JONES DAY

MARCH 2016

COMMENTARY

Cybersecurity's Moment and What it Means for Financial Services

The recent announcement of President Barack Obama's Cybersecurity National Action Plan, with programs aimed at improving the security of public and private data,[1] is a reminder that cybersecurity—including identifying, defending against, recovering from, and notifying others about cyber attacks—is having its moment.

With the world becoming ever more connected, the number of cyber attacks, and the level of sophistication of those attacks, continues to increase. The goals of cyber attackers are evolving from traditional criminal activities to attacks aimed at disrupting major infrastructure and economic activity, and the financial sector is a particularly appealing target.[2] Significantly, the impact of an attack is not isolated to the target entity—it can affect partners, vendors, customers, consumers, even entire markets. As such, the growing recognition of the threat and the urgency to act by regulatory agencies, Congress, and the president himself is hardly surprising. Using a variety of tools and methods at its disposal, the federal government is putting ever more emphasis on cybersecurity as a core national priority.

While it would be impractical to review all federal cybersecurity activity over the last year, certain actions, and the trends they indicate, are of particular interest and relevance to the financial services sector.[3]

Cyber-Related Sanctions List

In April 2015, the president issued an executive order titled "Blocking the Property of Persons Engaging in Significant Malicious Cyber-Enabled Activities."[4] A first of its kind, the executive order imposes sanctions on foreign persons who engage in significant cyber attacks against U.S. interests and was issued as part of a comprehensive, "whole-of-government strategy" to address cyber threats to the U.S.[5]

In particular, the order was designed to combat cyber threats to both national security and U.S. economic interests, including attacks on critical infrastructure, attacks on computers and computer networks, and attacks that misappropriate funds or private personal or commercial information (such as credit card data or trade secrets) for commercial advantage or gain.[6] The key is that the activities must pose a "significant threat" to "national security, foreign policy, or economic health or financial stability" in order to be sanctionable.[7] In other words, the presidential action focuses on the "most significant cyber threats we face,"[8] the "worst

© 2016 Jones Day. All rights reserved.

of the worst," with the intention to use this tool in a targeted manner only against extraordinary threats beyond the reach of other diplomatic and law enforcement means.[9]

This order was followed in December 2015 by the Office of Foreign Assets Control's ("OFAC") first set of regulations pursuant to this rule, the Cyber-Related Sanctions Regulations.[10] These initial regulations extend OFAC's existing sanctions regime to persons pursuing malicious cyber-enabled activities of the sort identified in the order. Specifically, when a person is designated on OFAC's Specially Designated Nationals and Blocked Persons ("SDN") list, that person's property and interests in property that are in the United States or are in the possession or control of a U.S. person must be blocked.[11] This includes money, deposits, debts, stocks, bonds, mortgages, and any number of other financial instruments that may be held or received by a U.S. financial institution.[12] Even when funds or credit owned by a person on the SDN list are just passing through a U.S. financial institution as part of a transaction, that institution must block that property in an account at the institution.[13] Simply put, with limited exceptions, when property of a blocked person is found at a U.S. financial institution, it must be put into a blocked account and left alone unless OFAC authorizes otherwise. As a practical effect, U.S. financial institutions, like other U.S. persons, generally cannot receive blocked property as payment for any business transaction with a blocked person or an entity owned by such a person.[14]

By issuing this order and these rules, the executive branch appears to recognize that the threat is broader than that typically posed by other criminal activity, and the challenge in combating it is often more than traditional law enforcement is equipped to handle, even as the executive branch increases efforts on that front as well.[15] Compliance with OFAC's sanctions programs may impose a short-term burden on financial institutions, but these sanctions ultimately can serve to protect such institutions as well, for example by limiting the resources of would-be attackers, providing a further incentive to ensure that procedures to handle blocked property are implemented appropriately.

