Debevoise & Plimpton

Breach Reading 2.0

A Midyear Review of Cybersecurity & Data Privacy

2016

Debevoise & Plimpton

Breach Reading 2.0:

A Midyear Review of Cybersecurity & Data Privacy

Contents

Introduction

By: Bruce Yannett

Welcome to Breach Reading 2.0 – an update for in-house counsel, executives and directors on the latest threats to data security and privacy and how the law now expects companies to manage those threats. Threat vectors are dynamic and ever-evolving, and legal scrutiny of corporate conduct likewise is ever-intensifying.

Breach Reading 2.0 includes both original articles and refreshed versions of the client updates that we issue from time to time throughout the year. Our goal is to deliver the news, the legal analysis, and even some practical pointers, all in a manner that hopefully is accessible to lawyers and non-lawyers alike.

We'd love to hear from you whether we've met that goal. Your feedback is welcome at breachreading@debevoise.com. You can also use that email address to sign up for our updates – which are always available too at our cyber and privacy practice page, www.debevoise.data.com.

Enjoy Breach Reading, and enjoy the summer.

SEC Oversight and Breach Disclosures

"Get me everything on everybody."

Since we last published breach reading, the Securities and Exchange Commission ("SEC") has used its regulatory authority to penalize investment advisers and registered broker-dealers that fail to implement adequate written cybersecurity programs. Combined with the announcement that this area remains a focus for the Office of Compliance Inspections and Examinations ("OCIE") during examinations, the message is clear: implementing robust

cybersecurity policies and procedures is not just a best practice, but a regulatory requirement.

In the past 12 months, the SEC issued penalties in three instances for inadequate cybersecurity programs. Discussed more fully in our client update republished herein, investment adviser R.T. Jones Capital Equities Management, Inc. ("R.T. Jones") was the first subject of the SEC's cybersecurity enforcement authority after the issuance of OCIE's revised guidance in September 2015. R.T. Jones received a $75,000 fine for failing to maintain written cybersecurity policies and procedures. The SEC specifically noted it accepted the amount of R.T. Jones' settlement offer based in part on its remedial efforts to appoint an information security manager, draft written cybersecurity policies and retain a cybersecurity firm to provide ongoing reports and advice on its cyber program.

In April 2016, registered broker-dealer Craig Scott Capital, LLC ("CSC") was fined $100,000 and its two co-owners were fined $25,000 each for deficient cybersecurity policies and procedures. CSC used non-firm email addresses – including the personal email addresses of the co-owners – to receive and process sensitive customer information and electronic faxes. Though CSC had cybersecurity policies in place, the SEC found they were not "reasonably designed to protect customer records and information." Specifically the written cybersecurity policies included placeholders to be filled in later (*e.g.*, "[The Firm] has adopted procedures to protect customer information, including the following: [methods]."), failed to describe how information received via eFax should be handled, and included procedures CSC was not yet following, such as encrypting customer records transmitted to remote devices. The SEC found CSC also failed to follow the record preservation requirements of the Exchange Act after receiving information via

eFax because the non-firm emails were not automatically backed up and retained by the firm.

Then, in June 2016, the SEC issued a $1,000,000 fine against Morgan Stanley in connection with the breach of confidential consumer information on its systems. From 2011 until 2014, a Morgan Stanley employee exploited flaws in the technical controls in place on the firm's financial portals that allowed him to access customer information without proper authorization, including customers' full names, account numbers, phone numbers, street addresses, account balances and information about fixed income holdings. The employee then bypassed controls meant to prevent the transfer of information off of firm systems and moved personal information from about 730,000 customer accounts to a personal server. Subsequently, a third party breached the personal server and posted the customer information for sale online. Morgan Stanley discovered the information for sale during a routine Internet sweep. The SEC assessed the fine even though Morgan Stanley already had cybersecurity policies and procedures in place, taking issue instead with the firm's ineffective authorization controls, which failed to limit access to the portals, and with Morgan Stanley's failure to test and audit the adequacy of these technical controls for a 10-year period since their creation. The SEC's decision came in stark contrast to the Federal Trade Commission ("FTC"), which in August 2015 had informed Morgan Stanley it had closed its investigation into the same matter without taking any enforcement action.

Each of these enforcement actions represents important guidance for the SEC's expectations for the cybersecurity programs of investment advisers and broker-dealers. Given the small number of such actions, however, SEC regulated entities should also look to the underlying regulations and OCIE's risk alerts. Indeed, these actions

represent the tip of the iceberg for the SEC. The Head of the SEC's Enforcement Division warned in an April 2016 webcast that "[t]here'll be others coming down the pike."

Regulation S-P has served as the primary means for the SEC's enforcement authority in the cybersecurity area. Rule 30(a) of Regulation S-P, 17 C.F.R. § 248.30, known commonly as the "Safeguards Rule," requires investment advisers and broker-dealers to "adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records." These policies and procedures should be "reasonably designed to:

(1) Insure the security and confidentiality of customer records and information;

(2) Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and

(3) Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer."

What this practically means is more fully described in OCIE's September 15, 2015 Risk Alert, which we explore in detail in the client update included here. In that Risk Alert, OCIE highlighted a second round of examinations of the cybersecurity practices and procedures of registered entities. Notably, OCIE identified six specific categories upon which it would focus, including (1) governance and risk assessment; (2) access rights and controls; (3) data loss prevention; (4) vendor management; (5) training; and (6) incident response.

The SEC's actions and guidance in the past year reflect a growing trend among regulators to convert cybersecurity best practices into legal and regulatory requirements. The Morgan Stanley action in particular shows that the SEC will not defer to the decisions of other regulators such as the FTC in reviewing the actions of registered entities.

And the CSC decision drives home the point that simply using an off-the-shelf model policy not specifically tailored to the practices of your firm will not be enough to satisfy the SEC, especially if your actual practices aren't aligned with the policy. Investment advisers and broker-dealers would do well to implement a robust program with written policies and procedures that cover the categories specified by the OCIE guidance, reflect a well-thought out approach to the threats faced by your firm and accurately capture the actual practices at your firm.

How Companies Adjust Their SEC Filings Following a Cybersecurity Event

In the wake of a breach, hack or other cybersecurity event, determining what to disclose to the SEC and the public, and when to disclose it, can be a monumental task. One starting place is to look at what other companies have done in response to similar events. Based on a survey of Fortune 100 companies that experienced cybersecurity events between 2013 and 2015, we have observed the following trends in subsequent company disclosures in public filings:

- **Companies generally do not file 8-Ks or make other supplemental filings following a cybersecurity incident**. Cybersecurity events are often first publicly revealed through media coverage, rather than an announcement by the breached company itself. Even following media coverage of a breach, companies in our survey rarely issued 8-Ks, generally waiting instead for a periodic filing. There are good reasons to hold off on disclosing a cybersecurity event in an 8-K shortly after it is initially reported in the media – chief among them, the early reports about an incident are often incorrect. As a result, companies that rush to issue an 8-K before completing a thorough investigation risk that their disclosure will be incomplete, or worse yet, inaccurate.
- **Not all companies update their risk factors immediately following a cybersecurity incident**. About half of the companies surveyed updated or added a cybersecurity risk factor in their first periodic filings following an incident. This was driven in part by the fact that companies were particularly

unlikely to update their risk factors relating to cybersecurity in a 10-Q.

- **Companies generally do, however, update their risk factors in their annual 10-K filings**. Companies generally update cybersecurity risk factors in 10-K filings following an event, even if those risk factors were already updated in an intervening 10-Q. Within the survey data, more than 75% of companies made such an update in their next 10-K. Those companies that previously disclosed a cybersecurity event either through an 8-K or 10-Q, used subsequent annual reports as an opportunity to further tailor their risk factor discussion.
- **Most companies disclose the specific cybersecurity event only once, if they reference the cybersecurity event at all**. A majority of the companies surveyed did not engage in continued disclosure after an initial company disclosure reporting a specific cybersecurity event, whether this occurred in a periodic or 8-K filing. Moreover, some companies did not expressly reference an intrusion even when updating their risk factors in response. Instead, they updated their risk factors to reflect a general risk relating to cybersecurity, without disclosing whether a specific incident had occurred. This approach may be more appropriate when the particular cybersecurity event is circumscribed in nature or duration, thus having a more limited impact on the company's finances.
- **Companies that believe the cybersecurity event is material are more likely to make an 8-K filing and update their risk factors over the course of multiple filings**. Within the survey, companies with particularly severe or material cybersecurity events (*e.g.*, Anthem and Target) were exceptions to the above trends. Such companies made disclosures extending over several quarters and were less likely to wait until their 10-K filings to

make a disclosure. These companies were also among those that chose to make specific reference to the cybersecurity event in their risk factors. Unsurprisingly, companies facing the greatest exposure from a data breach report earlier, more frequently and more explicitly than companies with less exposure.

Trends in corporate responses to cybersecurity events will likely evolve as the accompanying law and policy changes, but at the moment it appears that corporations are not hastening to disclose related information in SEC filings outside the context of a very significant breach. Firms facing a cybersecurity event should always ensure their response is tailored to the particular intrusion.

Client Update:

The Shape of Things to Come: OCIE Announces Examination Priorities for 2016

The staff of the Securities and Exchange Commission (the "SEC") recently published a summary of the select priorities of the SEC's Office of Compliance Inspections and Examinations ("OCIE") in connection with the National Exam Program (the "2016 Priorities Summary").[1] The examination priorities for 2016 generally focus on the same themes as the 2015 priorities: (i) protecting retail investors; (ii) assessing market-wide risks; and (iii) using data analytics to identify signals of potential illegal activity.

Of particular interest to private equity fund sponsors, the 2016 priorities include: (i) a continued focus on fees and expenses; (ii) controls and disclosures associated with side-by-side management of clients with different fee structures; (iii) cybersecurity; (iv) private placements relying on Regulation D under the Securities Act of 1933; and (v) investment advisers who have not yet been examined. In view of the continued emphasis that the SEC is placing on private fund examinations and recent SEC enforcement actions involving private fund expense allocation issues and potential conflicts of interest – as well as our experience representing private equity firms being examined by OCIE – private equity fund sponsors should continue to be prepared for rigorous examinations on these issues.

---

[1] *Available at* http://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2016.pdf. For a summary of the 2015 examination priorities, see our client update, "What Will the 'Eyes and Ears' of the SEC Choose to See and Hear this Year? OCIE Announces Examination Priorities for 2015" (Feb. 4, 2015), *available at* http://www.debevoise.com/insights/publications/2015/02/what-will-the-eyes-and-ears-of-the-sec-choose.

FOCUS ON RETAIL INVESTORS AND INVESTORS SAVING FOR RETIREMENT

The 2016 Priorities Summary reflects the SEC's concerns about the evolving breadth of investment options available to retail investors. This set of examination priorities includes:

- *ReTIRE*. OCIE launched a multiyear examination initiative in June 2015 that focuses on SEC-registered investment advisers and broker-dealers with respect to the services they offer to investors with retirement accounts, including examining the reasonable basis for recommendations to investors, conflicts of interest, supervision and compliance controls and marketing and disclosure practices.
- *ETFs*. OCIE will review exchange-traded funds ("ETFs") for compliance with applicable exemptive relief, their unit creation and redemption process, sales strategies, trading practices and disclosures with respect to excessive portfolio concentration, primary and secondary market trading risks and suitability.
- *Fee Selection and Reverse Churning*. Where an adviser or dually registered adviser/broker dealer offers a variety of fee arrangements (*e.g.*, asset-based fees, hourly fees, wrap fees, commissions), OCIE will "focus on recommendations of account types and whether the recommendations are in the best interest of the retail investor at the inception of the arrangement and thereafter, including fees charged, services provided, and disclosures made about such arrangements."
- *Branch Office Supervision*. OCIE will focus on the supervision of registered representatives and investment adviser representatives in branch offices, including using data analytics to identify potentially inappropriate trading.

- *Variable Annuities*. OCIE will be assessing the suitability of sales of variable annuities to investors and the adequacy of disclosure and supervision of such sales.
- *Public Pension Advisers*. With respect to advisers to municipalities and other government entities, OCIE will be focusing on pay-to-play and the identification of undisclosed gifts and entertainment.

ASSESSING MARKET-WIDE RISKS

With respect to structural risks and trends, OCIE plans to focus on the following initiatives:

- *Cybersecurity*. OCIE is in the middle of its second initiative, launched in September 2015, to examine broker-dealers' and investment advisers' cybersecurity compliance and controls. OCIE states that it expects that these exams will include testing and assessment of firms' implementation of procedures and controls.[2]
- *Regulation Systems Compliance and Integrity ("SCI")*. SCI entities (*e.g.*, registered clearing agencies, alternative trading systems, plan processors and exempt clearing agencies) will be evaluated on whether they have "established, maintained, and enforced written policies and procedures reasonably designed to ensure the

[2] See our prior client updates: "SEC Sanctions Investment Adviser for Failing to Adopt Cybersecurity Policies and Procedures" (Sept. 24, 2015), *available at* http://www.debevoise.com/insights/publications/2015/09/sec-sanctions-investment-ad; "SEC Release Updated Cybersecurity Examination Guidelines" (Sept. 18, 2015), *available at* http://www.debevoise.com/insights/publications/2015/09/sec-releases-updated-cybersecurity-examinat; "SEC Issues Cybersecurity Guidance for Registered Investment Advisers and Funds" (May 7, 2015), available at http://www.debevoise.com/insights/publications/2015/05/sec-issues-cybersecurity-guidance; "SEC Regulation of Cybersecurity and Tech Risk Coverges," *Law360* (Oct. 23, 2015), *available at* http://www.law360.com/articles/718238/print?section=banking.

capacity, integrity, resiliency, availability, and security of their SCI systems."

- *Liquidity Controls*. OCIE expects to examine advisers to mutual funds, ETFs and hedge (and other private) funds with exposure to potentially illiquid fixed income securities and registered broker-dealers that have become new or expanding liquidity providers in the marketplace with respect to controls over market risk management, valuation, liquidity management, trading activity and regulatory capital.[3]
- *Clearing Agencies*. The SEC staff will conduct annual examinations of all clearing agencies that have been designated systemically important.

USING DATA ANALYTICS TO IDENTIFY SIGNALS OF POTENTIAL ILLEGAL ACTIVITY

OCIE plans to utilize its data analytics capabilities to focus on registrants that appear to be potentially engaged in fraudulent and/or other illegal activity. The examination initiatives will focus on: (i) individuals with a track record of misconduct and the firms that employ them; (ii) anti-money laundering programs of clearing and introducing broker-dealers (and whether the filing of the suspicious activity reports is consistent with their business models); (iii) pump and dump schemes and market manipulation by broker-dealers and transfer agents; (iv) excessive or otherwise inappropriate trading by

---

[3] This priority is likely linked to the SEC's focus on mutual fund liquidity, investments in derivatives and the challenges of managing a fixed income portfolio in a changing interest rate environment. *See, e.g.*, "Use of Derivatives by Registered Investment Companies and Business Development Companies," SEC Release No. IC-31933 (Dec. 11, 2015); "Open-End Fund Liquidity Risk Management Programs," SEC Release No. 33-9922, IC-31835 (Sep. 22, 2015); "Risk Management in Changing Fixed Income Market Conditions," IM Guidance Update No. 2014-01 (January 2014).

brokers and registered representatives; and (v) the promotion of new, complex and high-risk products and the related sales practices that can raise issues relating to suitability and breaches of fiduciary obligations.

OTHER INITIATIVES

OCIE expects to allocate examination resources to other priorities, including: (i) conducting examinations of newly registered municipal advisors; (ii) reviewing private placements, including offerings involving Regulation D or the EB-5 Immigrant Investor Program; (iii) examination of "never-before-examined" investment advisers and investment company complexes; (iv) private fund advisers and, in particular, fees and expenses and controls and disclosures associated with side-by-side management of performance-based and purely asset-based fee accounts; and (v) examining transfer agents with a particular focus on transfer agents providing paying agent services for their issuers.

CONCLUSION

OCIE's 2016 examination priorities cover a broad range of market participants and target a variety of their products, practices and procedures, including a continued focus on private fund sponsors. Registered investment advisers, including private fund sponsors – in particular, "never-before-examined" investment advisers – should be prepared for rigorous examinations that focus on these issues.

This client update was originally issued on January 13, 2016.

SEC Regulation of Cybersecurity and Tech Risk Converges

In the last several years, cyberattacks affecting high-profile companies have received much publicity. Technology-related disruptions in the securities markets also have received significant publicity and resulted in enforcement actions. In combination, these events have put cybersecurity and technology risk at the forefront of the agenda of the U.S. Securities and Exchange Commission.

First, the SEC used its regulatory power to promulgate Regulation Systems Compliance and Integrity ("Reg SCI"), proposed in spring 2013 and adopted in fall 2014, with an implementation date of Nov. 5, 2015.[1] Reg SCI sets a series of standards for SCI entities (exchanges and large alternative trading systems, among others) with respect to their development, implementation and monitoring of SCI systems (defined to include systems relating to the execution, clearing and settlement of trades), including notification protocols and a safe harbor from liability for individuals. "Systems intrusions" (Reg SCI-speak for cybersecurity breaches) are one of the main contingencies for which SCI entities must take these steps, implement corrective actions and provide notification to the SEC and affected market participants.

