively disclaim any expectation of a profit. Or they could provide purchasers with greater concrete rights in the project, including rights as a manager or more robust voting rights, so that they are not dependent on the creators of the tokens. That way, the purchaser strays away from the category of passive investors highlighted by Director Hinman: "The purchaser usually has no choice but to rely on the efforts of the [ICO] promoter to build the network and make the enterprise a success. At that stage, the purchase of a token looks a lot like a bet on the success of the enterprise and not the purchase of something used to exchange for goods or services on the network."[46] In addition, token issuers could intentionally target purchasers who would use the digital asset for personal use or consumption, which, according to the U.S. Supreme Court, falls outside the definition of a security.[47]

Director Hinman even offered other alternatives: "[C]onduct the initial funding through a registered or exempt equity or debt offering and, once the network is up and running, distribute or offer blockchain-based tokens or coins to participants who need the functionality the network and the digital assets offer. This allows the tokens or coins to be structured and offered in a way where it is evident that purchasers are not making an investment in the development of the enterprise."[48] As in the case of Bitcoin and Ether, Director Hinman acknowledged that if "the network on which the token or coin is to function is sufficiently decentralized—where purchasers would no longer reasonably expect a person or group to carry out essential managerial or other efforts—the assets may not represent an investment contract."[49] In this instance, the concern for material information asymmetries (one of the several legal underpinnings supporting the disclosure requirements of the Securities Act to protect investors) recedes, and consequently there is no security.

Overall, the burgeoning cryptocurrency industry has galvanized SEC and CFTC oversight and enforcement, necessitating the need for further legal guidance to meander this ever-changing regulatory landscape. Of course, not all is indecipherable: ICO issuers have the benefit of knowing that, at a minimum, the *Howey* test will apply, the 70-plus-year-old test that determines that a security is a security.

ENDNOTES:

[1]*See, e.g.*, SEC, *Initial Coin Offerings (ICOs)*, *available at* https://www.sec.gov/ICO (last visited Dec. 5, 2018); SEC, *Report of Investigation Pursuant to Section 21(a) of the Sec. Exch. Act of 1934: The DAO*, July 25, 2017, *available at* https://www.sec.gov/litigation/investreport/34-81207.pdf (last visited Dec. 5, 2018).

[2]Jay Clayton & J. Christopher Giancarlo, *Regulators Are Looking at Cryptocurrency*, Wall Street Journal, Jan. 24, 2018, *available at* https://www.wsj.com/articles/regulators-are-looking-at-cryptocurrency-1516836363 (last visited Dec. 5, 2018). Although the focus of this article is on the SEC's regulation of virtual currencies as securities, Bitcoin and other virtual currencies are subject to dual regulatory oversight by both the SEC and CFTC, which regulates the purchase or sale of virtual currencies as a "commodity," as defined in Section 1a(9) of the Commodity Exchange Act ("CEA"). *See Commodity Futures Trading Commission v. My Big Coin Pay, Inc.*, 334 F. Supp. 3d 492, Comm. Fut. L. Rep. (CCH) P 34345 (D. Mass. 2018),

available at https://www.cftc.gov/sites/default/files/2018-10/enfmybigcoinpayincmemorandum092618_0.pdf (last visited Dec. 5, 2018) (hereinafter, "*My Big Coin Pay*"); *see also In the Matter of: Coinflip, Inc., d/b/a/ Derivabit, & Francisco Riordan*, CFTC Docket No. 15-29 (Sept. 17, 2015) ("The definition of 'commodity' is broad. . . . Bitcoin and other virtual currencies are encompassed in the definition and properly defined as commodities.") (citation omitted), *available at* https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoinfliprorder09172015.pdf (last visited Dec. 5, 2018).

[3]SEC, *Report of Investigation Pursuant to Section 21(a) of the Sec. Exch. Act of 1934: The DAO*, July 25, 2017, *available at* https://www.sec.gov/litigation/investreport/34-81207.pdf (last visited Dec. 5, 2018).

[4]For a listing of such actions, *see* SEC, *Cyber Enforcement Actions*, *available at* https://www.sec.gov/spotlight/cybersecurity-enforcement-actions (spotlighting a number of SEC enforcement actions) (last visited Dec. 5, 2018); *see also* SEC, *Statement of Digital Asset Securities Issuance and Trading*, Nov. 16, 2018, *available at* https://www.sec.gov/news/public-statement/digital-asset-securites-issuuance-and-trading (last visited Dec. 5, 2018).

[5]To get a sense of the breadth of these fundraising efforts, PricewaterhouseCoopers and Crypto Valley Association note that, within the first five months of this year, ICO issuers raised $13.7 billion, nearly double the amount raised in the entire previous year. Accompanying this statistic is the fact that the average size of ICOs this year is $25.5 million, compared to $12.8 million last year. PricewaterhouseCoopers & Crypto Valley Assoc., "Initial Coin Offerings: A strategic perspective," June 2018, *available at* https://cryptovalley.swiss/wp-content/uploads/20180628_PwC-S-CVA-ICO-Report_EN.pdf (last visited Dec. 5, 2018). A useful tool to visualize the scope of ICOs is Coindesk's ICO Tracker, *available at* https://www.coindesk.com/ico-tracker (last visited Dec. 5, 2018).

[6]SEC, *Investor Bulletin: Initial Coin Offerings*, July 25, 2017, *available at* https://www.investor.gov/additional-resources/news-alerts/alerts-bulletins/investor-bulletin-initial-coin-offerings (last visited Dec. 5, 2018).