Cybersecurity for the Securities Industry

Also in April 2015, the Securities & Exchange Commission ("SEC") released cybersecurity guidance for investment companies and investment advisors.[16] Though the SEC recognized that preventing every cyber attack is impossible, the guidance (while not mandatory) highlights certain ways in which firms should think about cyber risk in order to mitigate the impact of cyber attacks, particularly as they relate to compliance with federal securities laws.[17] The SEC suggests conducting regular cybersecurity assessments that will allow a firm to "better prioritize and mitigate risk."[18] These assessments may allow the firm to understand what data it collects, the threats and vulnerabilities it faces, the impact of a breach, the existing controls in place to protect against threats, and the effectiveness of the firm's governance structure in managing cybersecurity risks.[19] The guidance encourages firms to create a strategy "designed to prevent, detect and respond to cybersecurity threats" that would include data access controls, encryption, monitoring for intrusions and data loss, data backup procedures, and development of an incident response plan.[20] According to the SEC, such strategies should be implemented using written policies and procedures and training so that employees understand the potential threats and the measures used to counter such threats.[21] The SEC also cautioned firms to pay attention to the cybersecurity measures of third-party services providers.

In addition, on September 15, 2015, the SEC announced its 2015 Cybersecurity Examination Initiative, outlining factors for consideration in its second cybersecurity examination sweep.[22] This initiative is designed to assess the cybersecurity preparedness of securities firms, including the ability to protect customer data and the implementation of basic controls.[23] Specifically, the SEC plans to look at governance and risk assessment, access rights and controls, data loss prevention, vendor management, training, and incident response.

Only a few days after issuing this alert on the new examination initiative, and in many ways underscoring the April 2015 guidance, the SEC announced a settlement with investment advisor R.T. Jones Capital Equities Management ("R.T. Jones") for failing to have in place cybersecurity policies and procedures "reasonably designed" to protect the personal information of clients and nonclients in its possession.[24] The settlement alleged that this failure was a violation of Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30(a)), known as the "Safeguards Rule," and represents resolution of the first SEC enforcement action of its kind.[25] Notably, though a breach

did occur, the settlement does not indicate that there was any actual harm to those whose information was potentially exposed; indeed, it does not appear that R.T. Jones was even able to definitively determine whether personal information was revealed.[26] As revealed in the settlement, the simple fact that the firm did not use sufficient care and rendered personal information "vulnerable" was a sufficient basis for the SEC to bring an enforcement action.[27]

Taken together, these activities, among others, demonstrate the SEC's focus on cybersecurity and data protection as priorities for the foreseeable future. As such, the failure to implement appropriate policies and procedures may leave firms at risk for both cyber attacks and regulatory action.

FFIEC Cybersecurity Assessment Tool

In June 2015, the Federal Financial Institutions Examination Council ("FFIEC") released its long-awaited Cybersecurity Assessment Tool ("CAT").[28] This tool provides a process through which financial institutions, using a "repeatable and measurable process," can "identify their risks and determine their cybersecurity preparedness," in terms of detecting, defending against, and recovering from risk.[29] Specifically, the CAT guides financial companies through an evaluation of their "inherent" cyber risks (looking at the type and seriousness of cybersecurity risks) as well as their cybersecurity "maturity" level (the controls and risk management practices in place to mitigate risk).[30] By comparing risks and maturity levels, and by ensuring that such an assessment has board-level oversight, the CAT provides a process that helps companies identify gaps, set priorities for investment and improvement, and align risks with controls on an ongoing basis.

As with the SEC's cyber guidance, though no firm is strictly required to implement the CAT, or having implemented it, to adjust either risk or maturity,[31] the FFIEC clearly expects financial institutions to regularly assess cyber risks and cyber protections in place to determine whether they are properly aligned.

The Limits of FTC Authority

In August 2015, the Third Circuit Court of Appeals ruled on Wyndham Worldwide's challenge to the Federal Trade Commission's ("FTC") authority in regulating data security.[32] The FTC originally sued Wyndham for failing to adequately protect customer data that was disclosed in a series of breaches, arguing that Wyndham's conduct constituted unfair and deceptive practices under the FTC's "Section 5" authority.[33] The district court ruled in favor of the FTC on Wyndham's motion to dismiss.[34] On appeal, the Third Circuit upheld the use of the FTC's "unfairness" authority to regulate cybersecurity practices and further found that Wyndham had fair notice that its data protection practices could be deemed unfair.[35]

After the Third Circuit's ruling, the FTC settled with Wyndham, requiring Wyndham to implement a comprehensive cybersecurity program and subjecting the company to 20 years of audits.[36] The Third Circuit's decision may further embolden the FTC and other agencies to use their existing authority in future cybersecurity matters where financial companies fall short in protecting systems and data.