Second, starting in April 2014, the SEC's Office of Compliance Inspections and Examinations (the "OCIE") issued the first of three

[1] Regulation Systems Compliance and Integrity, Securities Act Release No. 34-73639 (Nov. 19, 2014) (hereinafter, the "Reg SCI Release"); *see also* Proposed Rule: Regulations Systems Compliance and Integrity, Securities Act Release No. 34-69077 (Mar. 8, 2013).

risk alerts focused on cybersecurity.[2] This first risk alert announced examination priorities for an upcoming review of cybersecurity preparedness at broker-dealers and investment advisers. The OCIE conducted this first slate of examinations and released its findings in a second risk alert on Feb. 3, 2015.[3] Then, on Sept. 15, 2015, the OCIE issued a third risk alert identifying a new set of cybersecurity priorities applicable during its 2016 exams and giving financial services firms guidance as to the OCIE's expectations of how they should be addressing cybersecurity.[4]

The risk alerts in conjunction with Reg SCI provide insight into the SEC's current position on what constitutes adequate cybersecurity preparedness for broker-dealers and investment advisers. While clear written policies and procedures are a key component, firms are well-advised to have strong internal structures to ensure effective implementation and ongoing assessment of both the policies and the systems themselves. And as a recent enforcement action indicates, simply reporting a cyberbreach to the SEC and taking mitigating

---

2 *See* OCIE Cybersecurity Initiative (Apr. 15, 2014), *available at* https://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf. The SEC also held a roundtable on cybersecurity in March 2014. In her opening remarks at this roundtable, SEC Chair Mary Jo White asserted that cybersecurity threats are global and present a great risk to our economy. Chair White went so far as to say that such risks are "first on the Division of Intelligence's list of global threats, even surpassing terrorism." See a transcript of the Cybersecurity Roundtable, *available at* https://www.sec.gov/spotlight/cybersecurity-roundtable/cybersecurity-roundtable-transcript.txt.

3 OCIE Cybersecurity Examination Sweep Summary (Feb. 3, 2015), *available at* https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf.

4 OCIE's 2015 Cybersecurity Examination Initiative (Sept. 15, 2015), *available at* https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf.

steps to protect clients after the fact may not be sufficient in the current climate, especially where customer privacy might be implicated.

Below we summarize in more detail Reg SCI and the risk alerts and then briefly discuss key provisions of Reg SCI — not discussed in the risk alerts — that may provide insight into the SEC's cutting-edge thinking about cybersecurity. We also look for insights from the SEC's recent settlement with a registered investment adviser regarding a cybersecurity breach. With the popular focus on all things "cyber," the financial services industry would do well to pay close attention.

REG SCI

The SEC adopted Reg SCI in response to a number of significant technology issues experienced by various market participants.[5] Although no cybersecurity incident appears to have been among the catalysts, the SEC included protocols around "systems intrusions" as part of the requirements under Reg SCI in recognition of the importance that systems security can play in technological disruptions. As such, all of Reg SCI's requirements, as summarized below, apply to all aspects of a firm's technology, including cybersecurity.

Simply put, Reg SCI attempts to regulate the development, implementation and ongoing monitoring of technology infrastructure at so-called "SCI entities." This designation includes most self-regulatory organizations (*e.g.*, exchanges, FINRA and MSRB), alternative trading systems with volume above certain minimums and a few other significant market utilities such as

[5] *See* Reg. SCI Release at 7.

clearing agencies. It is important to note that Reg SCI as of now does not apply broadly to the broker-dealers and investment advisers examined by the OCIE. SEC Chair Mary Jo White and other SEC officials have stated that the SEC is looking into whether to extend the regulation to "other market participants" including broker-dealers.[6]

The rule defines SCI systems as "all computer, network, electronic, technical, automated, or similar systems of, or operated by or on behalf of, an SCI entity that, with respect to securities, directly support trading, clearance and settlement, order routing, market data, market regulation, or market surveillance."[7] Reg SCI outlines two categories of SCI systems: critical SCI systems and indirect SCI systems. Critical SCI systems are defined as any systems that "directly support functionality relating to: (1) Clearance and settlement systems of clearing agencies; (2) Openings, reopenings and closings on the primary listing markets; (3) Trading halts; (4) Initial public offerings; (5) The provision of consolidated market data; or (6) Exclusively-listed securities ..."[8] This category also applies to those systems that "provide functionality to the securities markets for which the availability of alternatives is significantly limited or nonexistent and without which there would be a material

---

6 *See* Chair White's "Statement at Open Meeting on Regulation SCI" (Nov. 19, 2014) (stating that Commissioner White directed the SEC staff to prepare recommendations "as to whether an SCI-like framework should be developed for other key market participants, such as broker-dealers and transfer agents"); *see also* Commissioner Stein's Remarks before the Securities Traders Association's 82nd Annual Market Structure Conference (Sept. 30, 2015), *available at* http://www.sec.gov/news/speech/stein-market-structure.html.

7 Reg SCI Release at 712.

8 *Id.* at 709.

impact on fair and orderly markets."[9] Indirect SCI systems are defined broadly as "any systems of, or operated by or on behalf of, an SCI entity that, if breached, would be reasonably likely to pose a security threat to SCI systems."[10]

Reg SCI mandates that SCI entities institute policies and procedures designed to ensure that SCI systems "have levels of capacity, integrity, resiliency, availability, and security, adequate to maintain the SCI entity's operation capability and promote the maintenance of fair and orderly markets."[11] These policies should include periodic testing and updating of cybersecurity procedures and the establishment of business continuity and disaster recovery plans in the event of breaches. The business continuity plan must be "reasonably designed to achieve next business day resumption of trading and two-hour resumption of critical SCI systems following a wide-scale disruption."[12]

SCI entities also need to put into place procedures to identify responsible SCI personnel.[13] The regulation provides a safe harbor from liability for any such SCI personnel who have "reasonably discharged" their duties or who were "without reasonable cause to believe" the system was not in compliance with the firm's policies,

---

9 *Id.*

10 *Id.* at 710.

11 *Id.* at 712.

12 *Id.* at 712, 713.

13 *Id.* at 715.

the system's intended functionality or applicable Reg SCI requirements. No safe harbor applies to SCI entities.[14]

Reg SCI also regulates how SCI entities must respond to an "SCI event," which is defined in three categories. The first is a "systems disruption," which includes any event "that disrupts, or significantly degrades, the normal operation of an SCI system."[15] The second, "systems compliance issues," is defined as "an event … that has caused any SCI system … to operate in a manner that does not comply with the [Securities Exchange] Act [of 1934] and the rules and regulations thereunder or the entity's rules or governing documents, as applicable."[16] The third category is a "systems intrusion," defined as "any unauthorized entry into the SCI systems or indirect SCI systems of an SCI entity" and thus includes, among other things, cybersecurity breaches, introduction of malware and any breach related to employee misconduct or negligence.[17]

Upon the occurrence of an SCI event, the SCI entity must take "appropriate corrective action to mitigate potential harm to investors and market integrity" and "devote adequate resources to remedy the SCI event as soon as reasonably practicable."[18] Appropriate action includes providing written notification to the SEC within 24 hours of the event as well as periodic status updates on the investigation into, and resolution of, the event. The SCI entity must also send the SEC a report discussing who the event

---

14 *Id.* at 209.

15 *Id.* At 712.

16 *Id.*

17 *Id.* at 140, 141, 712.

18 *Id.* at 715.

affected and to what extent. Relatedly, Rule 1002(c) of Reg SCI requires an SCI entity to disseminate information regarding major events to all of its members or participants, and about certain lesser SCI events to affected members or participants.[19] The reporting standards are much less burdensome for events defined as "de minimus."[20]

THE FEBRUARY RISK ALERT

The February risk alert reported on the findings of examinations the OCIE staff conducted of 57 registered broker-dealers and 49 registered investment advisers, intended to "evaluate how these entities handled the legal, compliance and regulatory issues related to cybersecurity."[21] The OCIE did not provide substantive guidance on best practices or expectations for broker-dealers and investment advisers, but simply reported on what the examinations found. As part of the examinations, the OCIE staff obtained information from each firm on how it (i) identified cybersecurity risks, (ii) adopted and

---

19 Reg SCI Release at 667,

20 *Id.* at 717, 718; Reg SCI also imposes affirmative reporting requirements and other obligations on SCI entities regardless of whether there has been a breach. The entities must (1) submit a quarterly report detailing any material changes to SCI systems as well as to the security of indirect systems (*Id.* at 730); (2) conduct yearly "SCI reviews," which should assess "internal control design and effectiveness of its SCI systems and indirect SCI systems to include logical and physical security controls, development processes, and information technology governance" (*Id.* at 711); (3) send to the SEC and the entity's board of directors a report including the SCI review and senior management must respond within 60 days of receiving the report (*Id.* at 720); and (4) to "make, keep, and preserve" certain documents demonstrating compliance, and to provide them to the SEC upon request (*Id.* at 721). Moreover, a penetration test of "network, firewalls and production systems" must happen every three years. See *Id.* at 720.

21 February Risk Alert at 1.

implemented policies, procedures and oversight for cybersecurity and (iii) protected their networks and information in the event of a breach or intrusion. The February risk alert gives a statistical breakdown of the practices uncovered by the examinations.

Much of the emphasis of the February risk alert concentrates on written procedures and processes for cybersecurity risk assessment and mitigation. The report found that the majority of examined broker-dealers (93 percent) and investment advisers (83 percent) had in place written information security policies and procedures. Most of the firms periodically performed audits in order to assess compliance with these policies and procedures. Most entities reported performing firmwide inventorying, cataloguing or mapping of their technology systems and resources. Many firms reported that they were using external standards (like those of the National Institute of Standards and Technology, the International Organization for Standardization, and the Federal Financial Institutions Examination Council) as models for their cybersecurity processes and procedures. Most of the examined firms' information security policies and procedures did not address how they would determine whether they were responsible for client losses in cyber-related incidents. In almost every category, a higher percentage of the examined broker-dealers had implemented the types of policies and practices scrutinized by the OCIE staff than was the case for the examined investment advisers.

While a majority of the broker-dealers (nearly 75 percent) had incorporated cybersecurity measures into contracts with their vendors and business partners, the investment advisers were found

to be lagging in this area.[22] The February risk alert noted that most of the firms subject to the examination had experienced a cyber-related incident either directly or through one or more of their vendors, and that the majority of the cyber-related incidents were related to malware and fraudulent emails. The OCIE staff reported that a quarter of the losses due to fraudulent emails resulted from employees failing to follow the firm's identity authentication procedures.[23]

SEPTEMBER RISK ALERT

On Sept. 15, 2015, the OCIE issued the September risk alert announcing that it will conduct a second round of examinations of broker-dealers and investment advisers to assess cybersecurity preparedness. The OCIE identified six areas on which this next round of examinations will focus. The September risk alert discusses each area in some detail and in doing so provides insight into the OCIE's expectations for broker-dealers and investment advisers. It also includes a sample document request list, which suggests the kinds of documentation relating to cybersecurity that the OCIE expects to see at firms.[24]

---

22 Cybersecurity preparedness in relation to third parties receives more attention in the September Risk Alert, see September Risk Alert at 2, Appendix at 4.

23 Training and implementation of written procedures are more of a focus in the September Risk Alert, see September Risk Alert at 2-3, Appendix.

24 *See* Debevoise & Plimpton LLP, Client Update: SEC Releases Updated Cybersecurity Examination Guidelines (Sept. 18, 2015), *available at* http://www.debevoise.com/~/media/files/insights/publications/2015/09/20150915a_sec_releases%20updated_cybersecurity_examination_guidelines.pdf.

The first category is "Governance and Risk Assessment." This category includes looking into whether registrants have procedures for risk assessment in place that are appropriate for their business and whether the firm periodically evaluates them. It will also assess the level of communication to, and involvement of, senior management and directors, including information on the firm's chief information security officer and other employees responsible for cybersecurity matters. The OCIE's document requests might seek, for example, policies and procedures related to protection of client records and board minutes, and briefing materials regarding cybersecurity matters.

The second category is labeled "Access Rights and Controls." Examiners may ask how firms control access to various systems and data through management of user credentials, authentication and authorization methods. Remote access, customer logins and password protocols fall within this area. The SEC also focused on this issue in its 2010 Market Access Rule.[25]

The third category, "Data Loss Management," centers on how firms monitor the content that employees and third parties transfer to and receive from outside the firm. Employee and third-party uploads and email attachments are mentioned in this context. The OCIE seems particularly interested in the controls in place for protecting the personally identifiable information of customers, which has

[25] Risk Management Controls for Brokers or Dealers with Market Access, Securities Act Release No. 34-63241 at 12-22, 126-127 (Nov. 3, 2010), *codified at* 17 C.F.R. § 240.15c3-5; *see also* OCIE National Exam Risk Alert: Master/Sub-accounts (Sept. 29, 2011), *available at* https://www.sec.gov/about/offices/ocie/riskalert-mastersubaccounts.pdf.

implications, among others, under the SEC's Regulation S-P governing privacy of customer information.[26]

The next two areas likely stem in part from concerns raised in the February risk alert. The fourth category is "Vendor Management." According to the OCIE, some of the largest cybersecurity breaches have come from hacking of third-party vendor platforms that then provide a means of entrance to the real target's systems. The OCIE intends to review how firms choose and monitor their vendors, including requests for documents or notices that firms require from their vendors related to technology systems and cybersecurity measures at the vendor. The fifth category, "Training," looks at the adequacy of training given by firms to employees and third-party vendors who might form the first line of defense against cybersecurity risks.

The final category is "Incident Response." Examiners will evaluate whether and how the firm's business continuity plan handles mitigation and recovery from a cybersecurity breach. They may also ask for information regarding how firms have handled incidents in the past.

The September risk alert sharpens the focus on third-party vendor management and preparedness for cybersecurity incidents through written procedures and their proper implementation. Vendors have

---

[26] Rule 30 of SEC Regulation S-P, known as the "Safeguards Rule", mandates that investment advisers, broker-dealers and investment companies create and maintain reasonably designed written policies and procedures to protect the security and confidentiality of customer records and information. *See* Privacy of Consumer Financial Information (Regulation S-P), Securities Act Release No. 34-42974 (Nov. 18, 2003), *as codified at* 17 C.F.R. § 248.

been the attack vector in a remarkable number of high-profile breaches. While the first set of examinations attempted to determine whether firms had in place cybersecurity procedures and processes, this second alert seems to assume these policies will be in place and indicates that going forward the focus will be on implementation, training and access controls.

DISCUSSION

Several key themes appear in Reg SCI and the risk alerts. First, all three focus on the firm's written policies and procedures. While not a new concept for either broker-dealers or investment advisers, the adoption of policies and procedures specific to technology moves them into a new realm. Indeed, the September risk alert makes clear that the OCIE now assumes that both broker-dealers and investment advisers have created and implemented policies and procedures with respect to cybersecurity. Consequently, the OCIE will now focus on whether these procedures have been implemented at all levels of the firm and with respect to all systems, including those provided by vendors.

A second theme concerns the level of responsibility (as distinct from liability) for all types of employees, and especially senior management and the board for developing and implementing the procedures, understanding the systems and technologies, and regularly monitoring and testing to ensure compliance and appropriate functioning. It seems beyond doubt that the SEC wants an "all hands on deck" approach to these issues. The third theme revolves around vendor management and requirements to not only understand vendor systems but also to ensure that vendors do not provide entrance into the firm. The SEC recognizes with this approach that the weak link could be a vendor even where the firm itself has robust protocols.

Two requirements in Reg SCI do not seem yet to be a focus specifically of the OCIE cybersecurity initiative. First, Reg SCI includes affirmative reporting obligations, both to the SEC and to other market participants. As a result, SCI entities will need to develop policies and procedures for generating and delivering such reports, and the recipients will need to think about how to use that information and what actions to take upon receipt. SCI entities will also need to carefully consider what should be included in such reports and when dissemination of reports to other market participants is necessary.

Second, Reg SCI contemplates personal liability for individuals at SCI entities in the event of an incident. The undeniable implication of the safe harbor for individuals who reasonably discharge their duties demonstrates the SEC's preparedness to use its regulatory enforcement power to hold SCI personnel responsible for technology problems. The inclusion of the potential for individual liability reflects how seriously the SEC takes the risk-mitigation obligations it has imposed through Reg SCI. Moreover, the safe harbor from liability for those who were "without reasonable cause to believe" the system was not in compliance implies that individuals have a duty of inquiry as to whether systems might be the subject of an intrusion. Consequently, SCI entities and the individuals they employ must remain cognizant of this duty to continue to monitor systems in an effort to detect breaches.

Whether these notification and liability requirements will become standard for cybersecurity events remains to be seen. That cybersecurity liability resonates in the halls of the SEC was shown just one week after publication of the September risk alert with the settled enforcement matter against R.T. Jones Capital Equities Management, a registered investment adviser. Though the breach at

R.T. Jones was minor, did not cause significant financial losses for customers, and was identified and reported to the SEC as well as customers, these factors were not the focus of the action. Marshall S. Sprung, co-chief of the SEC Enforcement Division's Asset Management Unit, articulated the SEC's focus on preventative procedures: "As we see an increasing barrage of cyber attacks on financial firms, it is important to enforce the safeguards rule even in cases like this when there is no apparent financial harm to clients ... Firms must adopt written policies to protect their clients' private information and they need to anticipate potential cybersecurity events and have clear procedures in place rather than waiting to react once a breach occurs."[27] We also hear quite clearly the echoes of the focus on policies and procedures in both the risk alerts and Reg SCI in the findings that R.T. Jones did not include in its procedures and protocols (i) periodic risk assessments, (ii) the use of firewalls, (iii) encryption of client information, or (iv) clear guidelines for responding to a cybersecurity breach.