[7]William Hinman, Director, SEC Div. of Corp. Fin., Remarks at the Yahoo Finance All Markets Summit: "Digital Asset Transactions: When Howey Met Gary (Plastic)", *available at* https://www.sec.gov/news/speech/speech-hinman-061418 (last visited Dec. 5, 2018). Contrast this with Director Hinman's statement that Ether, the cryptocurrency of the Ethereum network, is not a security: "And putting aside the fundraising that accompanied the creation of Ether, based on my understanding of the present state of Ether, the Ethereum network and its decentralized structure, current offers and sales of Ether are not securities transactions." *Id.* (To be sure, Director Hinman's remarks are not official statements of the SEC, but they are insightful.) This sentiment is not shared by Gary Gensler, former Chairman of the CFTC, who argued that Ether and other cryptocurrencies could be classified as securities. *See* Annaliese Milano, *Everything Ex-CFTC Chair Gary Gensler Said About Cryptos Being Secs.*, Coindesk, Apr. 24, 2018, *available at* https://www.coindesk.com/ex-cftc-chair-gary-gensler-on-tokens-securities-and-the-sec (last visited Dec. 5, 2018).

[8]SEC, *Report of Investigation Pursuant to Section 21(a) of the Sec. Exch. Act of 1934: The DAO*, July 25, 2017, *available at* https://www.sec.gov/litigation/investreport/34-81207.pdf (last visited Dec. 5, 2018); *see also United Housing Foundation, Inc. v. Forman*, 421 U.S. 837, 850, 95 S. Ct. 2051, 44 L. Ed. 2d 621, Fed. Sec. L. Rep. (CCH) P 95206 (1975) ("[T]he name given to an instrument is not dispositive.").

[9]SEC, *SEC Issues Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities*, July 25, 2017, *available at* https://www.sec.gov/news/press-release/2017-131 (last visited Dec. 5, 2018).

[10]Kelly J. O'Brien, *This Techstars Boston alum is planning to raise $15M - all through cryptocurrency*, Biz Journals, Aug. 8, 2017, *available at* https://www.bizjournals.com/bosto

n/news/2017/08/08/this-techstars-boston-alum-is-planning-to-raise.html (last visited Dec. 5, 2018).

[11]SEC, *Two ICO Issuers Settle SEC Registration Charges, Agree to Register Tokens as Securities*, Nov. 16, 2018, *available at* https://www.sec.gov/news/press-release/2018-264 (last visited Dec. 5, 2018).

[12]*See, e.g.*, Rhys Dipshan, *Ripple Labs Faces Third Secs. Fraud Suit Over Its Cryptocurrency*, The Reporter, July 3, 2018, *available at* https://www.law.com/therecorder/2018/07/03/ripple-labs-faces-third-securities-fraud-suit-over-its-xrp-cryptocurrency/ (last visited Dec. 5, 2018).

[13]The Securities Act defines a security as "any note, stock, treasury stock, security future, security-based swap, bond, debenture, evidence of indebtedness, certificate of interest or participation in any profit-sharing agreement, collateral-trust certificate, preorganization certificate or subscription, transferable share, investment contract, voting-trust certificate, certificate of deposit for a security, fractional undivided interest in oil, gas, or other mineral rights, any put, call, straddle, option, or privilege on any security, certificate of deposit, or group or index of securities (including any interest therein or based on the value thereof), or any put, call, straddle, option, or privilege entered into on a national securities exchange relating to foreign currency, or, in general, any interest or instrument commonly known as a 'security,' or any certificate of interest or participation in, temporary or interim certificate for, receipt for, guarantee of, or warrant or right to subscribe to or purchase, any of the foregoing." 15 U.S.C.A. § 77b(a)(1).

Similarly though not identically, the Exchange Act defines a security as "any note, stock, treasury stock, security future, security-based swap, bond, debenture, certificate of interest or participation in any profit-sharing agreement or in any oil, gas, or other mineral royalty or lease, any collateral-trust certificate, preorganization certificate or subscription, transferable share, investment contract, voting-trust certificate, certificate of deposit for a security, any put, call, straddle, option, or privilege on any security, certificate of deposit, or group or index of securities (including any interest therein or based on the value thereof), or any put, call, straddle, option, or privilege entered into on a national securities exchange relating to foreign currency, or in general, any instrument commonly known as a 'security'; or any certificate of interest or participation in, temporary or interim certificate for, receipt for, or warrant or right to subscribe to or purchase, any of the foregoing; but shall not include currency or any note, draft, bill of exchange, or banker's acceptance which has a maturity at the time of issuance of not exceeding nine months, exclusive of days of grace, or any renewal thereof the maturity of which is likewise limited." 15 U.S.C.A. § 78c(a)(10). Options to purchase most securities are "securities" and those options, along with security-based swaps are regulated by the SEC, although the CFTC and the SEC have joint regulatory jurisdiction over options with commodity components (which are "mixed swaps" under Section 1a(47)(D) of the CEA).

[14]*S.E.C. v. Edwards*, 540 U.S. 389, 393, 124 S. Ct. 892, 157 L. Ed. 2d 813, Fed. Sec. L. Rep. (CCH) P 92656 (2004).

[15]*S.E.C. v. W.J. Howey Co.*, 328 U.S. 293, 66 S. Ct. 1100, 90 L. Ed. 1244, 163 A.L.R. 1043 (1946).

[16]*Id.* at 298-99.

[17]*Id.*; *see also Edwards*, 540 U.S. at 393; *S.E.C. v. Rubera*, 350 F.3d 1084, 1090, Fed. Sec. L. Rep. (CCH) P 92631 (9th Cir. 2003) (internal quotation marks omitted). Among the debates concerning the third prong is whether the expectation of profits should be derived *solely* or *substantially* from the efforts of others. Some courts take a literal approach, while the SEC and other courts have broadened the reach of the third prong. *Compare Hirsch v. duPont*, 396 F. Supp. 1214, 1218-20, Fed. Sec. L. Rep. (CCH) P 95210 (S.D. N.Y. 1975), judgment aff'd, 553 F.2d 750, Fed. Sec. L. Rep. (CCH) P 96011 (2d Cir. 1977) ("However, despite the rejection of Howey in other jurisdictions, decisions of this district and circuit until recently followed it and

gave no indication that the Howey test would not be applied literally."), *aff'd*, *Hirsch v. du Pont*, 553 F.2d 750, Fed. Sec. L. Rep. (CCH) P 96011 (2d Cir. 1977)*withS.E.C. v. Koscot Interplanetary, Inc.*, 497 F.2d 473, 480, Fed. Sec. L. Rep. (CCH) P 94710 (5th Cir. 1974) ("Moreover, a close reading of the language employed in Howey and the authority upon which the Court relied suggests that, contrary to the view of the district court, we need not feel compelled to follow the 'solely from the efforts of others' test literally.") and SEC, *Report of Investigation Pursuant to Section 21(a) of the Sec. Exch. Act of 1934: The DAO*, July 25, 2017, *available at*https://www.sec.gov/litigation/investreport/34-81207.pdf (last visited Dec. 5, 2018).