CFTC Proposed Testing Rules

In mid-December of 2015, the Commodity Futures Trading Commission ("CFTC") proposed rules governing the testing of cybersecurity capabilities of certain regulated entities.[37] These rules call for five specific types of cybersecurity testing and would require board-level involvement in reviewing testing results.[38]

Importantly, the CFTC does not view these rules as being particularly new or radical, but rather formally requiring best practices in cybersecurity that it believes many regulated entities should already be following.[39] Firms should expect that the CFTC will be looking at cybersecurity implementation to ensure that regulated entities are taking appropriate action to protect their systems and the broader market.

Cybersecurity Information Sharing Act

Also in mid-December, Congress passed and the president signed into law the Cybersecurity Information Sharing Act ("CISA"), which had been debated in one form or another since 2013.[40] CISA promotes the sharing of cyber threat information between private businesses and the government in order to better detect and defend against cyber attacks, in large part by offering liability protections to private entities.[41] On February 16, 2016, the Department of Homeland Security

("DHS") issued guidance on information sharing as required by CISA, providing additional detail on the processes for sharing information between the government and the private sector.[42] These processes, and the protections they provide, are designed to allow for more robust sharing of threat information to and from the government, with the goal of leading to better detection of and protection from cyber threats.[43]

Cybersecurity National Action Plan

The focus on cybersecurity was emphasized in the president's February 2016 Cybersecurity National Action Plan. While much of the $19 billion proposed under the plan is unlikely to survive the budget process, the dramatic 35 percent increase over prior year cybersecurity spending is a reflection of the growing significance of cybersecurity in the national security and economic policy discussion.[44]

The plan puts a particular emphasis on protecting not only governmental systems but private sector systems as well, and on encouraging public-private coordination, as reflected by the following:

- The mandate of the Commission on Enhancing National Cybersecurity;[45]
- The creation of a National Center for Cybersecurity Resilience, to allow companies to test security in a "contained environment";[46] and
- The directive to DHS to double the number of cybersecurity advisors to assist the private sector in assessing cybersecurity readiness and in implementing best practices.[47]

The administration is further promising a spring release of a policy for "national cyber incident coordination" and a methodology for "evaluating cyber incidents" that it says will allow for better public-private communication and response to cyber threats.[48]

CFPB Enforcement Action

On March 2, 2016, the Consumer Financial Protection Bureau ("CFPB") asserted its interest in cybersecurity in a settlement with Dwolla, an online payments system.[49] According to the CFPB's consent order, Dwolla promoted its services as safe and secure, and made specific representations that its data protection program was compliant with—and even exceeded—industry standards, that personal data was encrypted, and that mobile applications were secure.[50]

In fact, according to the CFPB, these claims were untrue. In the consent order, the CFPB alleged that Dwolla's procedures failed to meet industry standards, left personal data unencrypted, and allowed applications to be released without testing their security.[51] Moreover, in language mirroring that used by the FTC in *Wyndham*,[52] the CFPB's consent order more generally found that Dwolla, despite promises of safety and security, "failed to employ reasonable and appropriate measures to protect data obtained from consumers from unauthorized access," including appropriate policies governing the collection and storage of personal information, adequate risk assessments, and adequate employee training on data security.[53] Notably, the CFPB did not allege that a breach had actually taken place; the fact that Dwolla put customer data at risk was sufficient.

That the CFPB is now active in regulating cybersecurity should come as no surprise, particularly after the FTC and SEC actions. Indeed, Dwolla's deceptive statements simplified the CFPB's task, as the Bureau did not have to argue that certain security protocols are necessary in every case, only that Dwolla's stated policies fell short of both its general and specific affirmative representations about security. That said, the CFPB, like the FTC before it, appears to be making clear its view that, for a company like Dwolla, the deficiencies identified mean that the cybersecurity program is not reasonable and appropriate.[54]

Conclusions and Lessons

So what does this all mean? In looking at these actions, three connected themes emerge.

The Future of Federal Cybersecurity Activity. The breadth of agencies and entities involved in cybersecurity demonstrates that it is not a partisan issue likely to go away over the next election cycle. Though the president's particular agenda may not be fully implemented, cybersecurity has risen in prominence as the federal government more fully appreciates the threats

to security and economic life. As the threat landscape continues to evolve, companies, and particularly those in such critical infrastructure industries like financial services, can expect more rules governing data protection practices and the continued attention of supervisory and enforcement authorities.