CONCLUSION

In a speech at a Managed Funds Association conference on Friday, Chair White noted cybersecurity as a major operational risk for private fund sponsors.[28] On that same day, the director of the SEC Division of Enforcement noted: "If firms don't have appropriate policies and procedures in place, that could be a [regulation S-P]

---

27 http://www.sec.gov/news/pressrelease/2015-202.html.

28 Chair White's "Five Years On: Regulation of Private Fund Advisers after Dodd-Frank" (Oct. 16, 2015) (noting cybersecurity as a major operational risk and saying: "Staff guidance earlier this year encouraged advisers to assess their ability to prevent, detect and respond to attacks in light of their compliance obligations under the federal securities laws, and detailed a number of measures advisers may wish to consider. Pay careful attention to the areas discussed in the guidance." (footnote omitted))

violation."[29] The twin regulatory initiatives represented by the risk alerts and Reg SCI warrant further attention at both broker-dealers and investment advisers.

This article was originally published on October 23, 2015 on Law360.com.

[29] *See* Priya Anand, MarketWatch, *A crackdown is coming on firms with lax cybersecurity* (Oct. 16, 2015), http://www.marketwatch.com/story/a-crackdown-is-coming-on-firms-with-lax-cybersecurity-2015-10-16.

Client Update:

SEC Sanctions Investment Adviser for Failing to Adopt Cybersecurity Policies and Procedures

In a recently disclosed action, the Securities and Exchange Commission ("SEC") found a registered investment adviser, R.T. Jones Capital Equities Management, Inc. (the "Adviser"), liable for failing to adopt written policies and procedures designed to protect customer records and information. This Order makes good on the promises embodied in the SEC Division of Investment Management's April 2015 IM Guidance and the SEC Office of Compliance Inspections and Examinations ("OCIE") Cybersecurity Examination Guidelines issued earlier this month that the SEC will continue to focus on firms' development of robust cybersecurity protections. This case highlights the importance of the recommendations outlined at the end of this Client Update.

BACKGROUND

The Adviser offered investment advice to participants in a retirement plan through a managed account program called Artesys. In order to confirm prospective clients' eligibility to enroll in the program, the Adviser would request their names, dates of birth, and social security numbers. The company would then check that information against a database it maintained containing the same personally identifiable information ("PII") from each of the more than 100,000 eligible participants. This database was stored, unencrypted, on a third-party-hosted web server.

In July 2013, the Adviser discovered a potential breach of that server. It did not have written cybersecurity policies or an incident response plan in place, but it promptly retained cybersecurity consultants, who were able to confirm that an intruder had gained full access and

rights to copy the information in the database. Although the consultants couldn't determine whether the client data had actually been accessed, exfiltrated, or otherwise compromised during the breach, the Adviser provided notice, and free identity theft monitoring, to all clients whose data may have been compromised. (To date, no client has reported suffering financial harm from the incident.)

THE SEC'S FINDINGS

The SEC found that these facts represented a willful violation of Rule 30(a) of Regulation S-P, 17 C.F.R. § 248.30(a), which requires broker-dealers and investment advisers to maintain written policies and procedures to safeguard customer records and information.

The SEC censured the Adviser, ordered it to cease and desist from any continuing or future violations of the Regulation, and fined it $75,000. The Order notes that the company cooperated with the government and promptly took remedial steps including appointment of an information security manager, retention of a cybersecurity firm to provide reports and advice, implementation of a written information security policy, and elimination of the data security flaws that contributed to the breach.

This case serves as a useful reminder that registered investment advisers should carefully consider how to adopt the measures to address cybersecurity risks recommended by the SEC's Division of Investment Management in guidance issued in April of this year. That guidance instructed funds and advisers to establish strategies – memorialized in written policies and procedures – for preventing, detecting, and responding to cybersecurity threats.

RECOMMENDATIONS

The Order points up the risks of disregarding the SEC's expectation that firms develop and continually refresh written policies and procedures for dealing with cybersecurity incidents. Firms should consider taking the following steps to protect themselves:

- Develop, test and regularly update a formal, written Incident Response Plan. Ideally, this IRP should be distinct from any business continuity plans.
- Adopt and follow written cybersecurity policies and procedures.
- Engage outside counsel and consultants experienced with cybersecurity issues to assist in complying with the SEC's guidance.
- Develop and implement document and data retention policies. Prune data in accordance with those policies. Hackers can't steal what you don't have.
- Mind your third-party vendors. Consider contractual provisions that mandate a certain level of cybersecurity controls, appropriate indemnifications and obligations to notify you in the event of a breach.
- Consistent with business needs, consider where encryption can be deployed to protect sensitive data.

This enforcement action continues the regulatory trend of converting technology "best practices" (*e.g.*, encrypting sensitive data) into legally mandated requirements for managing cyber risk. It also underscores that regulators tend to borrow from each other in crafting mandates and guidance about cybersecurity, with the SEC joining Massachusetts and the Federal Financial Institutions Examination Council in calling on companies to develop written information security policies. All companies – regardless of whether they are SEC filers – would do well to consider the SEC's

enforcement action in crafting their own data security programs. As the SEC and other government agencies increasingly focus on cybersecurity issues, companies must as well; the failure to do so may carry with it the consequences of an enforcement action.

This client update was originally issued on September 24, 2015.

Client Update:

SEC Releases Updated Cybersecurity Examination Guidelines

In 2014, the SEC's Office of Compliance Inspections and Examinations ("OCIE") conducted examinations of 57 registered broker-dealers and 49 registered investment advisers to assess the adequacy of their cybersecurity compliance and controls. OCIE's Examination Priorities for 2015 included continued cybersecurity examinations of broker-dealers and investment advisors, as well as examinations of transfer agents.

Following up on that priority, on September 15, 2015, OCIE issued a Risk Alert announcing that it will conduct a second round of examinations of registered broker-dealers and investment advisors to assess the registrants' cybersecurity preparedness.[1] OCIE identified six areas on which these examinations will focus:

- governance and risk assessment;
- access rights and controls;
- data loss prevention;
- vendor management;
- training; and
- incident response.

[1] The full text of the Risk Alert is available through the OCIE webpage, http://www.sec.gov/ocie, or in PDF format at http://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf.

The Risk Alert includes a sample document request that is instructive in its breadth, and continues the regulatory trend of focusing on:

(1) senior-level engagement with cybersecurity; (2) preparation by companies for cyber events, which includes having an incident response plan and testing it; and (3) management of cyber risk related to the use of third-party vendors.

Reflecting that focus, OCIE seeks copies of the policies and procedures relating to protection of customer records and information, information about how firms prevent data loss and classify data, and descriptions of how firms manage cybersecurity risks for third-party vendors. The request also seeks copies of incident response plans, patch management practices, board minutes regarding cyber-related risks and documents regarding employee training about cybersecurity.

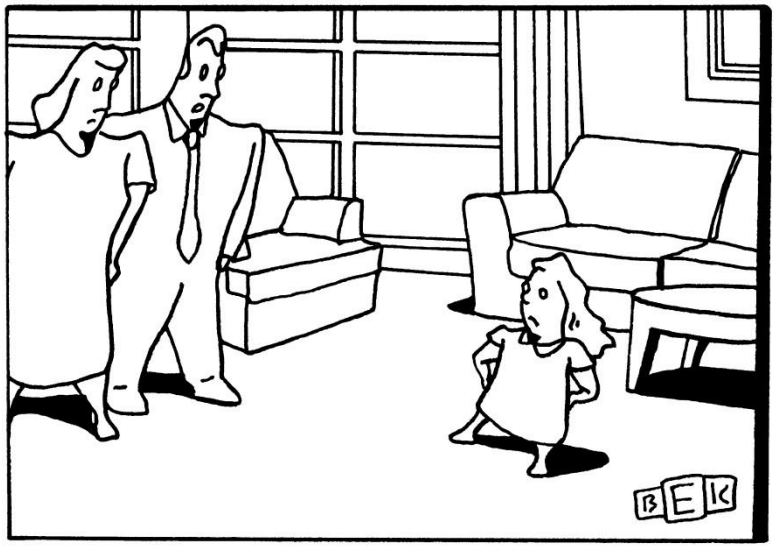
Whereas in the first round of exams, many of the requests sought to determine merely whether a firm had policies and procedures regarding certain of these topics, this updated sample document request reflects OCIE's expectation that firms will already have in place policies and procedures on these topics. The revised request also reflects an increased focus on employee access rights and access controls, an issue the FTC has recently highlighted in its guidance.

Because the updated sample request reflects what OCIE views as important elements of a firm's cybersecurity program, SEC registrants should review the sample document request closely and address any gaps that a potential examination might reveal in the firm's cybersecurity program. The adequacy of a firm's

cybersecurity protections is likely to be a continued focus for OCIE in future exams.

This client update was originally issued on September 18, 2015.

Regulatory Actions and Guidance



"Yes, we do have the authority to regulate you."

Regulators other than the SEC have continued to remain active in the cybersecurity space, with federal entities, such as the Federal Trade Commission ("FTC"), Federal Communications Commission and Consumer Financial Protection Bureau ("CFPB") each engaging in ever-more-robust regulatory efforts.

We begin with a discussion of cross-device tracking and the FTC's warning letters to several app developers relaying privacy concerns over this novel form of tracking. We then analyze the Third Circuit's ruling in the FTC action against Wyndham hotels, which

affirmed the FTC's authority to bring cybersecurity enforcement actions on the grounds that failing to maintain reasonable cybersecurity measures can constitute unfair and deceptive business practices. We also review some recent developments in mobile privacy – from federal guidance on cyber security for mobile devices, to the CFPB's foray into regulating mobile financial services. This chapter also discusses the CFPB's first-ever cybersecurity enforcement action. We close with an analysis of recent revisions to annual privacy notice requirements under the Gramm-Leach-Bliley Act.

Do the Apps Have Ears?–Cross-Device Tracking

How would you feel if you learned that your smartphone was listening while you watched television – and that it showed you an ad for a LeBron James jersey because it overheard you watching the NBA Finals? Or if the phone overheard your family watching cartoons, then showed you an ad for the latest kids' movie? If these scenarios make you wonder where the law should draw the boundaries of privacy, you are not alone: The Federal Trade Commission (the "FTC") sent warning letters to a dozen app developers about just such technology.

Welcome to the world of "cross-device tracking," in which not only your smartphone and television, but many other devices you use in your daily life may also connect to each other, share information about you and customize the services that they provide to you as a result. Cross-device tracking is rapidly expanding. Players across the privacy space will be closely watching to see how the law keeps pace.

THE TECHNOLOGY

Our smartphone example relates to mobile applications on phones, so a quick vocabulary lesson is in order. In the parlance of the mobile space, an "app developer" is the company whose brand is on the app from a consumer's perspective. For example, let's imagine that Big Grocery Company hires a third-party code-writing firm, Acme Apps Inc., to create a Big Grocery shopping app. Acme does all the technical work to create the app, but the app is then issued to the public under Big Grocery's name. Big Grocery, not Acme, is the app developer.

The FTC sent warning letters to app developers whose apps included code from an Indian company called Silverpush. The Silverpush code used an ultrasonic pitch signal – inaudible to humans, but detectable by an app – called a "unique audio beacon," or "UAB."[1]

When an app with the Silverpush code detected a UAB embedded in a TV commercial, a web browser advertisement or a radio spot, the app had the capacity to determine that the user's mobile device was close to the source of the UAB. The app also could send information back to the app developer, including the device's International Mobile Station Equipment Identity, or IMEI, a unique identifying number; the GPS location of the device; or even the user's email address.[2] Ads could then be customized to reflect where the user had been, or what the user (or, to be more precise, the user's phone) had apparently viewed or heard.

The apps in question were available on Google Play, one of the three major U.S. app stores or "platforms." The FTC noted that the UAB technology was not actually activated in any of the apps that it reviewed. Silverpush quickly responded that it had "exited from all UAB [] business and shifted to a newer product line," and that it would "appreciate if Silverpush is not associated with UAB based business going forward."[3]

---

1 Iain Thomson, "How TV ads silently ping commands to phones: Sneaky Silverpush code reverse-engineered," *The Register* (Nov. 20, 2015), http://www.theregister.co.uk/2015/11/20/Silverpush_soundwave_ad_tracker/.

2 *Id.*

3 *See* Karl Bode, "Silverpush Stops Using Sneaky, Inaudible TV Audio Tracking Beacons After FTC Warning," *TechDirt* (Apr. 13, 2016), https://www.techdirt.com/articles/20160318/09445033954/Silverpush-

So yes, the apps had ears – though they weren't actually listening, or at least not yet. But the story does not end there, because Silverpush's code is just one example of the growing universe of technologies designed to track users across their array of devices. Smartphones, tablets, desktops, "smart" televisions, wearable health devices or any other Internet-enabled devices, such as thermostats, household appliances and even cars are among the devices that currently communicate with each other about your behavior, or may do so in the future. Not only are Facebook, Google and Oracle among the major companies heavily involved in cross-device tracking, but smaller companies' cross-device "data streams" have been the target of recent investments and mergers.[4]

This developing technology obviously creates a potential boon for marketers. Tracking of user behavior historically has been accomplished mainly through cookies. These are small digital files that sit in your web browser and create a record of where you go and what you do when using that browser.

Whereas cookies are usually only good at tracking information from a particular web browser, cross-device tracking allows advertisers to monitor a plethora of information across multiple devices owned by the same person or household.[5] Cross-device tracking can capture, among other things, which content or ads are viewed on each device,

---

stops-using-sneaky-inaudible-tv-audio-tracking-beacons-after-ftc-warning.shtml.

4 *See* Allison Schiff, "2016 Edition: A Marketer's Guide To Cross-Device Identity," *Ad Exchanger* (Feb. 29, 2016), http://adexchanger.com/data-exchanges/2016-edition-marketers-guide-cross-device-identity/.

5 *See* Federal Trade Commission, *Cross-Device Tracking: An FTC Workshop*, https://www.ftc.gov/news-events/events-calendar/2015/11/cross-device-tracking.

and whether the person then searches for or buys the product on another device. That is critical information, given that 90% of consumers now conduct their online research and shopping using multiple devices.[6]

Companies can also use this information to further tailor advertisements.[7] For example, a mobile phone fitness app could target a car promotion to a user wearing a "smart" watch just as she jogs by the car dealership.

Cross-device tracking works by creating "device maps" to link devices likely owned by the same user. There are two primary methods for creating device maps:

- "***Deterministic***": Assume that a user has a paid subscription to her local newspaper's website, and logs in on her desktop computer to read the news. She then logs in on her iPad to complete a crossword. The newspaper's advertisers can determine that this user likely owns both devices.[8]
- "***Probabilistic***": If two devices cannot be matched via login information or email addresses, companies can use statistical models to predict whether those devices are likely owned by the

---

6 *See* Oracle Cross-Device Learning Center, "Cross-Device Advertising," https://www.crosswise.com/cross-device-learning-center/cross-device-advertising/.

7 *See generally* AdTaxi, "The advantages of tracking consumers across devices," http://www.adtaxinetworks.com/the-advantages-of-tracking-consumers-across-devices/.

8 *See* Todd Wasserman, "Why cross-device tracking is the latest obsession for marketers," *Campaign U.S.* (Aug. 27, 2015), *available at* http://www.campaignlive.com/article/why-cross-device-tracking-latest-obsession-marketers/13617429.

same user. For example, if the IP address or GPS location of two devices is generally the same each evening, then it is *probable* that those devices belong to the same individual or household.

Proponents of cross-device tracking cite improved user experience and more tailored ads (think: booking tickets to Italy and instantly receiving ads with recommendations for Rome AirBnb listings). Accurate device maps even offer the potential for enhanced fraud protection.[9]

Privacy advocates are not so sanguine. The Center for Democracy and Technology (the "CDT") has commented that, while a person's "activity on each device generates different data streams about her preferences and behavior that are [usually] siloed in these devices and services that mediate them," cross-device tracking has allowed advertisers to "combine these streams by linking them to the same individual, enhancing the granularity of what they know about that person."[10] The CDT contends that probabilistic tracking, in particular, is "a practice that is invisible to the user and extremely difficult for the user to control."[11]

Well before the Silverpush letters, the FTC identified cross-device tracking as a subject of interest at an agency workshop. As FTC

---

9 *See* Federal Trade Commission, Segment 1 Transcript of FTC Workshop on Cross-Device Tracking (Nov. 16, 2015) (hereinafter "FTC Segment 1 Transcript"), https://www.ftc.gov/system/files/documents/videos/cross-device-tracking-part-1/ftc_cross-device_tracking_workshop_-_transcript_segment_1.pdf.

10 Center for Democracy and Technology, *Comments for November 2015 Workshop on Cross-Device Tracking* (Oct. 16, 2015), https://cdt.org/files/2015/10/10.16.15-CDT-Cross-Device-Comments.pdf.

11 *Id.*

Chairwoman Edith Ramirez commented, "some of the techniques that companies employ to collect data passively across devices mean that online tracking is even more hidden from the typical consumer."[12]

THE FTC WARNING LETTERS

By way of background, a warning letter might be described as one of the less sharp arrows in the FTC's enforcement quiver. The FTC typically issues warning letters to multiple companies engaged in a commercial practice the FTC staff finds troubling. The FTC also typically publishes a no-names version of the warning letter on its website. The net effect is to alert the market to the FTC staff's concerns, without the Commission actually commencing an enforcement proceeding.

The FTC's warning letters went to the developers of 12 apps that the FTC suspected incorporated Silverpush's UABs.[13] The FTC's message was clear: If any of these apps "enabled third parties to monitor television-viewing habits of U.S. consumers"[14] and its

---

12 *See* FTC Segment 1 Transcript, *supra* note 9.