[18]*Howey*, 328 U.S. at 300 (emphasis added).

[19]No. 18CV2287-GPB(BLM), *Securities and Exchange Commission v. Blockvest, LLC*, 2018 WL 6181408 (S.D. Cal. 2018).

[20]*Id.*, at *1.

[21]*Id.*, at *2.

[22]*Id.*, at *1.

[23]*Id.*, at *3 (citations omitted).

[24]*Id.*, at *4 (citations omitted).

[25]*Id.*, at *7-8.

[26]*Id.*, at *7.

[27]Id.

[28]*Id.*

[29]Id.

[30]*Id.*, at *7-8.

[31]The Court further concluded that the government could not show a reasonable likelihood of a repeated wrong because Ringgold was willing to halt moving forward with the ICO until his venture complied with the regulations at issue. *Id.*, at *8.

[32]No. 18-10255 (SDW) (SCM), *Solis v. Latium Network, Inc.*, 2018 WL 6445543, at *3 (D.N.J. 2018).

[33]Id.

[34]*Id.*, at *1-2.

[35]*Id.*, at *3 (citing *U.S. S.E.C. v. Infinity Group Co.*, 212 F.3d 180, 187-88, Fed. Sec. L. Rep. (CCH) P 90966, 55 Fed. R. Evid. Serv. 185, 46 Fed. R. Serv. 3d 625 (3d Cir. 2000) (internal quotation marks omitted) (quoting *Steinhardt Group Inc. v. Citicorp*, 126 F.3d 144, 150, Fed. Sec. L. Rep. (CCH) P 99527 (3d Cir. 1997))).

[36]*Id.*, at *1, 3.

[37]*Id.*, at *3.

[38]Id.

[39]*Id.*

[40]*My Big Coin Pay*, *see supra* note 2.

[41]*Id.*, at *2.

[42]*Id.*, at *5 (citing 17 C.F.R. § 180.1(a)).

[43]*See* Nowell Bamberger, Robin Bergen & Emily Michael, "Virtual Currencies, Manipulation, Cooperation and More: CFTC Enf't Div.'s 2018 Annual Report," Compliance & Enf't, Program on Corp. Compliance & Enf't, N.Y. Univ. School of Law (Nov. 28, 2018), *available at* https://wp.nyu.edu/compliance_enforcement/2018/11/28/virtual-currencies-manipulation-cooperation-and-more-cftc-enforcement-divisions-2018-annual-report/ (last visited Dec. 5, 2018).

[44]Nikhilesh De & Aaron Stanley, *SEC Official Says 'Plain English' Guidance on ICOs is Coming*, Coin Desk, Nov. 5, 2018, *available at* https://www.coindesk.com/sec-official-says-plain-english-guidance-on-icos-is-coming (last visited Dec. 5, 2018).

[45]SEC, *SEC Launches New Strategic Hub for Innovation & Fin. Tech.*, Oct. 18, 2018, *available at* https://www.sec.gov/news/press-release/2018-240 (last visited Dec. 5, 2018).

[46]William Hinman, Director, SEC Div. of Corp. Fin., Remarks at the Yahoo Finance All Markets Summit: Crypto, "Digital Asset Transactions: When Howey Met Gary (Plastic) (June 14, 2018), *available at* https://www.sec.gov/news/speech/speech-hinman-061418 (last visited Dec. 5, 2018).

[47]*Forman*, 421 U.S. at 853.

[48]Id.

[49]*Id.*

THE SEC, INTERNAL ACCOUNTING CONTROLS, AND THE HUMAN ELEMENT

By Thomas O. Gorman

Thomas O. Gorman is a Partner in the Washington, D.C. office of Dorsey and Whitney. He also publishes SEC Actions (www.secactions.com), a blog that focuses on the Securities and Exchange Commission. This article is based on a blog post that was published on November 27. He is also a member of the Editorial Advisory Board of Wall Street Lawyer. Contact: gorman.tom@dorsey.com.

Exchange Act section 13(b)(2)(B), added to the 1934 Act as part of the Foreign Corrupt Practices Act of 1977, is concerned with internal accounting controls. The statute requires that there be sufficient controls to ensure that transactions are executed as directed by management; to permit the preparation of the financial statements; and to ensure that access to assets is permitted only in accord with management's authorization. The section underscores the fact that management serves as the steward of the shareholders' investment.

The "internal accounting controls" focus of the section has been repeatedly emphasized by the Commission in a variety of cases that range from FCPA corruption actions to those centered on accounting fraud. Two recent developments, however, suggest that issuers take a new look from a different prospective when evaluating internal accounting controls: The Commission's section 21(a) Report on Certain Cyber-Related Frauds (October 16, 2018) and its FCPA settlement, *In the Matter of Vantage Drilling International.*[1]

The report is well grounded in the language of the statute and the traditional views of the agency regarding internal accounting controls, citing at points the history of the section. The Report also ties those notions together with risk management policies, stating that "[c]ybersecurity risk management policies and procedures are key elements of enterprise-wide risk management, including as it relates to compliance with the federal securities laws," quoting from the Commission Statement on Guidance on Public Company Cybersecurity Disclosures.