Public-Private Coordination. The government appears to believe that a public-private partnership is the only feasible path forward in cybersecurity. Information sharing is a critical piece of the comprehensive puzzle that also includes law enforcement efforts, government identification and encouragement of best practices, and private sector risk assessment and cybersecurity implementation.

Financial services firms, as lynchpins of national economic health, have the opportunity to be at the center of this emerging partnership. Firms should weigh the risks and costs of broad information sharing and partnering with federal agencies against the apparent rewards. In this context, those rewards may include an ability to help shape federal cyber policy as it develops to limit the regulatory burden while also enabling an industry-driven system of robust and thoughtful protections and policies.

Best Practices and Existing Law. Though regulators have been hesitant to mandate specific cybersecurity practices,[54] recognizing that every firm has its own particular situation and appropriate methodology, they are of one voice in pushing firms to conduct risk assessments to evaluate their current cybersecurity situations and to implement appropriate practices to defend against, mitigate, and respond to cyber attacks. The rules and guidance from regulators can be taken as warnings of regulatory expectations. In cases where a firm fails to meet agency expectations, particularly in the event of preventable cybersecurity incidents, regulators may be increasingly willing to deploy existing legal authority to bring supervisory and enforcement actions, and to test the bounds of their authorities even as the parameters of that authority continue to evolve.

Moreover, aside from the regulators themselves, partners and corporate customers, as well as consumers, may increasingly demand a robust cybersecurity framework before sharing data and exposing their systems to another entity, lest they open themselves to unnecessary risk. By treating cybersecurity as an enterprise-wide risk management issue, thoughtfully implementing best practices, and working where possible with regulators, firms can protect their systems, create a more secure business climate, and mitigate the operational, reputational, legal, regulatory, and financial risk imposed by cyber threats.

Lawyer Contacts

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com/contactus/.

Lisa M. Ledbetter
Washington
+1.202.879.3933
lledbetter@jonesday.com

Todd S. McClelland
Atlanta
+1.404.581.8326
tmcclelland@jonesday.com

Mauricio F. Paez
New York
+1.212.326.7889
mfpaez@jonesday.com

Albert J. Rota
Dallas
+1.214.969.3698
ajrota@jonesday.com

C. Hunter Wiggins
Chicago
+1.312.269.1554
Washington
+1.202.879.7656
hwiggins@jonesday.com

Jay Johnson
Dallas
+1.214.969.3788
jjohnson@jonesday.com

Michael G. Morgan
Los Angeles
+1.213.243.2432
mgmorgan@jonesday.com

Eitan Levisohn
Washington
+1.202.879.3881
elevisohn@jonesday.com

Endnotes

1 Fact Sheet, The White House Office of the Press Secretary, Cybersecurity National Action Plan (Feb. 9, 2016) ("CNAP Fact Sheet").

2 By one estimate, the financial services sector has 300 percent more attacks than other industries. Press Release, RaytheonlWebsense, "Websense Security Labs Reveals Top Cyber Threat Trends in 2015 Financial Services Drill-Down Report" (June 23, 2015). Another survey found that financial services is one of the three industries most affected by security incidents. Verizon, 2015 Data Breach Investigations Report (2015).

3 While this *Commentary* focuses on federal activity, financial services firms should also make note of the uptick in state regulatory activity as well. For instance, New York State's Department of Financial Services has floated ideas for potential regulatory action in the cybersecurity space. *See* Letter from Anthony J. Albanese, Acting Superintendent of Financial Services, to Financial and Banking Information Infrastructure Committee ("FBIIC") Members (Nov. 9, 2015) (discussing potential new cybersecurity regulations); *see also* CA Dep't of Justice, California Data Breach Report February 2016 (Feb. 2016) (setting out minimum cybersecurity controls that all organizations should implement). For additional information on the breach report, see "California Attorney General Releases Data Breach Report," Jones Day Commentary (Feb. 2016).

4 Exec. Order No. 13694, 80 Fed. Reg. 18077 (April 2, 2015) ("Sanctions Order"). For additional information on the Sanctions Order, see "OFAC Sanctions Update: U.S. Government Authorizes Sanctions Related to Malicious Cyber-Related Activities, Encourages Telecom Investment in Cuba," Jones Day Commentary (April 2015).