13 *See* Federal Trade Commission, "Press Release: FTC Issues Warning Letters to App Developers Using 'Silverpush' Code" (Mar. 17, 2016), https://www.ftc.gov/news-events/press-releases/2016/03/ftc-issues-warning-letters-app-developers-using-Silverpush-code; Lesley Fair, "Letters to app developers caution against info surprises," *FTC Business Blog* (hereinafter "FTC Silverpush Blog Post"), https://www.ftc.gov/news-events/blogs/business-blog/2016/03/letters-app-developers-caution-against-info-surprises (Mar. 17, 2016).

14 *See* Federal Trade Commission, Sample Warning Letter to App Developers Using "Silverpush" Software (Mar. 17, 2016) (hereinafter, "FTC Sample Silverpush Warning Letter"), https://www.ftc.gov/system/files/attachments/press-releases/ftc-issues-warning-letters-app-developers-using-Silverpush-code/160317sampleSilverpushltr.pdf.

"statements or user interface stated or implied otherwise," the developers could be liable for violating Section 5 of the Federal Trade Commission Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce."[15]

THE LEGAL LANDSCAPE

In the data privacy context, Section 5's deception prong is generally interpreted to require companies to act consistently with their privacy policies and other consumer-facing statements about how personal data will be collected and used.[16] Section 5 also means, in the FTC's view, that companies have a particularly robust obligation to disclose data collection and usage practices that would be unexpected or potentially unwelcome to consumers.[17]

In its Silverpush warning letters, the FTC focused on the potential for deception. The FTC stated that the UAB technology was not clearly disclosed "contextually as part of the setup flow, in a dedicated standalone privacy policy, or anywhere else."[18] The FTC noted that the consumers were not warned that the Silverpush code was "configured to access the device's microphone to collect audio information even when the application is not in use."[19] Additionally,

---

15 15 U.S.C. § 45(a)(1); *see also* Federal Trade Commission, "A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority" (July 2008) (hereinafter "FTC Investigative and Enforcement Authority"), https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.

16 *See* Federal Trade Commission, FTC Policy Statement on Deception (Oct. 14, 1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.

17 *See* FTC Investigative and Enforcement Authority, *supra* note 15.

18 *See* FTC Sample Silverpush Warning Letter, *supra* note 14.

19 *Id.*

deceptive conduct might result if the apps "require[d] permission to access the mobile device's microphone prior to install, despite no evident functionality in the application that would require such access."[20]

The FTC's letters mentioned the FTC's Section 5 "unfairness" authority, but did not dwell on it. The relative silence, as compared to the deception discussion, is potentially significant.

The unfairness prong of Section 5 is addressed to substantive business practices that are likely to cause substantial injury to consumers that cannot be reasonably avoided, and which are not outweighed by countervailing benefits.[21] Because unfairness deals with substantive practices, disclosure cannot cure it.

It remains to be seen whether the FTC will contend – someday, on other facts – that cross-device tracking crosses the unfairness boundary. For now, the Commission appears to see cross-device tracking as a practice that is lawful when appropriately disclosed. The FTC also appears poised to delve deeper into the question of what empirically constitutes an effective disclosure, as highlighted by its upcoming September 2016 workshop, "Putting Effective Disclosures to the Test."[22]

---

20 *Id.*

21 *See* 15 U.S.C. § 45(n).

22 *See* Federal Trade Commission, *FTC to Host September Workshop on Testing Effectiveness of Consumer Disclosures* (May 24, 2016), https://www.ftc.gov/news-events/press-releases/2016/05/ftc-host-september-workshop-testing-effectiveness-consumer.

THE LESSONS

How is an app developer to stay on the right side of the still-hazy legal line? Some helpful hints are embedded in the FTC's Silverpush letters:

- ***You issue it, you own it***. It is notable that the FTC addressed its warning letters to the app developers – that is, the consumer-facing companies whose apps incorporated the Silverpush code. If the FTC also wrote to any of the other players in the app ecosystem – *e.g.*, Silverpush, any vendors that created the apps for the app developers or the app platforms that distributed the apps – that was not publicized. The message seems clear: If the app carries your company's brand, then the FTC will hold your company legally responsible for its technical contents. "The vendor did it" (with Colonel Mustard, in the library . . .) will not be a defense.
- ***Know what your app does*** . . . Given the FTC's stance, it would be wise for companies to fully understand the functionality of their own apps. That may sound simple, but can be complicated in practice: The vendors (*e.g.*, "Acme Apps," in our example above) may know better than the brand company exactly what functionality is baked into the app. The brand company can seek to protect itself by obtaining representations and warranties from the code-writing vendor about what they've included in the code. Pre-release technical due diligence by the app developer on the app's privacy features is also advisable. That can be as simple as someone at the brand company opening up the app and exploring it before it is released to the marketplace.[23]

[23] In the data security context, the Consumer Financial Protection Bureau has cited a company for failing to conduct pre-release security testing. *See In re Dwolla, Inc.*, CFPB No. 2016-CFPB-007 (Mar. 2, 2016),

- ***. . . and clearly tell consumers***. Avoiding a deception charge requires telling consumers what your app does, so clear terms in an app's privacy policy are a must. The FTC will expect especially robust disclosures where information will be captured in ways, or for purposes, that the average consumer would not expect. Companies thus might consider using "just in time" pop-up disclosures – those that appear on a smartphone screen at the relevant moments throughout the user experience. (For example, an app might show a dialog box when the microphone is used to collect data other than the consumer's own voice commands.) Avoiding a deception charge also means adhering to your disclosures and updating them in light of evolving business practices.

Perhaps the simplest lesson of Silverpush is this: companies should think carefully about how consumers would react in the real world if they knew just how an app functioned. The Silverpush letters plainly reflect the FTC staff's view that ordinary consumers would feel a gut-level discomfort with UABs.[24] As one commentator has pungently noted, "if our televisions, computer, and mobile devices talked about us and coordinated their behavior in a way we could hear, we would be creeped out."[25]

Try this, then, for a rule of thumb: if the details about how your app collects and uses data across devices would seem alarming to your

---

http://files.consumerfinance.gov/f/201603_cfpb_consent-order-dwolla-inc.pdf.

24 *See* FTC Silverpush Blog Post, *supra* note 13.

25 Bruce Schneier, "The Internet of Things That Can Talk About You Behind Your Back," *Schneier on Security* (Jan. 13, 2016), https://www.schneier.com/blog/archives/2016/01/the_internet_of.html.

grandmother, then it may be time to think about options. A company might double down on disclosures, increasing their prominence and clarity so as to avoid a deception charge. A company also might conduct a consumer survey to determine how average consumers think; put another way, maybe your grandmother actually isn't a good proxy for the intended audience. Or the company might even reconsider using the tracking technology.

It is early days still in the legal world for cross-device tracking. Companies should keep an eye out for further guidance from the FTC and other authorities regarding the emerging and increasing use of these novel technologies.

Reproduced with permission from Privacy & Security Law Report, 15 PLVR 1421, (July 11, 2016), The Bureau of National Affairs, Inc.

Client Update:

Court Upholds FTC Cyber Authority; Recent FTC Guidance on Insider Breaches Looms Larger

THE THIRD CIRCUIT UPHOLDS THE FTC'S CYBERSECURITY ENFORCEMENT AUTHORITY

Section 5 of the FTC Act states broadly that "unfair" and "deceptive" business practices are illegal. For about ten years, the FTC has brought a host of enforcement cases in the cybersecurity area. In a nutshell, the Commission asserts in these cases that data security practices are "unfair" if they are substantively inadequate, and "deceptive" if they run contrary to a company's own public statements. But the FTC has not issued formal cybersecurity guidance through a rulemaking process.

Wyndham Hotels got hit with an FTC enforcement action after it experienced multiple data breaches in 2008 and 2009. Wyndham hit back with a legal challenge, asserting that the FTC lacked the authority to sue it for deficient cybersecurity practices.

Ruling on August 24, a three-judge panel of the Third Circuit unanimously sustained the FTC's authority to bring an enforcement action against Wyndham, affirming a ruling below out of the District of New Jersey. The panel held that inadequate cybersecurity measures and privacy policies could constitute "unfair practices" under the FTC Act. The panel stated that Wyndham could be liable for unfair practices violations even where the conduct of the hackers was criminal, so long as the cybersecurity intrusions were foreseeable – and, the panel noted, an unforeseeability argument "would be particularly implausible as to the second and third attacks."

In rejecting Wyndham's argument that the company had insufficient notice of the particular cybersecurity practices favored by the FTC, the Court pointed to materials like the FTC's complaints in earlier cybersecurity cases and to a cybersecurity guidebook issued by the FTC in 2007.

MORGAN STANLEY'S INSIDER BREACH

In light of the Third Circuit's emphasis on past FTC guidance, the FTC's recent announcement that it would *not* take enforcement action against Morgan Stanley is all the more timely and important.

In January 2015, Morgan Stanley announced that a financial advisor in its wealth management division had stolen client data for some 350,000 accounts, representing nearly 10% of the bank's wealth management clients. Almost none of the compromised accounts were the thief's particular clients. Following the breach, account names, numbers and other customer information relating to approximately 900 accounts appeared on public websites.

The FTC opened an investigation of Morgan Stanley's data security practices prior to the breach. But on August 10, 2015, the FTC's Bureau of Consumer Protection, Division of Privacy and Identity Protection, published a closing letter – that is, it publicly ended its investigation without taking enforcement action.

A closing letter is the FTC enforcement staff's way of saying to industry, "[w]e're taking a pass in this specific case – but the rest of you are now on notice of our reasons, so next time we may not be so lenient."

WHAT MORGAN STANLEY DID RIGHT

In its closing letter, the FTC staff highlighted the key aspects of Morgan Stanley's data security program that contributed to the decision not to pursue enforcement action:

- **Morgan Stanley "implemented a policy allowing employees to access only the personal data for which they had a business need."** The thief was acting contrary to company policy by reaching for the data of clients he did not personally serve; this was viewed as important by FTC. To state the obvious, an employee who cannot get access to sensitive stuff in the first place cannot steal that stuff.
- **Morgan Stanley implemented technological tools to monitor "the size and frequency of data transfers by employees."** Such monitoring, done right, can help flag anomalous data flows that are indicative of a breach.
- **The company deployed tools to block employee access to high-risk applications and websites.** Many financial institutions and other organizations now restrict access to applications and sites that are seen as risky – in particular, webmail, social media and other potential exfiltration points for stolen data.
- **Morgan Stanley prohibited employees from using USB drives or other removable media.** Although Morgan Stanley's policy ultimately was not properly configured in this instance, the FTC may view the existence of such a policy as required going forward.
- **Morgan Stanley responded swiftly once it had notice of the breach.** The company reviewed and, where necessary, remediated its network security protections and policies. The company also identified and terminated the employee; promptly alerted law enforcement; worked to remove the compromised data from the Internet; notified affected clients; and offered identity protection

services to the clients. Given the FTC's praise for Morgan Stanley on these issues, companies are well advised to review, refresh and test their written incident response plans to see how they compare.

Insider or "Snowden" risk is widely viewed as one of the most daunting challenges in all of data security. After all, it is impossible to run a business without giving your employees liberal access to data and system resources. The closing letter is a reminder to companies in all industries that, however daunting the challenge may be, the FTC sees robust efforts to tackle Snowden risk as a legal requirement.

The closing letter specifically warns that "risks, technologies, and circumstances change over time," and that "companies must adjust security practices accordingly." For today, though, companies are well advised to carefully assess their own Snowden-risk mitigation strategies in light of the Morgan Stanley closing letter. A good approach is to ask with particularity not just "are we doing X?", but "how well are we doing X and are there gaps we need to close?". This approach should help position a company to receive the FTC's next closing letter, rather than its next lawsuit.

This client update was originally issued on August 25, 2015.

Client Update:

New Federal Guidance on Cybersecurity for Mobile Devices

On November 4, the National Institute of Standards and Technology ("NIST"), an arm of the Department of Commerce, issued a new draft practice guide entitled "Mobile Device Security: Cloud & Hybrid Builds." This represents NIST's growing focus on mobile security – a subject NIST has touched on before, but did not specifically address in its much-ballyhooed 2014 "Framework for Improving Critical Infrastructure Cybersecurity," better known as simply the Framework. NIST has opened its Mobile Device Security practice guide to public comment until January 8, 2016.

The Mobile Device Security guidance was issued by NIST's National Cybersecurity Center of Excellence ("NCCoE"), a partnership among NIST and companies in the technology industry. The guidance emerged from NIST's collaboration with Microsoft, Intel, Lookout and Symantec.

NIST has established itself as a standard-bearer in cybersecurity benchmarking. The 2014 NIST Framework, although designed on its face for use by "critical infrastructure" organizations, has been widely adopted across the private sector. NIST's leadership impact has been felt not only from a technical and business perspective but from a legal one as well.

For example, Commissioner Julie Brill of the U.S. Federal Trade Commission – an agency that brings many cases against companies over their allegedly inadequate cybersecurity – has lauded the 2014 NIST Framework as "fully consistent with the FTC's enforcement framework." The U.S. Securities and Exchange Commission has encouraged funds and investment advisers to "consult this

Framework when considering a strategy to mitigate exposure to cyber attacks." The U.S. Department of Justice likewise has cited the NIST Framework as a key source for cybersecurity guidance.

Leading accounting firms and insurance companies, too, have taken note of the NIST Framework. At least one major insurer has started to incorporate the Framework into its underwriting for cyber coverage.

Companies looking to stay ahead of the regulatory and market curve on cybersecurity might therefore do well to consider NIST's new draft recommendations. The reasons for concern about mobile security in the corporate context are clear. Bring Your Own Device ("BYOD") programs, for example, are widely recognized as a threat vector; in the BYOD environment, companies lack control over what employees may download to their personally owned devices when not connected to the company network. One popular alternative to BYOD is the so-called Corporate Owned and Personally Enabled device, or COPE – where the company provides a smartphone or tablet to an employee, who is free to customize it and to use it for both business and personal purposes. COPE is generally considered less risky than BYOD, but still presents the risks of commingling the employee's personal uses and data with the company's.

NIST's new draft guidance maps out in some detail how companies might mitigate the security risks caused by employee use of mobile devices. This makes it quite different from the NIST Framework, which speaks more in terms of broad categories of issues and tends to leave implementation details to a company's discretion. The mobile security draft includes a 144-page "How-To" guide that covers topics such as:

- configuring mobile devices, *e.g.*, by implementing an entirely cloud-based or hybrid solution;
- separating the company's data and employee personal data stored on or accessed from the mobile device, *e.g.*, by leveraging Operating System capabilities to prevent user-level applications from exchanging data with each other, thereby "sandboxing" sensitive applications; and
- de-provisioning mobile devices that no longer require access to company data (lost devices, stolen devices, devices of employees leaving the company), *e.g.*, by configuring devices to automatically wipe all stored data after a certain number of failed authentication attempts.

The new draft guidance goes so far as to cite specific, commercially available products (Microsoft Office 365, Lookout's Android application for detecting malicious software, and Symantec's Secure Site Pro service for generating digital authentication certificates) that might be used to help configure a mobile device management system. NIST specifically notes it is not endorsing the products named in the practice guide.

We have compared notes on the new NIST guidance with our colleagues at Stroz Friedberg, a leading cybersecurity firm. Edward Stroz, the firm's Executive Chairman, observes:

"The impact of mobile devices in enterprise security is often underestimated, in part because legacy best practices for enterprise security lag developments in mobile technology. In most enterprise environments today, the number of mobile devices often equals or surpasses the number of desktops and laptops. The NIST document recognizes that the widespread adoption of mobile devices to

communicate, search, and access sensitive information poses a potential threat to information security measures because traditional boundaries established between trusted and untrusted systems are vanishing.

As mobile devices are used to store sensitive enterprise data and pose a higher risk of loss or theft, needed controls must be prioritized to prevent or mitigate potential information loss. In this context, we expect that the NIST Cybersecurity Practice Guide on Mobile Device Security will be helpful to companies by providing scientific, prioritized guidance following a risk-based methodology, in much the same way as the NIST Cybersecurity Framework has."

What actions might organizations want to consider taking right now in light of the new draft guidance from NIST?

- Given the impact of the existing NIST Framework on both technical and legal standards, it is not too soon for legal departments to consult with their colleagues in IT, IT security, risk and other key stakeholders and begin assessing how the organization's mobile security practices stack up against the new draft guidance. Nor is it too soon to begin planning and implementing any remedial steps that might be appropriate in light of the guidance.
- Organizations that wish to be heard on the substance of the draft guidance have the option of submitting comments to NIST. The comment period runs until January 8, 2016, a relatively tight timeline given the holiday season.

This client update was originally issued on November 9, 2015.

Client Update:

The CFPB Eyes Mobile Financial Services

Last month, the Consumer Financial Protection Bureau (the "CFPB" or "Bureau") released a report regarding the use of mobile financial services ("MFS") by underserved populations (the "Mobile Report" or "Report").[1] The Mobile Report compiles public responses to its 2014 Request for Information ("RFI")[2] on MFS, defined by the CFPB in this Report as financial services and products accessed through mobile devices such as phones or tablets.

In the Mobile Report, the CFPB explores how underserved populations including low-income, unbanked, underbanked and/or economically vulnerable consumers are engaging with MFS. In particular, the Mobile Report focuses on four areas: (i) the types of MFS available to underserved populations, and the scope of consumer interaction with MFS; (ii) opportunities for MFS to expand and reach these consumers; (iii) challenges and risks associated with MFS, particularly in relation to these consumers; and (iv) recommendations for further study and discussion. Although the Mobile Report states that it is "not intended to identify areas in which the Bureau may or will take regulatory, supervisory, or

---

1 CONSUMER FINANCIAL PROTECTION BUREAU, MOBILE FINANCIAL SERVICES (Nov. 2015), *available at* http://files.consumerfinance.gov/f/201511_cfpb_mobile-financial-services.pdf.