Subsequent sections of the report emphasize that the cyber schemes investigated were typically simple and there were often numerous red flags. Yet there were repeated failures. Those failures resulted in many instances because the personnel did not take the appropriate steps or fully appreciate the situation. As the report states: "Systems of internal accounting controls, by their nature, depend also on the personnel that implement, maintain, and follow them." This "human element," tied to section 13(b)(2)(B) concepts adds a dimension to the traditional discussion of internal accounting controls.

Key to the ultimate outcome of *Vantage Drilling* is a similar concept. That action involved in the first instance a relatively new drilling firm seeking to acquire a deep-water drilling vessel under construction at a Korean ship yard for a Taiwanese shipping magnate identified as Director A. Through a series of agreements Vantage Drilling was to acquire the deep-water drilling vessel and other assets. As part of the deal, the shipping magnet would become a director. No due diligence was done on Director A.

Vantage Drilling later learned that Director A made misrepresentations at the same ship yard in connection with another vessel and even at one point claimed not to be able to pay for a ship. Yet the drilling firm "did not enhance its internal accounting controls in regard to its transactions with respect to Director A," according to the order. That failure ultimately took the firm down the path to a bribery scheme hatched and executed by Director A.

While the order in *Vantage Drilling* does not specifically discuss the "human element" of internal controls in those terms like the Report, the reason to strengthen the internal controls in that action was the risk posed by Director A. Stated differently, the man was not trustworthy and tying the enterprise to him put the stewardship of management, and thus the shareholders' investment, at risk. Vantage Drilling, however, failed to recognize this risk and take precautionary steps—a failure which resulted in its undoing when the bribery scheme was uncovered in the now infamous "Operation Car Wash" scandal in Brazil.

Vantage Drilling's failure is little different from that of management at the various firms cited in the report. When faced with an untrustworthy Director A—as with the cyber threats—management failed to act as an effective steward, failed to take the proper steps or even to appreciate the risks to the enterprise and thus the shareholders' investment. It is this human element of internal accounting controls, and the failures with regard to this element, that was critical to the actions underlying the Report and in *Vantage Drilling*.

It is the emergence of this human element of internal accounting controls that is critical to the cyber-security report and the FCPA case. It is the recognition of this element which issuers must carefully consider and evaluate in terms of risk, training and the testing of internal accounting controls in the future.

ENDNOTES:

[1]*In the Matter of Vantage Drilling International,* Adm. Proc. File No. 3-18899 (Nov. 19, 2018).

LESSONS LEARNED FROM THE GOLDMAN SACHS 1MDB INCIDENT: HOW INADEQUATE COMPLIANCE METHODS COMPROMISED ONE OF THE WORLD'S BIGGEST BANKS

By Isaac Kohen

Isaac Kohen is the Chief Technology Officer at Teramind, a global provider of employee and user activity monitoring, user behavior analytics, insider threat detection, forensics and data loss prevention solutions. Kohen started his career in quantitative finance developing complex trading algorithms for a major Wall Street hedge fund. You can follow him on Twitter: @teramindco.

It's been nearly a decade since Najib Razak, the former prime minister of Malaysia, launched the 1MDB state investment fund intended to facilitate growth for Malaysia's middle class.

However, an unprecedented level of greed, corruption, bribery, and theft has transformed

this investment fund into one of the most controversial examples of financial mismanagement in history, implicating politicians and financial institutions in a multi-billion dollar heist that is playing out in front page headlines.

Most prominently, the U.S. financial juggernaut, Goldman Sachs, is at the center of the scandal, as the bank both helped facilitate the fund's expansion and was complicit in its mismanagement. Most recently, Malaysian authorities filed criminal charges against Goldman Sachs, accusing the bank of knowingly defrauding the Malaysian public of more than $6 billion. It's the most recent iteration of the many legal implications that Goldman faces.

As *The New York Times* concluded, "Goldman recently received subpoenas from New York regulators, held talks with federal prosecutors and is likely to incur billions of dollars in penalties. It is one of the most serious crises in the bank's 149-year history."[1] The consequences have been steep. Goldman's stock has plummeted 27% since November 2018, and both the bank's financial liability and internal integrity are being questioned.

Goldman took some steps to extricate itself from the scandal. For instance, the bank terminated Tim Leissner, the senior banker for the 1MDB project who personally netted millions in fees, but the move seems trite amidst a diatribe of accusations aimed at the bank.

Of course, a scandal of this magnitude at a prestigious financial institution like Goldman Sachs raises a lot of questions. Most prominently, how could something like this happen?

The answer, it turns out, is startlingly simple and frustratingly avoidable.

Outdated Compliance Measures

Financial institutions live within a highly regulated environment, and Goldman invests heavily in its human-based compliance measures. According to former Goldman Sachs CEO Lloyd Blankfein, the bank has increased compliance staff by more than 3,000 employees since 2012 to support heightened compliance efforts.[2] These employees monitor and enforce clearly outlined rules and regulations that govern the industry, but they rely on self-reporting and whistleblowers, rather than a foolproof monitoring and oversight system in addition to the self-reporting guidelines in place.

Goldman attributes the 1MDB scandal to rogue employees who avoided compliance measures for personal gain. Characterizing the Goldman employees involved in the project as rebellious and misguided, Mr. Blankfein asserts, "These are guys who evaded our safeguards, and lie, stuff like that's going to happen."[3]

However, when it comes to compliance reporting for the 1MDB project, U.S. prosecutors note that Goldman's "system of internal accounting controls could be easily circumvented and that the firm's business culture, particularly in Southeast Asia, at times prioritized consummation of deals ahead of the proper operation of its compliance functions."[4] Goldman employees describe a "culture of secrecy" at the financial institution,[5] a factor that likely made it easier for employees to work around compliance measures.