5 Statement by the President on Executive Order "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," 2015 Daily Comp. Pres. Doc. 223 (April 1, 2015) ("Statement"); Transcript, The White House Office of the Press Secretary, On-the-Record Press Call on the President's Executive Order, "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities" (April 2, 2015) ("Press Call").

6 Sanctions Order, 80 Fed. Reg. at 18077; Fact Sheet, "The White House Office of the Press Secretary, Executive Order Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities" (April 1, 2015). The Sanctions Order also provides for sanctions against those who those who knowingly take advantage of stolen trade secrets. Sanctions Order, 80 Fed. Reg. at 18077.

7 *Id.*

8 Frequently Asked Questions Related to Executive Order 13694 "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," Office of Foreign Assets Control.

9 Press Call.

10 Cyber-Related Sanctions Regulations, 80 Fed. Reg. 81752 (issued Dec. 31, 2015) (codified at 17 C.F.R. pt. 578). As OFAC has made clear, future regulations pursuant to the Sanctions Order are to be expected. *Id.* at 81753.

11 *Id.* at 81754.

12 *Id.* at 81755. As with existing sanctions programs, the rule covers a broad range of U.S. financial institutions, including banks, securities broker-dealers, commodity futures and options brokers and dealers, investment companies, employee benefit plans and U.S. holding companies, U.S. affiliates and U.S. subsidiaries of financial institutions, as well as securities and commodities exchanges themselves, and the U.S. branches of foreign institutions. *Id.* at 81756.

13 *Id.*

14 *Id.* at 81754, 81756.

15 *See* CNAP Fact Sheet (noting increased funding by the Department of Justice).

16 Sec. & Exch. Comm'n, Guidance Update No. 2015-02, Cybersecurity Guidance (April 2015).

17 *Id.* at 2-3.

18 *Id.* at 2.

19 *Id.* at 1-2.

20 *Id.* at 2.

21 *Id.* The guidance also suggests training investors and clients about how to reduce cybersecurity risks to their accounts. *Id.*

22 Sec. & Exch. Comm'n, Off. of Compliance Inspections and Examinations, National Exam Program Risk Alert Vol. iv, issue 8, OCIE's 2015 Cybersecurity Examination Risk Initiative (Sept. 15, 2015) ("OCIE Initiative"). The first sweep was announced in April 2014, with results published in February 2015. *Id* at 1. For more information on those results, *see* "FINRA and SEC Issue Cybersecurity Reports Identifying Common Industry Practices," Jones Day *Commentary* (Feb. 2015). In January 2016, the SEC made clear that advancing these examination efforts was a 2016 priority. Sec. & Exch. Comm'n, Off. of Compliance Inspections and Examinations, National Exam Program Examination Priorities for 2016 at 3 (Jan. 11, 2016).

23 OCIE Initiative at 1-2.

24. R.T. Jones Capital Equities Mgmt., Inc., Release No. IA 4204, File No. 3-16827, 2015 WL 5560846 at 3 (Sept. 22, 2015) (Order).

25 *Id.* at 3. Though the SEC cited R.T. Jones for failing to adopt written procedures, as required by the rule, it is clear from the settlement that the underlying issue was the lack of any proper procedure, written or not. *Id.*

26 *Id.* at 2.

27 *Id.* at 1, 3.

28 Fed. Fin. Institutions Examination Couns., Cybersecurity Assessment Tool (June 2015) ("CAT").

29 Fed. Fin. Institutions Examination Couns., Cybersecurity Assessment Tool, Overview for Chief Executive Officers and Boards of Directors 1 (June 2015).

30 CAT at 3-8. In many ways, the CAT reflects the SEC's April guidance (discussed above) in terms of assessing cyber risk, identifying existing controls, and aligning a cybersecurity program.

31 It should be noted that FFIEC examiners are already using the tool during examinations, at least for data collection purposes, while some state regulators are mandating that banks conduct assessments. *See, e.g.*, Off. of the Comptroller of the Currency, OCC Bull. 2015-31, FFIEC Cybersecurity Assessment Tool (June 30, 2015); Texas Dep't of Banking, Industry Notice 2015-8, Cybersecurity Assessments & the FFIEC Cybersecurity Assessment Tool (Sept. 15, 2015) (requiring

assessments be completed by December 31, 2015 and recommending use of the FFIEC tool); Letter from David J. Cotney, Commissioner of Banks, to Chief Executive Officers (Sept. 30, 2015) (requiring assessments be completed by March 31, 2016 and recommending use of the FFIEC tool). The FFIEC recently closed a comment period on the tool, and it is unclear if and when it may be updated.