2 CONSUMER FINANCIAL PROTECTION BUREAU, REQUEST FOR INFORMATION REGARDING THE USE OF MOBILE FINANCIAL SERVICES BY CONSUMERS AND ITS POTENTIAL FOR IMPROVING THE FINANCIAL LIVES OF ECONOMICALLY VULNERABLE CUSTOMERS (Jun. 2014), *available at* http://files.consumerfinance.gov/f/201406_cfpb_request-for-information_mobile.pdf.

enforcement action,"[3] FinTech companies and other providers of consumer financial products or services would do well to pay attention to the Mobile Report findings as they will likely inform the Bureau's strategies in these areas.[4]

We describe the key findings of the Mobile Report below.

I. MFS AND UNDERSERVED CONSUMERS

In the RFI, the CFPB defined MFS as covering mobile banking and mobile financial management services. It specifically did not address mobile point of sale payments, except with respect to mobile payment products that are targeted specifically for low-income and underserved consumers. A number of commenters sought clarification about the governing standard for determining what constitutes MFS to avoid confusion and ensure that the discussions around public policy take place in the context of commonly understood terms and scope.

In the Mobile Report, the CFPB appears to adopt the suggestion by commenters that MFS should not be considered a discrete set of products and services, but rather a channel through which consumers can access financial services and products through many devices. Nonetheless, the Mobile Report highlights certain MFS areas of particular interest to the CFPB, including mobile banking, personal financial management tools, text messaging, mobile

---

[3] Mobile Report, *supra* note 1, at 4, *available at* http://files.consumerfinance.gov/f/201511_cfpb_mobile-financial-services.pdf.

[4] *See, e.g.*, Prepaid Accounts Under the Electronic Fund Transfer Act (Regulation E) and the Truth in Lending Act (Regulation Z), 79 Fed. Reg. 77101, 77121 (Dec. 23, 2014) (noting that among its payments-related actions, the Bureau was in the process of reviewing comments to the RFI).

applications, prepaid products, mobile payments, mobile carrier billing and mobile P2P.

Although noting that questions remain as to the scope of MFS, the Mobile Report focuses on the challenges facing potentially disruptive technology. In particular, commenters focused on digital financial literacy as a major barrier to the potential benefits in MFS. The Mobile Report stresses that while improving access to these products may be an important step, it is not an end in itself. As one commenter stressed, "mobile banking does not make people smarter or supply individual financial acumen. Improving financial literacy remains a priority even in a mobile world."[5]

The Mobile Report notes that though more consumers have access to MFS on data-driven devices like smartphones, the increase in smartphone ownership has not directly transformed into a similar explosion in MFS usage.[6] In particular, consumers with incomes below $15,000 per year remain chronically under-banked, despite the rise in smartphone ownership. Even among those underserved consumers who do manage their finances within the traditional banking system, the Mobile Report observes that large proportions prefer to bring their money to a branch office.[7] The Mobile Report opines that this may be a result of the character of the deposits (much higher percent of cash versus check or card transactions), to the immediacy that a physical bank provides. Notwithstanding these facts, the Mobile Report notes that underserved consumers had higher rates of mobile banking and mobile bill pay than among

---

5 Mobile Report, *supra* note 1, at 52.

6 *Id*. at 15-16.

7 *Id*. at 72-73.

all consumers suggesting that MFS may be an important means to integrate the underserved into the mainstream financial marketplace.[8]

II. OPPORTUNITIES FOR MFS TO EXPAND

The Mobile Report highlights a few important areas for MFS-aligned firms to consider when designing products and services: (i) the speed of mobile check deposit (and Mobile Remote Deposit Capture ("MRDC") technology); (ii) the safety of consumer data in every respect (discussed further below); (iii) determining if, and by how much, MFS could lower consumer and financial institution costs; and (iv) expanding financial services education generally and digital literacy more specifically to ensure that consumers know how to safely navigate the technology necessary to conduct their financial transactions and achieve their financial goals.

Of particular note is the discussion surrounding the opportunity to design products that focus on the specific issues facing underserved consumers. The Mobile Report suggests that innovative products focusing on reducing the delay in access to funds could better provide unbanked low-income consumers with financial products to fit their needs because it may have the potential to save time and reduce costs for those households that use nonbank check cashing services. Specifically, underserved consumers tend to both need access to their funds faster than a normal check deposit may allow, and also tend to hold a larger portion of their finances in cash.[9] The Mobile Report suggests that if MFS could be expanded to address the delay in access to cash it could fill a real need for underserved

---

8 *Id*. at 19-20.

9 *Id*. at 22.

customers, a more secure (and less expensive) mechanism to access cash.[10]

Given that the Bureau shares joint rulemaking authority with the Board of Governors of the Federal Reserve (the "Federal Reserve") with respect to the consumer related provisions of the Expedited Funds Availability Act/Regulation CC, it will be interesting to see if the CFPB proposes any new disclosures on MRDC funds availability and/or encourages the Federal Reserve to make clear the manner in which Regulation CC funds availability rules apply to such deposits.

The Mobile Report, however, acknowledges that expediting funds availability could pose new challenges to financial institutions in combatting fraud.[11] As discussed further below, fraud, which exists at every end of the chain of distribution, is the central reason that checks take time to process and related funds take long to clear. Although the Report does not offer any solutions on this front, it suggests that the CFPB is thinking carefully of how to balance this business reality with consumers' desire for fast access to funds.

III. RISK AREAS FOR CONSUMERS

The Report outlines a number of risk areas for consumers engaging in MFS channels including: (i) data and transaction security, including the risk of data breaches and identity theft; (ii) privacy concerns, including the unauthorized sharing or tracking of consumer information for marketing and other purposes; and (iii) the risks of discrimination based on financial information.

---

10 *Id.*

11 *Id.* at 22-23.

The cybersecurity risk is ever-present in MFS channels, and the Mobile Report describes the risks generated by lost or stolen mobile devices, differences in operating systems, and denial of service attacks which may be particularly problematic for underserved consumers given their limited resources, which make them less able to absorb financial losses or interruptions that may result from security-related problems. The Report notes that real and perceived privacy and security concerns remain a significant barrier to adoption of MFS, and suggests that MFS products must develop cutting-edge security features to protect consumers from identity theft or other kinds of financial fraud in order to address these concerns.[12]

The Mobile Report observes that consumers are increasingly concerned about the lack of privacy of their data when using MFS products and services. The Report cites commentary from the Federal Trade Commission which notes the high number of companies involved in the mobile payments system and the large volume of data collected.[13] Moreover, the Mobile Report features several suggestions by commenters that current disclosures may be insufficient for consumers to make informed decisions and that the current disclosure requirements should be adapted to mobile technology in ways that enhance understanding about the product such as its costs and fees.[14]

The Mobile Report also highlights the CFPB's concern about possible discrimination by financial institutions in their use of these

---

12 *Id*. at 59.

13 *Id*. at 60.

14 *Id*.

online financial profiles created using big data. In particular, the Report focuses on comments expressing concern that the explosion of consumer financial data, both from MFS-type services and social media, could lead financial institutions to make credit decisions that would result in a sort of "virtual redlining," in violation of the Equal Credit Opportunity Act ("ECOA").[15] For example, financial institutions could use financial profiles created through aggregation of data created, in part, by MFS services to make decisions on how and when to extend credit. Whether deliberate or inadvertent, financial institutions could wind up restricting their lending to certain groups or classes of people in violation of ECOA. Finally, the Mobile Report outlines the CFPB's concern about potential violations of the Fair Credit Reporting Act which mandates that consumers be notified when firms report certain information to credit ratings agencies, and, in turn, when firms use certain information to make decisions about a consumer's credit profile.[16]

We would expect the CFPB to focus on these risk areas as it evaluates whether supervision of this market is appropriate through a larger participant rule[17] or whether additional regulation or guidance is needed to clarify providers' responsibilities.

IV. SUGGESTED AREAS FOR FURTHER RESEARCH

The Mobile Report outlines a number of areas for further study. In particular, commenters suggested a need for additional research on

---

15 *Id.* at 61.

16 *Id.*

17 The Dodd-Frank Wall Street Reform and Consumer Protection Act authorizes the CFPB to supervise nonbanks that are larger participants of markets for consumer financial products or services as the CFPB defines by rule. 12 U.S.C. 5514(a)(1)(B), (a)(2).

the role of big data analytics in financial services and for increased dialogue about cybersecurity practices across all mobile platforms.[18] Additionally, commenters called for further research into the best mechanisms for teaching financial literacy and for extending financial products to consumers who may not have access to the traditional financial system.[19] One commenter suggested that the CFPB develop a consumer security toolkit which would help consumers protect information on their mobile device from all the different risks associated with the mobile platform.[20] One tech industry commenter also encouraged the CFPB to require financial firms to develop a "tokenization" policy, which would further encrypt communications between the financial institution and the MFS product.[21]

Additional commenters suggested that the CFPB do more research on specific populations and how they use mobile and access financial services, including information around language and culture, to help identify ways to remove barriers to access. In addition to the groups identified within the Mobile Report, commenters suggested more information should be sought on rural consumers, people with disabilities, consumers with limited English proficiency, recent immigrants, underserved or opportunity youth (*i.e.*, youth between the ages of 16 and 24 who are neither enrolled in school nor participating in the labor market) and those residing in traditionally underserved communities.

---

18 *Id*. at 77.

19 *Id*. at 78-79.

20 *Id*. at 79.

21 *Id*. at 80.

V. CONCLUSION

Ultimately, the Mobile Report stresses that MFS, while intriguing in its myriad possibilities and applications, will not function as a gateway for underserved consumers without an emphasis on financial products that fit their unique circumstances. The Report concludes that in order for MFS to help consumers access financial services and products and achieve costs savings, "there needs to be broader digital financial literacy, more confidence that appropriate consumer protections are in place and greater comfort with the technology, including around security and other potential risks associated with this data driven ecosystem."[22] We would expect that the CFPB will take a closer look at these areas as it seeks to "make markets for consumer financial products and services work for Americans."[23]

This client update was originally issued on December 17, 2015.

---

22 *Id.* at 82.

23 CFPB, Everyone Has a Story, *available at* http://www.consumerfinance.gov/everyone-has-a-story/.

Client Update:

CFPB's First-Ever Data Security Case

On March 2, the Consumer Financial Protection Bureau ("CFPB" or "Bureau") took action against Dwolla, an online payment platform, for deceiving its customers about its data security practices and its online payment system. This is the first data security enforcement action by the Bureau, through the use of its statutory authority to punish unfair, deceptive and abusive acts or practices ("UDAAP"). CFPB has now joined a long list of regulators, ranging from (for example) the SEC to the FTC to the FCC to the attorneys general of the 50 states, that are looking to make high-impact cyber cases.

Dwolla collects personal information including the customer's name, address, date of birth, telephone number, Social Security number, and bank account and routing numbers. Dwolla told customers it had set "a new precedent for the payments industry," providing "safe" and "secure" transactions and protecting personal information through data security practices that would "exceed" or "surpass" industry standards. Dwolla asserted, in particular, that it encrypted sensitive personal information and that its mobile applications were safe and secure.

CFPB found that Dwolla's data security practices, in fact, fell far short of its claims, and therefore took enforcement action even though Dwolla had not suffered a data breach. Specifically, the CFPB found, among other issues, that Dwolla failed to employ reasonable and appropriate measures to protect customer data; encrypted only some of the personal information in its systems; and released mobile applications before testing whether they were secure.

The Bureau thus ordered Dwolla to stop deceiving its customers about the security of its data, enact and train employees on new data security measures and policies, train employees how to protect customer data, fix any security weaknesses in its web and mobile applications and securely store and transmit customer data going forward. The CFPB also ordered Dwolla to pay a $100,000 civil monetary penalty.

WHAT SHOULD COMPANIES DO RIGHT NOW?

To reduce UDAAP risk, modesty may be the new order of the day in how a company should describe its cybersecurity practices to customers. Companies might also consider regularly cross-checking the statements about cybersecurity in their privacy policies, terms of service, and other communications to consumers against the level of security actually being provided. In conducting such a cross-check, companies should keep in mind the theory used in the Dwolla case: a company can be in violation of the law merely for having a mismatch between your public statements and your private practices – even without a data breach or consumer harm. The Dwolla case also shows that regulators are increasingly confident in concluding that specific technical gaps, such as incompleteness of encryption, can drive a finding of legal violation.

This client update was originally issued on March 8, 2016.

Client Update:

Changes to Annual Privacy Notice Requirements

As part of the Fixing America's Surface Transportation Act ("FAST Act"), President Obama recently signed into law an amendment to the Gramm-Leach-Bliley Act ("GLBA") that would eliminate the annual privacy policy notice ("Annual Notice") requirement for certain financial institutions. These changes, which follow a similar move by the Consumer Financial Protection Bureau ("CFPB"), will ease an existing regulatory burden and allow many financial institutions to avoid providing customers with Annual Notices.

CHANGES TO THE ANNUAL NOTICE REQUIREMENT

Title V of the GLBA requires financial institutions – including depository institutions, registered investment companies, U.S. private funds, registered investment advisers and securities broker-dealers – to protect the nonpublic personal information ("NPI") that they receive and to disclose their policies for collecting, using and disclosing NPI. Under the GLBA, financial institutions generally must provide their customers with: (1) an initial privacy notice with appropriate disclosures, at the time of establishing a customer relationship and (2) Annual Notices thereafter.[1]

The FAST Act eliminates the Annual Notice requirement, provided two conditions are met:

- **First**, the financial institution must only share NPI within the GLBA-listed exceptions that do not trigger the opt-out right. If the information sharing practice falls under one of these exceptions, the financial institution need not provide consumers

[1] *See* GLBA, Section 503; 12 U.S.C. § 6803.

the right to "opt-out" of such information sharing. Among the GLBA-listed information sharing arrangement exceptions are the following:

- With non-affiliated third parties for the purposes of performing services for or functions on behalf of the financial institution;
- As necessary to effect, administer or enforce a transaction requested or authorized by the consumer;
- To protect the confidentiality or security of the financial institution's records against fraud and for institutional risk control purposes;
- To provide information to insurance rate advisory organizations, ratings agencies, the institution's attorneys, accountants and auditors or others determining compliance with industry standards;
- To consumer reporting agencies; and
- To comply with applicable federal, state or local laws or rules.

- **Second**, the financial institution must not have changed its policies or procedures with respect to the disclosure of NPI since the last privacy notice was provided to its consumers.

Thus, a financial institution would only be required to provide an Annual Notice if it changes its privacy policies or discloses NPI to non-affiliated third parties in a manner that triggers an opt-out right.

COMPARISON TO THE CFPB'S MODIFICATION OF REGULATION P

The FAST Act amendments come on the heels of the CFPB's rule ("Final Rule") amending Regulation P, which applies principally to depository institutions, to permit "alternative delivery methods" for Annual Notices (such as notifying consumers in their account statement of the availability of the institution's privacy policy on its

website).[2] The Final Rule required covered institutions seeking to take advantage of the alternative delivery methods to meet certain pre-conditions, including both of the requirements set forth in the FAST Act.

The changes in Regulation P are likely to be supplanted by the FAST Act exception, given that the FAST Act allows firms to avoid Annual Notices altogether and given that the FAST Act's changes apply to all financial institutions and not exclusively those subject to the CFPB's Regulation P.

This client update was originally issued on January 6, 2016.

[2] *See* Amendment to the Annual Privacy Notice Requirement under the Gramm-Leach-Bliley Act (Regulation P), 79 Fed. Reg. 64057 (Oct. 28, 2014).

Industry Watch: Financial Services

"What's to prevent some total stranger anywhere in the world from paying my bills?"

Our earlier sections covered what the SEC and other federal regulators have been up to this year in the cybersecurity space. In this section, we discuss how two tools – the FFIEC Cybersecurity Assessment Tool and the NIST Cybersecurity Framework – which were developed to help companies begin to come to grips with and implement a robust cybersecurity program – are increasingly being relied upon as regulatory benchmarks in the financial services sector.

We also provide practical highlights from the recent Cybersecurity Interpretive Notice issued by the National Futures Association, and how members can start preparing for cybersecurity to be a part of examinations in the future. Finally, we take a look at cybersecurity steps that FinTech firms can take as part of their compliance programs.

A Year under the Cyber Assessment Tool and the NIST Framework

In June of 2015, the Federal Financial Institutions Examination Council (the "FFIEC") released its Cyber Assessment Tool (the "Tool"), to help banking institutions of all sizes assess and identify risks and weaknesses in their cybersecurity preparedness programs. Though originally intended to be a purely voluntary aid for financial institutions to improve cybersecurity processes, the Tool now seems to be approaching the status of a standard in the cyber preparedness examinations conducted at banks by such regulatory bodies as the Office of the Comptroller of the Currency (the "OCC"). The cybersecurity Framework promulgated by the National Institute of Standards and Technology Cybersecurity Framework (the "NIST Framework") also is approaching the status of a *de facto* regulatory compliance standard.

THE TOOL IN PRACTICE

The Tool consists of an inherent risk profile and a cybersecurity maturity assessment. The risk profile assessment includes a set of guided questions intended to evaluate five key areas of cybersecurity risk: (i) technologies and connection types; (ii) delivery channels; (iii) online and mobile products and technology services; (iv) organizational characteristics; and (v) external threats. This is intended to assess how great a risk the various areas pose to a particular bank.