Taken together, it's clear that Goldman's

compliance protocols were insufficient, failing to account for the real-world dynamic of power, greed, and financial incentive for avoiding established restrictions. In short, this moral and financial catastrophe was avoidable, and it's important to ensure that it is prevented from happening again.

A Natural Next Step

What's needed is robust user activity monitoring software to bridge the gap between the onus of human reporting and the nefarious incentives that encourage people to circumvent these procedures. In doing so, Goldman Sachs and other financial institutions can create an electronic, automated oversight model that makes it more difficult for employees to break the law. With features like real-time alerts and digital forensic evidence, organizations can demonstrate intent to comply with regulations while documenting any instances of malicious employee actions.

For example, employee monitoring software can establish rules that monitor user behavior and activity, serving as both a guardrail and a deterrent to bad behavior. Using these automated guidelines, from the boardroom-down, the compliance team can receive a warning notifying them to a potential problem while equipping them with the tools to stop specific events before they cause a bigger headache. The 1MDB scandal is almost a decade in the making, and, with these systems in place, it's possible that Goldman Sachs could have prevented its proliferation long before it engulfed the bank.

Of course, if misuse or criminality does occur, employee monitoring software provides the digital forensics to quickly identify anyone responsible, ensuring that accountability is swift, accurate, and complete. Hearsay is inherently difficult to corroborate, but recorded computer user sessions are indisputable, providing real-time or historical evidence of an employee's digital activity.

Goldman's involvement in the 1MDB scandal should be a warning to other financial organizations as proof that the consequences for malfeasance can be incredibly costly. Goldman will endure dramatic fines that will impact their bottom line, and the reputational damage will take years if not decades to repair.

By deploying proper technology oversight, financial firms can guard against the next scandal, which protects both their brand and their employees from the cascading consequences of inaction. In 2019 and beyond, monitoring, auditing, and forensic capabilities should be a top priority for organizations operating in regulated industries like the financial sector.

Goldman Sachs was late learning this lesson, but it can be an instructive moment for everyone else, and it means that now is the perfect time to make sure that your company isn't the next to endure an embarrassing and expensive scandal like 1MDB.

ENDNOTES:

[1]Matthew Goldstein and Alexandra Stevenson, "1MDB Case in Malaysia Deepens Goldman's Crisis," The New York Times, Dec. 17, 2018; *available at*: https://www.nytimes.com/2018/12/17/business/goldman-1mdb-malaysia.html?action=click&module=Top%20Stories&pgtype=Homepage.

[2]Jon Marino, "At Goldman, traders are out

and compliance is in," CNBC.coom, Feb. 9, 2016; available at: https://www.cnbc.com/2016/02/09/at-goldman-traders-are-out-and-compliance-is-in.html.

[3]Goldstein, Stevenson and Emily Flitter, "Goldman Sachs Ensnarled in Vast 1MDB Fraud Scandal," The New York Times, Nov. 1, 2018; *available at*: https://www.nytimes.com/2018/11/01/business/goldman-sachs-malaysia-investment-fund.html?module=inline.

[4]Samuel Rubenfeld, "Goldman Disclosure in 1MDB Probe Points to Potential Control, Culture Concerns"; The Wall Street Journal, Nov. 5, 2018; *available at*: https://www.wsj.com/articles/goldman-disclosure-in-1mdb-probe-points-to-potential-control-culture-concerns-1541461239.

[5]Patricia Hurtado and Greg Farrell, "Leissner Cites Goldman's 'Culture' of Secrecy in 1MDB Scheme," Bloomberg Markets, Nov. 9, 2018; *available at*: https://www.bloomberg.com/news/articles/2018-11-09/leissner-in-unsealed-plea-cites-goldman-culture-of-secrecy.

TECHNOLOGY, INVESTMENT AND SECURITY: THE MODERNIZATION OF CFIUS—*WHAT DOES IT MEAN FOR THE GLOBAL INVESTOR?*

By Timothy J. Keeler, Mark Uhrynuk, Brian F. McKenna, Thomas A. De Gregoris & Mickey Leibner

Timothy Keeler is a partner in the Government Relations & Public Law and International Trade practices of Mayer Brown in Washington, D.C.; Mark Uhrynuk and Brian F. McKenna are partners in the firm's Hong Kong office; Thomas A. De Gregoris is an associate in the firm's Corporate & Securities practice in Chicago; and Mickey Leibner is an associate in the Washington, D.C. office.
Contact: tkeeler@mayerbrown.com, mark.uhrynuk@mayerbrown.com, or brian.mckenna@mayerbrown.com

On August 13, 2018, President Trump signed into law the Foreign Investment Risk Review Modernization Act, or FIRRMA, legislation designed to enhance US national security and protect US technological achievements and superiority.

FIRRMA contains a number of provisions that modify the scope and responsibilities of the Committee on Foreign Investment in the United States, or CFIUS, in light of a constantly shifting economic landscape accentuated by exponential technological growth and advancement.

A Brief History

CFIUS dates back to an executive order signed by President Gerald Ford in 1975. Soon after, CFIUS developed into a multi-agency committee heavily influenced by the executive agencies of the US government responsible for the economy, national security, and foreign intelligence. Thirteen years later, in 1988, the purview of CFIUS was expanded by an Act of Congress known as the Exon-Florio amendment to the Defense Production Act. Among other expansions, the effect of the Exon-Florio amendment was to give CFIUS the ability to review and prohibit any foreign acquisition of a US business that could threaten US national security.

It would be 18 years until CFIUS saw another major overhaul. What spurred this second major change was public discontent over a Dubai company's planned 2006 acquisition of a com-

pany that managed a number of US ports. This controversy prompted Congress to reform CFIUS via the Foreign Investment and National Security Act of 2007, or FINSA. FINSA gave Congress greater oversight over CFIUS, increased accountability among CFIUS member agencies, and expanded its scope by including critical infrastructure as part of the CFIUS national security protection mandate.