32 *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015) ("*Wyndham Appeal*").

33 The FTC's authority under Section 5 of the Federal Trade Commission Act is codified at 15 U.S.C. § 45.

34 *FTC v. Wyndham Worldwide Corp.,* 10 F. Supp.3d 602 (D.N.J. 2014). Several arguments were raised at the district court that were not raised on appeal.

35 *Wyndham Appeal* at 243-260. The Third Circuit did not reach a conclusion as to whether Wyndham's alleged issues in fact failed the cost-benefit analysis of the unfairness test, only that the company had notice that the practices could be found unfair. *Id*. at 256.

36 Stipulation and Order for Injunction at 4-10, *FTC v. Wyndham Worldwide Corp*., No. 13-1887 (D.N.J Dec. 11, 2015).

37 System Safeguards Testing Requirements for Derivatives Clearing Organizations, 80 Fed. Reg. 80113 (proposed December 23, 2015) (to be codified at 17 C.F.R. pt. 39); System Safeguards Testing Requirements, 80 Fed. Reg. 80139 (proposed December 23, 2015) (to be codified at 17 C.F.R. pts. 37, 38, 49).

38 System Safeguards Testing Requirements for Derivatives Clearing Organizations, 80 Fed. Reg. at 80117–80124. As the proposals are substantively similar on these requirements, this commentary cites only to one proposal.

39 *Id*. at 80126-80131.

40 Cybersecurity Information Sharing Act of 2015, Pub. L. No. 114-113 (2015). This follows a February 2015 Executive Order designed to encourage and enable greater cyber threat information sharing between government and the private sector and among private sector entities. Exec. Order No. 13691, 80 Fed. Reg. 0349 (Feb. 13, 2015).

41 CISA at Title I. While many in the business community supported CISA, the passage of CISA is not without controversy, with many privacy advocates arguing against it.

42 Links to the guidance are available at the United States Computer Emergency Readiness Team website, US-CERT Automated Indicator Sharing.

43 It should be noted that additional guidance is expected, as are hearings on the implementation of CISA. Tim Starks, "Prospects for the Encryption Commission," Politico (Feb. 25, 2016 11:20 AM).

44 CNAP Fact Sheet.

45 Exec. Order No. 13718, 81 Fed. Reg. 7441 (Feb. 9, 2016).

46 CNAP Fact Sheet.

47 *Id*.

48 *Id*.

49 Dwolla, Inc., 2016-CFPB-0007 (Mar. 2, 2016) (Consent Order) ("Dwolla Order").

50 *Id*. at 5-6. Among other claims, Dwolla stated that its systems were compliant with the standard set forth by the Payment Card Industry ("PCI") Security Standards Counsel, an "open global forum that issues the data-security compliance standards for cardholder." *Id*. at 6. *See* Payment Card Industry, Data Security Standard Version 3.1 (April 2015).

51 Dwolla Order at 6-10.

52 Complaint at 18-19, *FTC v. Wyndham Worldwide Corp*., No. 13-1887 (D.N.J Dec. 11, 2015).

53 Dwolla Order at 6-8. While some or all of the CFPB's specific findings may also indicate a failure to comply with PCI standards, the consent order discusses these issues not merely as a failure to comply with specific PCI standards (despite Dwolla's claims that it was compliant) but in the more general context of a failure to implement reasonable and appropriate measures despite assurances of safety and security.

54 Whether the CFPB, had it not been able to argue deception, would have taken a cue from the FTC and brought an unfairness action for insufficient controls is an open question.

55 Even the CFTC testing practices, which call for particular kinds of tests, are described at a fairly high level, and the commissioners recognize the need for individual implementation strategies. System Safeguards Testing Requirements for Derivatives Clearing Organizations (Statement of Commissioner Sharon Y. Bowen), 80 Fed. Reg. at 80113, 80138 ("[W]e must be careful not to mandate a one-size-fits-all standard because firms are different.").

Jones Day publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information purposes only and may not be quoted or referred to in any other publication or proceeding without the prior written consent of the Firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our "Contact Us" form, which can be found on our website at www.jonesday.com. The mailing of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship. The views set forth herein are the personal views of the authors and do not necessarily reflect those of the Firm.