The questions in the risk profile section focus on (i) cyber-risk management and oversight; (ii) threat intelligence and collaboration; (iii) cybersecurity controls; (iv) external dependency management; and (v) cyber incident management and resilience. Each domain has

five levels of maturity: (i) baseline; (ii) evolving; (iii) intermediate; (iv) advanced; and (v) innovative. While management assesses an institution's maturity level in each domain, the assessment is not designed to identify an overall cybersecurity maturity level. A bank's appropriate cybersecurity maturity level depends on its inherent risk profile.

The binary "yes" or "no" nature of the questions in the risk assessment part of the Tool have been criticized for failing to provide firms an accurate picture of their cybersecurity risk. For example, financial institutions are asked to respond "yes" or "no" to statements like, "The risk management program incorporates cyber risk identification, measurement, mitigation, monitoring and reporting." While this question is straightforward, it does not allow firms to express the degree to which they use identification, measurement, mitigation, etc. to reduce cyber risk. Moreover, banks run the risk of responding in the affirmative too readily or, alternatively, failing to give their own efforts enough credit.

THE NIST FRAMEWORK

Some have expressed a desire for closer alignment between the Tool and the NIST Framework. While an appendix to the FFIEC's Tool includes a table that maps the Tool to the NIST Framework, the two are not perfectly aligned. For example, while the Tool and the NIST Framework cover many of the same substantive concerns, the Tool is more comprehensive and is more specific to financial institutions.

On June 9, 2016, NIST published a summary of observations based both on feedback received from commenters as well as from its recent Cybersecurity Framework Workshop 2016. The results showed general agreement among users that the NIST Framework has proven to be a useful tool for coordinating cybersecurity at a

high level. A March 2016 survey showed that 44% of surveyed companies have adopted the NIST Framework and 70% of these firms did so because they considered the framework to be a set of best practices.[1]

The NIST Framework, while designed to be a voluntary aid, is also morphing into a regulatory standard. For example, the NIST Framework was linked to the metrics of the 2016 Federal Information Security Modernization Act ("FISMA"). Specifically, FISMA uses the NIST Framework as its standard for evaluating management and reduction of cybersecurity risk and is organized around the NIST Framework's five major principles. Additionally, the Illinois Attorney General issued Information Security and Security Breach Notification Guidance that calls for companies to encrypt certain data using NIST-certified cryptographic modules.

The Tool has also appeared to move from a voluntary aid towards the status of a *de facto* regulation, since the OCC is now using the FFIEC's Cyber Assessment Tool in their examinations of national banks and federal savings associations. In the wake of the OCC's examinations, banking regulators of states such as Texas, Massachusetts and Maine have encouraged the use of the FFIEC's Cyber Assessment Tool.

CONCLUSION

As securities breaches and attempted hacks continue to make the news, it is no surprise that regulators will revise and examine existing cybersecurity guidance and assessment tools in an effort to

[1] Dimensional Research, Trends in Security Framework Adoption: A Survey of IT and Security Professionals, 2 (Mar. 2016), http://static.tenable.com/marketing/tenable-csf-report.pdf.

most effectively mitigate cyber risk. Consequently, it is likely that both the Tool and the NIST Framework will continue to evolve – perhaps towards greater alignment with each other, perhaps not. Financial institutions should keep an eye on the changes to both, and consider how their own cybersecurity programs might be adjusted accordingly. At the same time, regulators are likely to propose new cybersecurity guidance and assessment tools. For example, on June 29, 2016, the Bank of International Settlements introduced its own non-binding guidance on cybersecurity for companies in the financial sector. As regulators introduce new guidance and assessment tools, companies will need to continually evaluate how the ever increasing amount of guidance and assessment tools map on to their business.

Client Update:

NFA Cybersecurity Notice Takes Effect March 1

The Cybersecurity Interpretive Notice, issued by the National Futures Association ("NFA") and approved by the Commodity Futures Trading Commission, becomes effective March 1, 2016. The Notice requires all Members of NFA (futures commission merchants, swap dealers, major swap participants, introducing brokers, forex dealer members, commodity pool operators and commodity trading advisors) to have in place practices that are reasonably designed to diligently supervise the risks of unauthorized access to or attack of their information technology systems, and to respond appropriately should unauthorized access or attack occur.

The March 1 deadline is not expected to trigger any immediate charges of noncompliance. Rather, it is expected that NFA will work with Members to help them move into a position of compliance. Members should expect compliance to be a topic in future examinations.

KEY INFORMATION SYSTEMS SECURITY PROGRAM CONSIDERATIONS

Some highlights:

- The Notice focuses on five key areas for a Member's information systems security program ("ISSP"): a written program, security and risk analysis, deployment of protective measures against the identified threats and vulnerabilities, response and recovery from events that threaten the security of the electronic systems and employee training.
- The Notice specifically singles out risks related to third-party service providers and provides guidance on risk management

practices, such as performing due diligence on a third party's security practices and adding measures in contracts that address how confidential data will be protected and implementing procedures to respond to data breach notices from a service provider.

- Members will have a leg up if they have already been benchmarking their cybersecurity efforts against the standards of certain leading cybersecurity organizations. The Notice points favorably to a number of such standards as appropriate guideposts, including the Cybersecurity Framework issued by the National Institute for Standards and Technology and the Critical Security Controls for Effective Cyber Defense issued by the SANS Institute.
- Significant C-Suite and board-level engagement is required. The written ISSP should be approved in writing by the Member's Chief Executive Officer, Chief Technology Officer (or other executive level official) and senior management should periodically update the Member's board of directors (or similar governing body or committee) with information about the ISSP that is sufficient for monitoring the Member's information security efforts.
- The Notice calls for eternal vigilance: Members are called on to perform a regular review of their ISSP at least annually, using either in-house staff with appropriate knowledge or engaging an independent third-party information security specialist.
- NFA recognizes that one size does not fit all. The Notice does not establish specific technology requirements, instead proposing guidelines that leave the exact form of an ISSP up to each Member in light of its particular circumstances.
- Where a Member is part of a larger corporate structure that shares common information systems and has adopted and implemented privacy and security safeguards organization-wide,

the Member firm can satisfy the supervisory responsibilities described in the Notice through a consolidated entity ISSP.

NFA MEMBERS' "FAQ"

I Can't Possibly Meet All These Obligations by March 1. What to Do?

Keep calm and carry on. NFA has made clear that it will take a cooperative approach and not a punitive one. At a recent workshop, NFA said it will not simply start saying "violation, violation, violation" after March 1; rather, it will work with Members to help move them towards compliance. NFA recognizes that some Members will need to devote a significant amount of time and resources to meet their obligations and that any programs that are adopted will be refined over time.

The key for now is to get as far as you can by March 1, and to have a plan and timetable for the work that remains. All signs are that NFA realizes that good cybersecurity solutions tend to take time, and tend to be effective only if implemented in an orderly manner.

Where Do I Start?

We suggest that Members that are part of larger institutional groups with ISSPs, or that otherwise have existing ISSPs in place or in development, start by reviewing any such ISSP for consistency with the Notice. Members can then make plans to identify and close any delta between their existing ISSPs and the requirements of the Notice. Firms that are starting closer to scratch are encouraged to look to the NIST Framework and to NIST's list of implementation resources.

Will I Be Hearing from NFA?

Likely, yes. NFA intends to develop an incremental, risk-based examination approach regarding the Notice's requirements. NFA has not specified that cybersecurity will necessarily be a topic in your next examination, but it is prudent to assume that it will be.

Am I at Risk of Enforcement Action if My Cybersecurity Isn't up to Snuff?

History says eventually, yes. NFA has explicitly attempted to model the Notice on the cybersecurity efforts of other bodies, like the SEC and FINRA, that have begun to bring enforcement actions. The gist of these cases is that although a regulated firm is the victim of outside hackers, it can still be deemed legally responsible for not keeping its guard up. It seems likely, though not imminent, that NFA and the CFTC may in time take a similar approach.

This client update was originally issued on February 19, 2016.

Client Update:

Compliance Issues FinTech Firms (and FinTech Investors) Should Be Focused on in 2016

Financial technology ("FinTech") firms come in all shapes and sizes, and face a wide variety of issues in the course of their operations.[1] Commentators have begun to talk about 2016 as the year of FinTech, but the quantum leaps that many of the firms seek to create have been evolving for many years as the use of technology has grown and spread within financial services. We thought it would be useful to highlight the key compliance issues that FinTech firms should be focused on in 2016, whether they plan to revolutionize the delivery of a financial service, or simply provide better technology solutions to existing industry players. FinTech investors also can use this list to ask questions of the companies they have or will invest in as a way to gauge whether management's creativity extends to the concerns of key regulators.

ANTI-MONEY LAUNDERING

Financial services regulators focus intensely on anti-money laundering ("AML") compliance, which will remain a high-risk area for firms throughout the industry given the current political climate. A survey of the landscape yields three themes. First, the scope of the AML regime continues to expand, with new classes of market participants becoming subject to AML rules now that requirements for registered investment advisors have been proposed and are expected to come into force in the next twelve to eighteen months.[2]

---

1 FinTech firms generally use software or other technology to offer products and services in or relating to financial services.

2 *See* Anti-Money Laundering Program and Suspicious Activity Report Filing Requirements for Registered Investment Advisers, 80 Fed. Reg. 52680 (Sept. 1, 2015).

Also, New York State's Department of Financial Services has proposed AML-related rules that, if adopted, will impact money transmitter, check cashing and banking firms operating in the State.[3]

Second, AML compliance is being broadly interpreted to cover all manner of alleged misconduct. For example, the Financial Industry Regulatory Authority ("FINRA") often views inadequate monitoring protocols to be a violation of AML requirements.

Third, regulators also seek to hold individuals liable for AML failures, bringing a further and more personal dimension to compliance.[4]

It is therefore critical that FinTech firms and investors understand whether and to what extent their businesses are subject to AML laws and regulations. Those firms that provide technology to other market participants should not be surprised if their clients ask about features or capabilities that can assist with such compliance together with representations and warranties around such functionality.[5]

---

[3] N.Y. Dept. Fin. Serv., Proposed Superintendent's Regulations Part 504: Banking Division Transaction Monitoring and Filtering Program Requirements and Certifications (Dec. 1, 2015), *available at* http://www.dfs.ny.gov/legal/regulations/proposed/rp504t.pdf.

[4] *See, e.g.*, FINRA, 2016 Regulation and Exam Priorities Letter (Jan. 5, 2016), *available at* http://www.finra.org/industry/2016-regulatory-and-examination-priorities-letter; *see also*, the SEC's Office of Compliance Inspections and Examinations, Examination Priorities for 2016 (Jan. 11, 2016), *available at* www.sec.gov/about/offices/ocie/national-examination-program-priorities-2016.pdf.

[5] The AML rule proposal regarding investment advisers is discussed in: Debevoise & Plimpton LLP, *FinCen Proposes Anti-Money Laundering Rules for Investment Advisers* (Aug. 31, 2015), *available at*

CYBERSECURITY

Cyber and data security issues continue to present compliance challenges for all firms, with media reports of high-profile cyber events now a regular occurrence.[6] FinTech companies are no exception to this trend. In fact, the intersection between cyber/data security and the FinTech business model means that FinTech firms will likely find themselves increasingly in the cybersecurity "crosshairs" in 2016. In addition to regulators, customers will care deeply about these issues. FinTech companies also should look at their vendors to determine whether they raise any concerns.

FinTech companies and investors should understand the legal, regulatory and functional risks in the cybersecurity realm and consider appropriate responses. Above and beyond the obvious necessity of good systems design and testing, advanced preparation in the form of thoughtful escalation procedures and vendor management should become second nature. Regulators often focus on written policies and procedures, so firms should develop, implement and maintain a playbook to prevent, assess and remediate cybersecurity breaches, including possible external reporting.[7]

---

http://www.debevoise.com/~/media/files/insights/publications/2015/08/20150831_fincen_proposes_anti_money_laundering_rules_for_investment_advisers.pdf. The rule proposal by NYDFS is discussed in: Debevoise & Plimpton LLP, *NYDFS Proposes New Anti-Money Laundering Requirements, Liability for Compliance Officers* (Dec. 7, 2015), *available at* http://www.debevoise.com/~/media/files/insights/publications/2015/12/20151207_nydfs_proposes_new_anti_money.pdf.

6 Kara Scanell & Gina Chon, *Cyber Security: Attack of the health hackers*, FINANCIAL TIMES (Dec. 21, 2015), *available at* http://www.ft.com/intl/cms/s/2/f3cbda3e-a027-11e5-8613-08e211ea5317.html#axzz3vjnNV5Ei.

7 *See, e.g.*, Jeremy Feigelson, Lee Schneider & Max Shaul, *SEC Regulation of Cybersecurity Risk and Tech Risk Converges* (Oct. 23, 2015), *available at*

Finally, FinTech companies that provide any data hosting services or that will collect, store or maintain any sensitive data on their network should also consider purchasing data breach insurance. Traditional commercial general liability policies often do not cover privacy, data and network security risks.

THIRD-PARTY RELATIONSHIPS

Financial services regulators have increasingly focused on regulation and oversight of third-party outsourcing relationships, also called vendor management. For example, in October 2013, the Office of the Comptroller of the Currency (the "OCC") issued risk management guidance to national banks and federal savings associations for assessing and managing risks associated with third-party relationships.[8] Similarly, in December 2013, the Federal Reserve released supervisory guidance on understanding and managing outsourcing risks.[9] Both sets of guidelines make clear that the financial institution remains liable from a regulatory standpoint for all outsourced functions, require due diligence reviews prior to any such arrangement, and mandate that the regulators be given access to the vendor's records for purposes of discharging their supervisory obligations. FINRA has taken a similar view for broker-

---

http://www.law360.com/articles/718238/sec-regulation-of-cybersecurity-and-tech-risk-converges; Debevoise & Plimpton LLP, *The Cybersecurity Information Sharing Act* (Jan. 6, 2016), *available at* http://www.debevoise.com/insights/publications/2016/01/the-cybersecurity-information-sharing-act.

8 OCC, Risk Management Guidance (Oct. 30, 2013), *available at* http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html.

9 Fed. Res. Sys., SR 13-19: Guidance on Managing Outsourcing Risk (Dec. 5, 2013), *available at* http://www.federalreserve.gov/bankinforeg/srletters/sr1319.htm.

dealers.[10] Moreover, the CFPB has also indicated that it will focus on oversight of third-party vendors.[11] Thus, FinTech firms that act as service providers to financial institutions, or that are otherwise working with financial institutions, should be cognizant of the increased regulatory focus on third-party vendor management and should be prepared to have financial institutions (i) conduct due diligence; (ii) negotiate contractual provisions concerning breach notification, compliance with privacy regulations, audit rights, and indemnification; and (iii) limit access to specified parts of a financial institution's network.

CONSUMER AND INVESTOR PROTECTION REGULATIONS

Laws and regulations governing the provision of financial services and products to consumers/retail investors are part of the FinTech competitive landscape. Depending on the nature of the particular product or service, companies may need to understand:

- An array of laws and regulations enforced by the Consumer Financial Protection Bureau ("CFPB"), including the Truth in Lending Act, Truth in Savings Act, and the prohibition on unfair, deceptive and abusive practices ("UDAAP"). The CFPB, a new federal government agency created in the wake of the financial crisis, is tasked with protecting consumers in the financial sector. It has very broad jurisdiction (including over banks, credit card

---

10 *See also* FINRA, Regulatory Notice 05-48: Members' Responsibility When Outsourcing Activities to Third-Party Service Providers (Jul. 2005), *available at* https://www.finra.org/sites/default/files/NoticeDocument/p014735.pdf.

11 *See* CFPB, Bulletin Regarding Service Providers (Apr. 12, 2012), *available at* http://files.consumerfinance.gov/f/201204_cfpb_bulletin_service-providers.pdf.

issuers, payday lenders, check cashers, debt collectors and other financial companies assisting consumers with cash or loans).[12]

- Securities laws and regulations that apply to FinTech companies operating in the retail securities space such as the Investment Advisers Act of 1940 (the "Advisers Act"), which may require companies offering investment advisory services to register as investment advisors with the Securities and Exchange Commission ("SEC"). This includes advisors to certain types of investment funds, such as those utilizing hedge or private equity strategies. Companies offering brokerage services might have to register with the SEC and FINRA as a broker-dealer.
- Aspects of securities laws that govern securities offerings, whether public, private, or crowdfunded, for those FinTech companies seeking to raise capital from individual investors.[13]
- Laws and regulations relating to duties of care that might apply to certain FinTech firms, particularly to those offering trust and asset management services. For example, the Employee Retirement Income Security Act of 1974 ("ERISA") imposes fiduciary duties on persons exercising discretionary authority or control with respect to the management of ERISA plan assets. In April 2015, the U.S. Department of Labor (the "DOL"), which is the agency primarily responsible for promulgating regulations under ERISA, proposed a number of ERISA-related regulatory

---

12 *See, e.g.*, Debevoise & Plimpton LLP, The CFPB Eyes Mobile Financial Services (Dec. 17, 2016), *available at* http://www.debevoise.com/insights/publications/2015/12/the-cfpb-eyes-mobile-financial-services.