Then, in the summer of 2018, Congress enacted the FIRRMA revisions to CFIUS jurisdiction and process. FIRRMA contains a number of provisions that modify the scope and responsibilities of CFIUS to better protect US national security interests with respect to both foreign government-controlled and private investors.

Addressing Complexity—Evolving Jurisdictional Scope and Critical Focus on Technology

Generally speaking, CFIUS jurisdiction applies only to ***covered transactions***, which historically have been any merger, acquisition or takeover resulting in foreign control of any person engaged in interstate commerce in the United States. More specifically, the CFIUS mandate has been to review any covered transaction that might have an impact on US national security. Transactions where the acquiring entity is a foreign government (or controlled by a foreign government) have been given particular scrutiny. Under FIRRMA, the scope of these covered transactions has been re-assessed and expanded.

Since FINSA was enacted, CFIUS has faced a number of operational challenges as foreign investment transactions have increased both in number and complexity. In the past, transactions that fell under CFIUS jurisdiction have only included transactions that resulted in a "controlling" foreign interest. Historically, "control" meant that either the foreign person would acquire a majority interest in the US business, or that the foreign person would acquire a minority interest which resulted in a significant ability to decide important matters related to the US business (although CFIUS has found ownership at low levels—*e.g.*, 15% with a board seat—sufficient to grant "control"). Under FIRRMA, however, CFIUS now has jurisdiction over certain non-controlling investments, particularly those related to *critical technologies*, *critical infrastructure* or a US citizen's *sensitive personal data*, unless the investment is truly "passive." Accordingly, under FIRRMA, even a non-controlling investment will be a covered transaction if it affords a foreign person: (*i*) access to *material non-public technical information*; (*ii*) membership or observer rights on a board of directors or an equivalent governing body; or (*iii*) any involvement in substantive decision making (other than the voting of shares).

Furthermore, under FIRRMA, critical technologies include certain *emerging and foundational technologies*. This focus on non-controlling investment and transactions involving critical technology could have potentially significant implications on a range of technology transfer transactions including joint ventures.

FIRRMA also clarifies that CFIUS jurisdiction will be triggered by any change in a foreign person's ownership or control rights in respect of a US business that could result in foreign control of a US business or an investment in a

US business relating to critical technology, critical infrastructure, or sensitive personal data.

What About Real Estate?

Prior to FIRRMA, while the acquisition of a business in which a majority of the assets were real estate would have been subject to CFIUS jurisdiction, the mere acquisition of real estate would not have triggered a possible CFIUS review. In recent years, however, CFIUS has developed and begun to review transactions involving the acquisition of a US business in close proximity to sensitive US government facilities. Under FIRRMA, CFIUS jurisdiction has been expanded to include any type of real estate transaction in which the property is located within or in close proximity to an air or maritime port, US military installation, or any other property of the US government determined to be related to national security.

An Exception for Certain Investment Funds

FIRRMA contains a special exception for indirect investments by a foreign person held through an investment fund. Under FIRRMA, membership of a foreign person as a limited partner or an equivalent on an advisory board or a committee of an investment fund investing in critical technology, critical infrastructure or sensitive personal data would not trigger CFIUS jurisdiction if:

1. The fund is managed exclusively by a general partner or an equivalent;
2. The general partner or an equivalent is not a foreign person;
3. The advisory board or committee does not have the power to approve, disapprove or otherwise control investment decisions of the fund or decisions made by the general partner or an equivalent relating to investment held by the fund; and
4. The foreign person does not otherwise have any power to control the fund.

Balancing Interests—Investment and Innovation

As FIRRMA moved through the legislative process special efforts were made to balance the US government's interest in encouraging foreign investment with efforts to enhance protection against the shifting nature of national security risks. Accordingly, FIRRMA limits CFIUS jurisdiction to transactions that pose a threat to US national security via an investment in a US business or US real estate. An expanded scope (*e.g.*, the transfer of technology outside the US where there is no investment in a US business) would have begun to overlap with the US export control system (specifically as it relates to dual-use technology), making it more difficult for innovators based in the US to raise funding and move forward with research. A CFIUS scope broadened in this way would have incentivized research and development outside of the United States, potentially harming the US security interests that CFIUS was designed to protect. In some ways, FIRRMA is narrower in scope than analysts had previously predicted based on earlier drafts of the law. Under the final version of FIRRMA, CFIUS has not been granted the authority to review outbound transfers of intellectual property or technology unconnected to an investment in a US business.

Competition and Security—Special Concerns

In a section of FIRRMA titled "Sense of Congress on Consideration of Covered Transactions" CFIUS is allowed to consider in its analysis whether a covered transaction involves a *country of special concern*. While earlier versions of proposed legislation specifically identified certain countries (including China, Russia, Iran and North Korea), FIRRMA does not identify such countries by name but suggests that these are countries that have demonstrated or declared strategies of acquiring critical technology or critical infrastructure that would affect US leadership in areas related to national security. The same section of FIRRMA lays out additional factors which may be taken into account in considering national security risks.

These factors include:

- The cumulative effect or pattern of transactions by a foreign government or foreign person;
- The foreign person's record of complying with US laws and regulations;
- The impact on the capability and capacity of United States to meet national security demands, in particular the availability of human resources which may be critical to national security know-how; and
- Issues relating to sensitive personal data (such as personally identifiable information) or cybersecurity vulnerabilities.

Process Reforms—Mandatory Filings and Procedural Adjustments

FIRRMA has introduced a new, abbreviated filing option referred to as a "declaration." A declaration may be submitted instead of the complete joint voluntary notice that was required prior to FIRRMA. It is an abbreviated notification, limited to five pages in length, the exact contents of which are not yet specified by FIRRMA and are to be set out by CFIUS under a future regulatory rulemaking process. Not later than 30 days after receiving a declaration, CFIUS must take one of the following actions:

- Request that the transactional parties file the more extensive joint voluntary notice;
- Initiate a unilateral CFIUS review of the transaction;
- Inform the parties that CFIUS is unable to take action based on the abbreviated declaration and that the parties may file the more extensive joint voluntary notice and request notification from CFIUS that it has completed its review; or
- Inform the parties that CFIUS has completed its review.

Under FIRRMA, mandatory filings with CFIUS will be required for certain transactions. This requirement will cover any investment by a foreign person in which a foreign government has, directly or indirectly, a substantial interest, which results in the foreign person acquiring, directly or indirectly, a substantial interest in a US business. FIRRMA requires CFIUS to define what constitutes a "substantial interest," but FIRRMA does establish two statutory exceptions of investments that are not to be considered substantial interests:

- Investments below a 10% voting interest; and

- Certain interests held as a limited partner through an investment fund (as described more fully above).

FIRRMA has also authorized CFIUS to require mandatory filings for other investments and transactions involving US businesses if they relate to critical technology. Indeed, CFIUS recently proposed that, effective November 10, 2018, parties to non-passive investments (both controlling and non-controlling) will be required to notify CFIUS of such transactions. (See further the inset box "Pilot Programs" below.)

Additionally, under FIRRMA, the CFIUS review period has been extended from 30 to 45 days. After the review period, FIRRMA provides for a 45-day investigation period, but CFIUS will be able to extend that investigation period by a further 15 days in "extraordinary circumstances." These changes become effective for any review or investigation initiated on or after the date of FIRRMA's enactment into law.

Importantly, for foreign investors, FIRRMA also now requires more transparency and accountability from CFIUS during the process in the form of mandatory comments or official acceptance of a draft or formal filing within 10 business days of the submission of such filing. This is in contrast to the CFIUS process prior to FIRRMA in which transaction parties could see multiple week wait times for draft comments or acknowledgement of acceptance.

Under FIRRMA, CFIUS has the discretionary authority to require an administration fee in an amount not to exceed the lesser of 1% of the transaction value or US$300,000 (to be annually adjusted for inflation).

Most of the FIRRMA updates to CFIUS do not take effect immediately, but will become effective on the earlier of 18 months after the date of FIRRMA's enactment (13 August 2018) or 30 days after a public determination by the CFIUS chairperson that the required regulations, structure and resources necessary to implement the new regulations are in place.

What Now? Impact Assessment, Mitigation Strategies and Beyond

- Parties considering cross-border transactions or investments in which a foreign person proposes to acquire interests in a US business should be familiar with the CFIUS process as modified by FIRRMA. In particular, if such a transaction involves any of the aforementioned critical or emerging and foundational technologies, we recommend undertaking a thorough assessment and submitting the proposed transaction for CFIUS review. Also, as CFIUS jurisdiction now covers certain non-controlling investments in a US business, investors should be aware that this may allow CFIUS to assert jurisdiction over smaller transactions and investments that historically had not been subject to such regulatory scrutiny.

- As the application of critical technologies and the demand for data cut across more and varied industries, it is possible that CFIUS' jurisdiction could spread to transactions that might, on the surface, seem outside of its mandate. For example, as FIRRMA considers any transaction that involves potential foreign ownership, control or collection of sensitive personal data

to be a covered transaction, businesses in a number of consumer related sectors could be implicated: insurance products, healthcare, e-commerce, etc. Transaction participants should be creative when assessing whether a particular company uses technology or personal data in a way that may be caught by FIRRMA.

- Now that legislation has been enacted, some stability should begin to return to the market as there is a degree of certainty that flows from FIRRMA. FIRRMA should serve to promote a focus on those transactions that pose more defined risk to US national security interests. The last couple of years have generated much regulatory uncertainty, and uncertainty does not promote a strong cross-border M&A market. In this context, it is not surprising that, during a period of little visibility as to what the new FIRRMA rules might look like, inbound Chinese deals with American companies declined by 56% in 2017 with a continued decline through the third quarter of 2018. While many factors have caused deal making to drop-off, the regulatory uncertainty around CFIUS and FIRRMA contributed to this decline. We are cautiously optimistic that the enactment of FIRRMA will remove some of the regulatory overhang in the market.

- In addition, in June 2018, President Trump announced that he would not enforce new investment restrictions against China under Section 301 of the Trade Act of 1974, removing a longstanding cloud of doubt dampening the US-China M&A market. Had he decided to enact new restrictions, they were expected to target a number of key technology sectors, including information technology, aerospace, pharmaceuticals, alternative energy vehicles and robotics. This further clarity in the market should allow investors to gain a degree of confidence in the predictability of the regulatory hurdles in the US-China M&A process.

- All is not certain though, as a number of critical regulations still need to be developed and enacted. The pilot programs referred to above will inform CFIUS in its efforts to fully implement FIRRMA. If these programs are used to introduce additional challenges and hurdles for investors to navigate, a further chilling effect on international M&A transactions across multiple industries could arise.

This article was originally published in the Publications section of the website of Mayer Brown and is reproduced with permission. *The contents of this article are intended to provide a general guide to the subject matter and should not be treated as a substitute for specific advice concerning individual situations. Readers should seek legal advice before taking any action with respect to the matters discussed herein. For further information please contact the authors or Mayer Brown at mail to: bernadette.tio@mayerbrown.com.*

MARRIOTT DATA BREACH IS A WARNING FLAG FOR FINANCIAL FIRMS, REGULATORS CAUTION

By Richard Satran

Richard Satran is a financial journalist covering daily and emerging issues for Thomson Reuters Regulatory Intelligence (TRRI). This article is based on his recent report on the Marriott data breach.

Banks have avoided the major scandals over misuse of personal data and massive data breaches hitting social media and other sectors. But the threat is growing as bad actors become more sophisticated in their use of technology and dark markets to turn data into cash, and banks' digital operations expand to unfamiliar territory.