13 *See, e.g.*, Debevoise & Plimpton LLP, The SEC Hands Out a Halloween Treat to Crowdfunding Supporters (Nov. 17, 2016), *available at* http://www.debevoise.com/~/media/files/insights/publications/2015/11/20151117_the_sec_hands_out_a_halloween_treat_to_crowdfunding_supporters.pdf.

changes, including an extensive overhaul of the definition of "investment advice" for purposes of determining who is a fiduciary of employee benefit plans under ERISA.[14] The DOL's revised definition would treat as a fiduciary virtually anyone making an investment-related recommendation to an ERISA plan or an IRA, or to an ERISA plan participant or an IRA beneficiary, when receiving any compensation in connection therewith.[15]

This client update was originally issued on January 12, 2016.

[14] *See* Definition of the Term "Fiduciary"; Conflict of Interest Rule – Retirement Investment Advice, 80 Fed. Reg. 21928 (Apr. 20, 2015).

[15] For a further discussion of the DOL's proposal, *see* Debevoise & Plimpton LLP, *DOL Catches Many in Expanded Fiduciary Net; Is Proposed Exemption an Escape Hatch or a Trap Door?* (Apr. 21, 2015), *available at* http://www.debevoise.com/insights/publications/2015/04/dol-catches-many-in-expanded-fiduciary-net.

Industry Watch: Private Equity

"What is the name of your first pet?"

In this section, we take a look at some issues uniquely faced by private equity firms. In our first article, we analyze the potential litigation risks around representations and warranties contained in deal documents about data security and privacy – an issue that was brought to light in a recent lawsuit. We also provide practical pointers for private equity firms looking to develop robust and functional incident response plans.

The Intersection of Cyber and Representations and Warranties in M&A Deals

Private equity funds and others that buy or sell an operating business that handles customer data should be prepared to accurately and quickly assess the robustness of that entity's cybersecurity operations, not only for business reasons but also to mitigate litigation risk. A seller risks facing indemnity claims from a disappointed buyer if the data security standards in question are lax, even when the contract representations and warranties in the sale does not explicitly reference data security protocols or policies.

A recent case demonstrates the increasing role of cybersecurity hygiene in the context of private equity deals. In *Great Hill Equity Partners IV, LP v. SIG Growth Equity Fund I, LLP*, two private equity funds contracted for the sale of an e-payment entity, Plimus.[1] Great Hill's primary interest in obtaining Plimus was Plimus's business relationships with two major players in the e-commerce space, PayPal and Paymentech; and indeed, the sellers conceded that substantially all of Plimus's value was contained in those relationships.[2] After the sale, however, the buyer discovered that the relationship with Paymentech had been terminated and that its relationship with PayPal was nearing termination. Further investigation revealed that Plimus had violated the terms of the applicable contracts with PayPal and Paymentech by failing to comply with certain industry e-payment standards, and when those

1 No. 7906-VCG, 2014 WL 6703980 (Court of Chancery Delaware, November 26, 2014).

2 Id. at *4.

vendors found out, they moved to end their relationships with Plimus.[3]

Great Hill pursued multiple bases for liability, including simple fraud, for misrepresenting the actual state of the two business relationships. Of particular interest here, however, were its causes of action for breach of contract based upon breaches of representations and warranties set forth in the transaction documents. First, the seller had represented that Plimus was in full compliance with the contracts governing its relationship with PayPal and Paymentech.[4] Second, the seller had represented that Plimus and each of its subsidiaries "is and has been in compliance with the bylaws and operating rules of any Card System(s), the Payment Card Industry Standard (including the Payment Card Industry Data Security Standard), the operating rules of the National Automated Clearing House Association, the applicable regulations of the credit card industry and its member banks regarding the collection, storage, processing, and disposal of credit card data, and any other industry or association rules applicable to [Plimus] or any of its [s]ubsidiaries in connection with their respective operations."[5]

The court denied a motion to dismiss both causes of action.

The key takeaway from *Great Hill* is that cybersecurity matters, because even when it is not of primary concern to a buyer, it may be paramount to the entity's business partners. Here, the buyer

---

3 *Id*. at *6, *10.

4 *Id*. at *16.

5 *Id*. at *17.

primarily wanted to be sure that the contracts that would facilitate business with PayPal and Paymentech were in good standing. But because those contracts required compliance with certain cybersecurity protocols, Plimus's failures provided an alternate route to relief. Great Hill could proceed on the cause of action for breaches of representations and warranties regarding compliance with the standards themselves, regardless of whether PayPal and Paymentech had acted to terminate the relationships or even identified a problem.

The converse is also true. In *Great Hill* the buyer was smart (or perhaps lucky) to have insisted upon representations and warranties concerning cybersecurity compliance. But sellers who make no representations and warranties specifically related to cybersecurity may still have to answer for a lax cybersecurity program, due to the cascading effect data-handling procedures can have over an entire business.

For example, a common representation and warranty in M&A deals is that the entity being sold is in compliance with all state and federal laws governing its line of business. Buyers want to know that they can integrate a law-compliant and profitable business into their operations on day one after closing. In recent years, cybersecurity has become such an important concern that several states have incorporated portions of otherwise voluntary industry standards into their substantive law. Nevada law requires compliance with the Payment Card Industry Data Security Standards ("PCI DSS"), a strictly voluntary set of industry standards that protect vendors from suits by credit card companies over data breaches.[6] This

[6] NEV. REV. STAT. ANN. § 603A.215 (West 2011).

voluntary industry standard has also been incorporated, at least in part, in Minnesota[7] and Massachusetts.[8] Each of these states applies the relevant statutes to any company handling payment data from its residents. For that reason, for any company running a nationwide line of business, failure to comply with PCI DSS is tantamount to failure to comply with applicable law. And as a result, a seller may have exposure for breaching a general representation and warranty of legal compliance, even absent any explicit representation as to PCI DSS. Outside of the payment card industry, it is not unreasonable to expect that as other industry standards for cybersecurity are developed, they, too, may find their way into the law.

CONCLUSION

Private equity firms, and companies carrying out acquisitions and sales generally, should not overlook the possible litigation risks stemming from representations and warranties about, or incidental to, cybersecurity. An understanding of both the applicable cybersecurity law, industry standards and the cybersecurity posture of the entity to be purchased or sold should be woven into the due diligence process.

---

7 MINN. STAT. ANN. § 325E.64 (West 2007).

8 201 CMR § 17.00 (2010).

Incident Response Plans for Private Equity Firms: Build, Test, Update

Despite the growing data security threats facing private equity firms, many firms remain underprepared to respond to evidence of a data breach. In a recent survey of almost 100 U.S. private equity firms, 66% reported they have only a "partially implemented" cybersecurity program and 10% said they have no plan in place or have not implemented the plan in any way. It appears U.S. firms are reacting slowly to the growing threat of cyber attacks, despite the very real business risks and despite guidance from the SEC that failure to mitigate these threats through policies and procedures could be deemed a violation of the U.S. Investment Advisers Act of 1940 and the U.S. Investment Company Act of 1940.[1]

In the Fall 2015 issue of *The Debevoise & Plimpton Private Equity Report*, we provided guidance on steps private equity firms can take to protect themselves and their portfolio companies from cyber threats.[2] Among those steps are identifying and locating where the firm has vulnerable assets, making careful consideration of third-party vendors granted access to firm systems, and developing written procedures to prepare for a potential incident. In this issue, we discuss how firms can develop an incident response plan ("IRP") for responding to a cyber-incident, including the structure of the

---

1 *See* "SEC Issues Cybersecurity Guidance for Registered Investment Advisers and Funds," Debevoise & Plimpton Client Update, May 7, 2015, http://www.debevoise.com/insights/publications/2015/05/sec-issues-cybersecurity-guidance.

2 *See* "Mitigating Cyber Threats to Private Equity Firms and Their Portfolio Companies," *The Debevoise & Plimpton Private Equity Report*, Fall 2015, http://privateequityreport.debevoise.com/the-private-equity-report-fall-2015-vol-15-no-2/mitigating-cyber-threats-to-private-equity-firms.

plan, how to test the plan, and the importance of regularly updating the plan based on emerging threats.

STRUCTURE OF THE IRP

No "one size fits all" plan can be used as a private equity firm's IRP, though characteristics similar to all IRPs can help guide the development of the plan. What are those characteristics? How do you develop an IRP that is appropriate for your firm?

Identify Potential Incidents. Different kinds of incidents require different responses. In beginning to develop your IRP, you should consider the types of incidents that could affect your firm and its funds in order to ensure that appropriate responses are formulated. Cybersecurity incidents that disrupt business operations may well merit very different responses than data breaches in which personal health or financial information is exposed.

Create an Incident Response Team. An IRP sets out who will respond to an incident. For many firms, it will make sense to assemble a small, standing group that constitutes a core incident response team ("IRT"). Depending on the nature of the incident, employees from various different functions might be included in the response to that incident, and can be added to the core IRT on an as-needed basis. For example, you may consider adding particular subject matter experts within the firm whose inclusion on the IRT is logical given the nature of the breach, *e.g.*, someone from investor relations to respond to a phony communication to investors; someone from accounting to help resolve a funds transfer incident; a human resources professional for an insider breach; a deal team member when material nonpublic information on a pending transaction has been exposed; or the employee responsible for a vendor relationship, should a breach occur involving such a vendor

(*e.g.*, a vendor with access to the firm's network or that stores critical firm data).

Identifying your outside service providers in advance of an incident also can help round out the appropriate membership of an IRT. We recommend that you consider adding to the IRT three outside service providers: an external cyber-forensics expert who will assist in the technical aspects of the investigation; outside counsel to advise on a range of issues from consulting with law enforcement and regulators to breach notification laws; and a PR firm that can help message the response to an incident. By establishing these relationships in advance of an incident (and getting the engagement paperwork in order), you will have the time to select advisors that are the best fit for your firm and you will almost certainly increase your ability to respond more quickly to a cybersecurity event when it occurs. An added benefit to engaging service providers early, in times of peace, may be that they will come on-site to meet your core IRT and become familiar with your systems before an event. This advanced knowledge can help pave the way for a smooth breach response.

Specify Incident Response Tasks and Responsibilities. A firm should use the IRP to define the relevant tasks to be completed by the IRT and those persons who are responsible for each of those tasks. Many of the tasks likely will center on the investigation of the cyber-incident itself and setting the schedule for updates to be delivered to senior management at the firm. Other tasks include breach notification to potentially affected individuals and to law enforcement; these are among the tasks that, if handled properly, are more likely to insure that your firm responds successfully to a breach.

TESTING THE IRP

Even the best IRP may prove less useful if not pressure-tested before an actual incident occurs. Rather than waiting for a potential incident to test whether and how efficiently the IRP works, firms should consider running "tabletop" simulations of an incident response. These simulations typically present several scenarios to members of the core IRT (and, if feasible, extended members of the team, including outside service providers) and ask the team members how they would respond to each scenario. Participants in the tests may be asked to consider not just the facts potentially signaling a breach, but how they would react upon learning of the breach at different times and places. For example, a team member might be asked how the plan should be executed if news of a potential incident breaks when IRT members are away on business or on vacation, on the eve of a deal or fund closing, or just prior to an advisory committee or annual investor meeting.

KEEPING THE IRP CURRENT

An IRP is not a static document. Any response to an incident will provide lessons on the strength of the IRP. As you begin to execute the plan, whether in response to testing or actual incidents, the plan can be modified in light of the lessons learned. Responsibility for particular tasks may need to change, new tasks may be found necessary to respond effectively to a breach and adjustments to IRT membership may be needed in light of your assessment of tests and past incidents.

A periodic schedule for updating the IRP should be put in place. Further, firms should consider empowering key personnel to drive updates to the plan outside the normal update schedule when justified by new threat information or material changes in the firm's business, assets or architecture. Firms may also reconsider the plan

and retest it after a risk assessment of cybersecurity defenses (*e.g.*, the results of an annual penetration test).

THE IMPORTANCE OF HAVING AN IRP

Increasing threats of cyber attacks and increased regulatory scrutiny make it unwise for firms to go without a carefully developed IRP. The same survey mentioned at the beginning of this article, in which most respondents saw themselves as lacking a fully implemented cybersecurity program, also revealed that more than 60% of the respondents felt they would be the target of hackers in 2016. Further, the SEC's public statements and last year's SEC enforcement action against an investment adviser for failing to maintain adequate cybersecurity policies and procedures show that the SEC expects more from private equity firms and other investment advisers than merely having an IRP in place. The questions today are: How robust is the IRP? How well has it been tailored to the firm's specific business, assets and architecture? Has the plan been tested? Is the firm organized to periodically update the plan based on emerging threats?

This article was originally published in The Debevoise & Plimpton Private Equity Report, Winter 2016.

Industry Watch: Health Care

"My life has become a tangled web of fictitious user names and fiendishly clever passwords."

Given the high value criminals place on medical records, health data continues to be a popular target for hackers. In addition, medical devices that are Internet connected present new attack surfaces. Our first article takes a look at how healthcare data has proven to be

particularly valuable to criminals and, accordingly, a continuing target for cyberattacks. We examine some recent data breaches in the healthcare sector and discuss how the FDA is working to address these issues.

Then, we take an in-depth look at how the FDA has encouraged the adoption of the NIST Framework in its post-market guidance for manufacturers of medical devices. As discussed elsewhere in this book, the NIST Framework is increasingly looked to as a *de facto* gold standard across a number of industries.

Healthcare Data:

Drawing the Attention of Cyber Criminals and Regulators Alike

The healthcare industry has increasingly become a target of cyber criminals.[1] Healthcare information is highly valuable, making it a prime target for hacking, malware and ransomware. Such attacks interrupt patient care and potentially subject players in the healthcare industry to reputational harm, significant costs and legal liability. Government authorities are accordingly stepping up scrutiny of healthcare data security, and actors in this space are upping their defenses as well.

THE VALUE OF HEALTHCARE DATA

Think "data breach" and the mind may run first to situations like Target, where millions of credit card numbers are compromised. But healthcare data encompasses significant sensitive information, including names combined with home addresses, dates of birth, Social Security numbers and medical conditions or treatments. This information is highly attractive to wrongdoers. Indeed, healthcare data trades on the "dark web," where online criminals gather to trade

---

[1] *See* Mark Taylor, *Study: 23 percent of all data breaches occur in healthcare*, MEDCITYNEWS (May 6, 2016), http://medcitynews.com/2016/05/study-data-breaches-healthcare/?rf=1; Jacqueline Belliveau, *Healthcare Data Breaches Top Reported Data Security Incident*, HEALTHIT SECURITY (Apr. 12, 2016), http://healthitsecurity.com/news/healthcare-data-breaches-top-reported-data-security-incident; Heather Landi, *Healthcare Leads Data Breaches in 2015, Human Error Still Leading Cause, Report Says*, HEALTHCARE INFORMATICS (Apr. 1, 2016), http://www.healthcare-informatics.com/news-item/healthcare-leads-data-breaches-2015-human-error-still-leading-cause-report-says; Jacqueline Belliveau, *Healthcare Data Breaches Most Common in 2015 Incidents*, HEALTHIT SECURITY (March 31, 2016), http://healthitsecurity.com/news/healthcare-data-breaches-most-common-in-2015-incidents.

their wares, at prices that are often much higher than information obtained through data breaches involving other sectors or industries.[2]

As a result, to remain a step ahead of cyber criminals, healthcare institutions should consider making intelligent investments in cybersecurity, adopting pertinent technologies, actively overseeing their vendors that handle their data and engaging in robust employee training and education. The latter is especially important because cyber criminals often seek to exploit human error.

THE YEAR-TO-DATE IN HEALTHCARE DATA BREACHES

When a healthcare data breach occurs, an organization must report it to the Office for Civil Rights at the U.S. Department of Health and Human Services ("OCR"), the federal agency responsible for enforcing and ensuring compliance with (i) the Health Insurance Portability and Accountability Act ("HIPAA"); (ii) the Health Information Technology for Economic and Clinical Health Act ("HITECH"); and (iii) the corresponding Privacy, Security and Breach Notification Rules adopted under these statutes. If the incident affects 500 or more individuals, OCR is required to post it publicly on a Breach Portal website (often referred to as the "wall of shame").

According to the OCR's website, thus far in 2016, there have been over 110 reported breaches involving approximately four million

---

[2] *See* Nsikan Akpan, *Has health care hacking become an epidemic?*, PBS NEWS HOUR (Mar. 23, 2016), http://www.pbs.org/newshour/updates/has-health-care-hacking-become-an-epidemic/.

medical records.[3] Below is a representative sample demonstrating the variety of targets and attack vectors used by cyber criminals this year:

- In February 2016, 23,341 patients of a medical clinic in Ohio received a malware-infected email that was disguised as correspondence regarding a billing invoice. Opening the email attachment would download ransomware onto a patient's computer. It was determined that the email was sent by an individual who improperly gained access to a patient database maintained by one of the clinic's third-party vendors.[4]
- In February 2016, a hospital in Los Angeles was the victim of a ransomware attack that prevented employees from sharing communications or documents electronically, including medical records. The hospital ultimately paid a ransom in Bitcoin equivalent to about $17,000 to hackers who claimed responsibility for infecting its network and encrypting the data.[5]
- In March 2016, a hacker gained access to a computer system containing records relating to a drug and alcohol abuse program in New Mexico. As a result of the security breach, the names,

---

3 *See* U.S. Department of Health and Human Services, Office for Civil Rights, *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

4 *See 23K Patients of Mayfield Clinic Sent Malware-Infected Email*, HIPAA JOURNAL (May 10, 2016), http://www.hipaajournal.com/23k-patients-mayfield-clinic-sent-malware-infected-email-3422/.