The recent Marriott International data breach hit close to home for financial firms, exposing the personal financial data of 500 million customer accounts typically linked to bank-issued credit cards. Under the European Union's General Data Protection Regulation (GDPR) such a large-scale cyber-event could result in billion-dollar fines.

The obvious takeaway from the case was that cyber criminals go where the money is—and Marriott's trove of high-end frequent travelers offered a rich prize. The breach also showed the evolving threat of cyber-criminals using high-tech skills to devastating effect.

Financial services firms have a long history of protecting financial assets but have less experience in guarding shared data. The recent past has shown that personally identifiable information is coveted and can easily be turned into cash on the dark web. And rogue state-funded hackers suspected in many of the incidents may be the most difficult to thwart.

Bank compliance officers report that they routinely catch many hackers; but the Marriott case showed that sophisticated hackers working like a sleeper cell inside a company's network left the company less protected than it realized.

The Marriott breach remains under investigation by the company and regulators. But already it flashes warnings for financial firms. Here are five key concerns:

1. **The Marriott breach showed the security challenge of building online retail operations that banks could also face in their own expansion of online customer services.** In one recent example, the Financial Industry Regulatory Authority fined the large investment firm LPL Financial $2.5 million over alleged inadequate protection against cyber intrusions. The risk report issued by the U.S. Office of the Comptroller of the Currency (OCC) put cyber-attacks at the top of its list.

2. **The breach underscores the need for financial firms to have regular cybersecurity risk audits.** A foundational part of most cyber-defense programs, such audits were a key element of GDPR as well as the groundbreaking New York State Department of Financial Services cyber-regulations that took effect two years ago. ''Marriott should have had a well-resourced cybersecurity team in place to constantly probe their networks and systems for weaknesses, ideally scaled via

incentivized ethical hackers. Had this been the case, such an extended breach simply could not have happened," said Simon Migliano, head of research at Top10VPN.com, a cybersecurity research consultant.

3. **The problem for Marriott arose in its Starwood Hotels & Resorts unit acquired in 2016; this showed the risk of data protection in mergers and acquisitions, in which finance firms have broad exposure.** Investment bankers face due diligence responsibilities in which assessing cyber-risk is a key factor. More importantly, large banks and brokers are challenged with continually integrating sensitive data in acquired units as well as branch offices, foreign affiliates, counterparty ventures, and third party vendors.

4. **The breach showed that financial firms need to prepare for cyber-threats that OCC said were becoming "more sophisticated and more global."** Marriott reported that the intruders appeared to have penetrated the company's network deeply enough to use its encryption tools to avoid detection over a period of years. Cyber-attackers frequently cover their tracks by creating layers of network code that disguises the source of intrusions. The Securities and Exchange Commission has called for more funding to meet complex cyber-risks and to remain relevant as fintech takes over the securities industry. The OCC has warned bankers that online attacks are "increasing in speed and sophistication."

5. **The new attack shows that compliance teams must have an enterprise-wide overview of vulnerabilities in personal data used by the firm.** Compliance must play a key role in mitigating regulatory and reputational risk, especially in spotting and reporting events quickly. Many regulators are now requiring notification within 72 hours.

"Breaches are inevitable," Migliano, of Top10VPN.com, said. "All it takes is a single staff member to click on a phishing email or a hacker to stumble on a new vulnerability. The only effective cyber-defense strategy is to accept that reality, get on the front foot, and focus on detecting intrusions and vulnerabilities as rapidly as possible and responding in kind to minimize their impact."

FROM THE EDITORS

As the Supreme Court Hears Arguments in *Lorenzo*, Liability Hangs in the Balance

Early in December, the U.S. Supreme Court heard arguments in *Lorenzo v. the Securities and Exchange Commission (SEC)*, a case that could potentially impact how the courts assess material misstatements, liability in securities fraud, and even whether simply passing on false information constitutes fraud.

Further, the case could likely upend the strict elements on misstatements and fraudulent-scheme claims set forth in the High Court's 2011 decision in *Janus Capital Group, Inc. v. First Derivative Traders*.

During the *Lorenzo* arguments, the eight justices took up a September 2017 ruling by the U.S. Court of Appeals for the D.C. Circuit that had found former investment banker Francis Lorenzo liable for his role in a scheme to defraud investors when he sent misleading emails about Waste2Energy Holdings, Inc., a clean energy start-up and then-client of Lorenzo's. (Newly appointed Justice Brett Kavanaugh did not hear arguments in the case because he was a member of the three-judge appeals court panel that previously reviewed the issue.)

It appeared to Supreme Court watchers that the justices hearing Lorenzo were possibly signaling their collective reluctance to further narrow the definition of who can be held liable for violating securities laws. Observers noted that many of the justices seemed to agree with the SEC, which in 2015 had fined Lorenzo $15,000 and banned him for life from working in the securities industry; however at least two justices—Chief Justice John Roberts and Justice Neil Gorsuch—seemed to take up Lorenzo's side.

The crux of the *Lorenzo* case stems from whether a person who did not *personally* make fraudulent statements but knowingly passed them along can be found liable for engaging in a fraudulent scheme. In *Janus*—which the D.C. Circuit cited in throwing out Lorenzo's liability over the false statements, but not the SEC charges of participating in a fraudulent scheme—the Supreme Court limited the scope of who can be held liable for false statements to those with ultimate authority over the statements.

The appeals panel said the fraudulent scheme charges had merit because Lorenzo knowingly produced and sent the false statements in the emails.

During the arguments before the Supreme Court, Lorenzo's attorney contended that sending emails was not inherently deceptive, which prompted Justice Ruth Bader Ginsburg to note that the emails contained a "succession of untruths."

Lorenzo side also argued that the SEC is overreaching in trying to attach liability as primary violators of securities laws to people who at most are liable for aiding and abetting fraudulent schemes. Indeed, that argument seemed to carry some weight with some of the justices.

The Supreme Court must rule in the case by the end of June, and *Wall Street Lawyer* will be keeping a keen eye on this one.

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.