5 *See* Richard Winton, *Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating*, LA TIMES (Feb. 18, 2016), http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html.

addresses and medical treatment methods of as many as 12,000 patients were potentially exposed.[6]

- In March 2016, a hospital system in the Washington, D.C. metropolitan area experienced a ransomware attack during which employees were unable to access the hospital's network or patient records and received demands for payment in bitcoins. In response, the hospital shut down significant portions of its network for several days, forcing the cancelation of appointments and requiring the use of paper records to process patients.[7]
- In April 2016, it was announced that a third-party vendor for a pain treatment center in Arkansas was hacked, resulting in unauthorized access to medical information for over 19,000 individuals.[8]
- In May 2016, it was disclosed that a medical group in Texas experienced a major healthcare data breach. An unknown party gained unauthorized access to employee and patient information relating to over 50,000 individuals.[9]

---

6 *See* The Daily Times Staff, *San Juan County warns of data breach*, THE DAILY TIMES (May 19, 2016), http://www.daily-times.com/story/news/local/community/2016/05/19/san-juan-county-warns-data-breach/84596114/.

7 *See* Pete Williams, *MedStar Hospitals Recovering After 'Ransomware' Hack*, NBC NEWS (Mar. 31, 2016), http://www.nbcnews.com/news/us-news/medstar-hospitals-recovering-after-ransomware-hack-n548121; Jack McCarthy, *MedStar attack found to be ransomware, attackers demand bitcoin*, HEALTHCARE IT NEWS, (Apr. 4, 2016).

8 *See* Jacqueline Belliveau, *Potential Healthcare Data Breach Affects Over 19K Patients*, HEALTHIT SECURITY (April 21, 2016), http://healthitsecurity.com/news/potential-healthcare-data-breach-affects-over-19k-patients.

9 *See* Jacqueline Belliveau, *Hackers Access EHR Data in Potential Healthcare Data Breach*, HEALTHIT SECURITY (May 19, 2016),

ROBUST ENFORCEMENT ACTIONS & HIPAA AUDIT PROGRAM

Enforcement activities announced by OCR in 2016 emphasize the importance of security risk assessments, risk management plans and proactive measures designed to prevent healthcare information and data breaches. This includes a $3.9 million resolution with a research institution in March 2016, representing one of the largest settlement amounts ever for a HIPAA violation.[10]

The settlement stemmed from the theft of an unencrypted laptop from an employee's car that contained Social Security numbers and electronic protected health information ("ePHI") for approximately 13,000 individuals. OCR determined that the party failed to: (i) conduct an accurate and thorough risk analysis of ePHI in its possession, including the information on the stolen laptop; (ii) implement policies and procedures for granting workforce members access to ePHI; (iii) implement physical safeguards to restrict unauthorized access to laptops containing ePHI; (iv) implement policies and procedures governing the receipt, handling and removal of hardware and electronic media containing ePHI; and (v) implement a mechanism to encrypt ePHI, or use an alternative, equivalent measure to safeguard ePHI.[11]

---

http://healthitsecurity.com/news/hackers-access-ehr-data-in-potential-healthcare-data-breach.

[10] *See* U.S. Department of Health and Human Services, *Improper disclosure of research participants' protected health information results in $3.9 million HIPAA settlement* (Mar. 17, 2016), http://www.hhs.gov/about/news/2016/03/17/improper-disclosure-research-participants-protected-health-information-results-in-hipaa-settlement.html.

[11] *See* Resolution Agreement Between HHS and Feinstein Institute for Medical Research (Mar. 16, 2016), available at

In addition to the settlement amount, the party agreed to a three-year Corrective Action Plan, under which it must:

- Conduct a company-wide risk analysis and develop a corresponding Risk Management Plan;
- Conduct annual assessments regarding potential risks and vulnerabilities relating to ePHI;
- Develop a process to evaluate any environmental or operational changes that affect the security of ePHI;
- Review and revise policies and procedures relating to privacy and security, which must satisfy minimum content requirements regarding specific topics and issue areas;
- Provide extensive training to its workforce regarding the requirements of the Privacy, Security and Breach Notification Rules; and
- Submit an implementation report and annual reports to OCR detailing the company's compliance with the Corrective Action Plan.[12]

Through this action and the subsequent settlement agreement, OCR is sending a strong signal about measures that organizations will be expected to implement going forward to comprehensively protect healthcare data.

OCR also recently announced the launch of the second phase of its HIPAA Audit Program.[13] Under the HITECH Act, OCR is required

---

http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/feinstein/index.html.

12 *See id.*

to conduct periodic audits of covered entities and their business associates to ensure compliance with the Privacy, Security and Breach Notification Rules. The first phase of this process involved a pilot program that was performed in 2011 and 2012, with audits focusing exclusively on covered entities.

This year's second phase will include both covered entities and their business associates, and will involve approximately 200 desk and on-site audits. OCR has touted the audit program as providing an opportunity to examine mechanisms for compliance, identify best practices, discover risks and vulnerabilities and address issues before they result in breaches.

OCR's active cyber program may in part be a response to criticism by the Office of Inspector General for the U.S. Department of Health and Human Services ("OIG").[14] In two strongly worded reports issued in September 2015, OIG identified various weaknesses in OCR's enforcement activities regarding the protection of healthcare information and data.[15] OIG recommended that OCR make a

---

13 *See* U.S. Department of Health and Human Services, *OCR Launches Phase 2 of HIPAA Audit Program* (Mar. 21, 2016), http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/phase2announcement/index.html.

14 *See* Office of Inspector General for the U.S. Department of Health and Human Services, *OCR Should Strengthen Its Oversight of Covered Entities' Compliance with the HIPAA Privacy Standards* (Sept. 2015), *available at* http://oig.hhs.gov/oei/reports/oei-09-10-00510.pdf; Office of Inspector General for the U.S. Department of Health and Human Services, *OCR Should Strengthen Its Followup of Breaches of Patient Health Information Reported by Covered Entities* (Sept. 2015), *available at* http://oig.hhs.gov/oei/reports/oei-09-10-00511.pdf.

15 *See id.*

number of enhancements, including fully implementing the permanent HIPAA audit program as required by HITECH, maintaining complete documentation of all corrective actions and improving its case-tracking system.

CONCLUSION

Healthcare data, particularly in electronic form, is clearly necessary to, and increasingly relied upon for, the provision of modern medical treatments and services. It can also pose a serious risk to healthcare organizations if handled without robust security measures. Given the substantial value of healthcare information, it will likely continue to be a target for cyber criminals for the foreseeable future. As such, healthcare organizations are well-advised to continuously enhance their cybersecurity technologies, policies and procedures, including incident response plans that provide a workable playbook in the event of a cyber incident. In healthcare as in other industries, it is prudent to plan on the assumption that cyber events are a matter of "when" and not "if."

FDA's New Guidance on Cybersecurity for Medical Devices:

Important Lessons for the Entire Healthcare Industry

As the "Internet of Things" grows, the range of digital targets for malicious actors is growing with it.

Not long ago, researchers at the University of South Alabama reported the results of an exercise which confirmed that "a student with basic information technology and computer science background" could hack medical devices such as a pacemaker, defibrillator, or insulin pump, with devastating effects on the patient.

In the wake of this and similar warnings, the FDA issued "Postmarket Management of Cybersecurity in Medical Devices" (the "Postmarket Guidance").

While the guidance is technically non-binding and has not yet been finalized, it states that the failure to address cybersecurity vulnerabilities may be deemed a violation of the Food, Drug, and Cosmetic Act ("FDCA").

The guidance is directed to device manufacturers, but also emphasizes that securing devices is the responsibility of other stakeholders including health care facilities, providers and patients.

All healthcare stakeholders therefore should take heed to the FDA's recommendations, particularly its strong encouragement to join Information Sharing and Analysis Organizations ("ISAOs") and to implement the NIST Cybersecurity Framework.

GENERAL PRINCIPLES OF EFFECTIVE CYBERSECURITY MANAGEMENT

Information Sharing Analysis Organizations

The Postmarket Guidance makes clear that companies in the healthcare industry should keep abreast of developments in cybersecurity.

To accomplish that task, the FDA "strongly recommend[s]" that stakeholders participate in ISAOs. ISAOs foster collaboration among private entities and the government on cybersecurity intelligence.

By joining ISAOs, stakeholders can share and disseminate information on cybersecurity vulnerabilities and exploits. [*Editors note: Software tools designed to take advantage of a flaw in a computer system, frequently for malicious purposes such as installing malware.*]

The U.S. Government promoted the development of ISAOs in a February 2015 Executive Order, which directed the Department of Homeland Security ("DHS") to select a non-governmental organization to act as the ISAO Standards Organization that will issue a set of membership and operational best practices for all ISAOs.

The DHS has chosen as the Standards Organization a collaboration among the University of Texas at San Antonio, the Logistics Management Institute, and the retail Cyber Intelligence Sharing Center, though they have yet to issue any standard best practices for ISAOs.[1]

---

[1] ISAO Standards Organization, Products, https:// www.isao.org/products/

Nevertheless, DHS has provided some guidance as to its expectations for the best practices ISAOs will follow, based on four essential characteristics:

- ***Inclusive***: ISAOs' membership should be open to any business sector, to non-profit and for-profit organizations, and to those experienced and inexperienced in cybersecurity.
- ***Actionable***: ISAOs should provide their membership with automated, real-time information on cybersecurity threats and risks, with practical tips that members can effectively use to address these issues.
- ***Transparent***: ISAOs should provide clear information to prospective members on their operation and utility.
- ***Trusted***: ISAOs should allow members to request all their information and intelligence be treated as Protected Critical Infrastructure Information ("PCII"). PCII is protected from disclosure under the Freedom of Information Act or State Sunshine Laws, and is exempt from regulatory use and civil litigation.

Even without any guidance from the ISAO Standards Organization, a number of ISAOs have already been established, including those dedicated to specific business sectors.

Additionally, the Cybersecurity Information Sharing Act ("CISA"), which was passed last year, provides companies with further encouragement to participate in ISAOs.

CISA immunizes private companies from liability when sharing "cyber threat indicators" or "defensive measures" with DHS through

certain specific means.[2] Cyber threat indicators and defensive measures are broadly defined to include any intelligence on cybersecurity vulnerabilities and any defense designed to defeat or mitigate cyber threats. One accepted method of sharing information with DHS under CISA is through an ISAO.

The FDA has tacitly endorsed one ISAO for those in the healthcare sector: the National Health Information Sharing & Analysis Center ("NH-ISAC"). In August 2014, the FDA and NH-ISAC entered a Memorandum of Understanding ("MoU") describing terms of collaboration between their organizations for addressing cybersecurity in medical devices and the surrounding healthcare IT infrastructure.[3] The MoU serves as a broad outline of the goals of FDA and NH-ISAC collaboration, setting forth the intent of both organizations to share information on cybersecurity vulnerabilities and threats.

Membership in NH-ISAC provides healthcare stakeholders with a variety of tools to strengthen their cybersecurity defenses. Members in NH-ISAC receive access to a secure portal through which they can share information on cybersecurity threats and risks.

---

2 Note that any information shared must not contain "personal information." While not defined in the Act, personal information refers to any data defined as protected by specific sectors, *e.g.*, protected health information under the Health Insurance Portability and Accountability Act ("HIPAA").

3 Memorandum of Understanding Between the NH-ISAC and the U.S. FDA Center for Devices and Radiological Health, August 26, 2014, *available at* http://www.fda.gov/AboutFDA/PartnershipsCollaborations/MemorandaofUnderstandingMOUs/OtherMOUs/ucm412565.htm.

NH-ISAC also offers its expertise to design, develop, and implement cybersecurity exercises for member organizations hoping to test their defenses before any incident. Additionally, members can choose to have NH-ISAC monitor their public facing domain names and IP addresses for anomalous activity.

NIST Framework for Improving Critical Infrastructure Cybersecurity

Additionally, the FDA has joined other regulators in encouraging the adoption of the voluntary NIST Framework for Improving Critical Infrastructure Cybersecurity (the "NIST Framework").

The National Institute of Standards and Technology ("NIST"), an agency within the U.S. Department of Commerce, developed the framework in 2014 in response to a 2013 Executive Order charging Federal Government agencies with the improvement of cybersecurity in "critical infrastructure organizations."

The Executive Order broadly defined as "critical" any system or asset so important to the country that its "incapacity or destruction…would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

The NIST Framework has quickly gained traction in the private sector, in critical and non-critical industries alike. Law enforcement and regulators, including the U.S. Federal Trade Commission, U.S. Securities and Exchange Commission, and the U.S. Department of Justice, have increasingly cited NIST as a key source of cybersecurity guidance for U.S. companies.

The NIST Framework is focused on five core principles viewed as the basic building blocks for an effective cybersecurity program: Identify, Detect, Protect, Respond and Recover.

These principles guide companies in developing a plan for each phase of their cybersecurity strategy, from preparing for a potential breach, to detecting a potential breach quickly when it begins, and finally responding and recovering from a breach.

NIST offers these principles, like the entire framework, as a flexible tool for designing and strengthening cybersecurity. It can be specially tailored to the risk profile of the implementing company.

The NIST framework sets forth principles that help define the types of steps any company can take to strengthen its cybersecurity defenses, including:

- ***Identifying*** sensitive assets, vulnerabilities, personnel important in overseeing and executing in cybersecurity, and the risks facing the company from a possible cyber-attack;
- ***Protecting*** the company by training employees in cybersecurity awareness and implementing technical defenses to cyber-attacks;
- ***Detecting*** anomalies and potential security breaches in the company's system;
- ***Responding*** to a detected cybersecurity event to mitigate the harm and reviewing the lessons learned that can inform future defensive measures;
- ***Recovering*** from breaches if and when they happen.

When implementing these principles, healthcare stakeholders should focus on customizing them to industry-specific issues. For example, the "identify" step should involve the databases where

sensitive patient health information ("PHI") is stored. Furthermore, in the case of a network that maintains PHI, the risk tolerance must be low because a PHI release may result in a HIPAA violation. The "protect" principle will require training employees to recognize potential cyber-attacks, such as malicious actors trying to obtain the password for a patient's online account with his or her medical insurer.

The Postmarket Guidance includes specific recommendations to medical device manufacturers on implementing the NIST Framework based on the medical device risk management framework described in the guidance. We will therefore discuss the risk management framework for medical devices before turning to how the NIST framework should apply to them.

MEDICAL DEVICE MANUFACTURERS

Specific Guidance on Securing Medical Devices

The FDA describes in great detail how it expects medical device manufacturers will identify, assess, and respond to cybersecurity vulnerabilities. This description provides insight for all healthcare stakeholders on the cybersecurity standard of care the FDA believes that the healthcare industry should follow.

The FDA sets forth a framework focused on maintaining the "essential clinical performance" of medical devices, a term manufacturers should define with respect to individual devices. Manufacturers should work with others in the healthcare industry to identify device vulnerabilities and assess the risk posed to essential clinical performance.

The level of risk posed by a vulnerability will depend on an evaluation of (a) the ease of exploiting it and (b) the severity of the potential health impact that would follow. The FDA offers specific suggestions on the means for this evaluation:

- To evaluate a vulnerability's exploitability, the FDA cites the "Common Vulnerability Scoring System" ("CVSS") as a useful tool for assessing the exploitability of vulnerabilities. CVSS was issued by the Forum of Incident Response and Security Teams ("FIRST"), a nonprofit organization consisting of member organizations from various industries. FIRST works to provide best practices and tools for responding to cybersecurity threats.
- To evaluate the severity of a vulnerability's potential health impact, the FDA recommends guidance from ISO entitled "Medical devices—Application of risk management to medical devices." ISO is an independent, non-governmental international organization of national standards bodies that issues technological standards. The risk management scale for medical devices ranges from risks with negligible impact, which provide an "inconvenience or temporary discomfort," to risks with a potentially catastrophic impact that "results in patient death."

The FDA expects manufacturers to use such tools to assess vulnerabilities as presenting a "low," or controlled risk to a device's essential clinical performance, or a significant, "uncontrolled risk." The guidance includes a matrix for evaluating vulnerabilities as a controlled or uncontrolled risk based on the exploitability and severity of the potential health impact.

On one end are clearly controlled risks, which involve vulnerabilities with a low risk of exploitation and a negligible impact to health. On the other end are clearly uncontrolled risks, which involve

vulnerabilities with a high risk of exploitation and a potentially catastrophic impact on health.

These recommendations reflect a growing trend among regulators to be quite prescriptive on cybersecurity. For example, the New York Department of Financial Services communicated with a number of federal regulators late last year on the need for specific cybersecurity regulations in the financial services sector, suggesting mandates for the appointment of a chief information security officer and the implementation of multi-factor authentication.

The assessment of vulnerabilities as presenting a controlled or uncontrolled risk to essential clinical performance will determine how the manufacturer should respond to the issue, and whether the vulnerability must be reported to the FDA:

Controlled Risks: If the manufacturer determines risks are controlled, any changes that it makes to medical devices—such as routine updates and patches—to address identified risks do not need to be reported to the FDA. With respect to Class III medical devices that require premarket approval, and for which periodic postmarket reporting is required, reports must disclose even routine changes.

An example of a controlled risk might involve the detection on a medical device of malware designed to collect Internet browsing information. If the malware poses no threat to the device's essential clinical performance, then the manufacturer does not need to report to the FDA its steps to address the malware, unless the malware affected a Class III medical device.

Uncontrolled Risks: If the manufacturer determines risks are uncontrolled, the risks and remediation should be reported to the

FDA under 21 C.F.R. 806.10. However, the FDA indicates that it will not require reporting under this regulation when:

- No serious adverse events or deaths are known to be associated with the vulnerability;
- Within 30 days of learning of the vulnerability, the manufacturer implements changes or compensating controls on the device to bring the risk to an acceptable level and notifies users; and
- The manufacturer is a participating member of an ISAO, such as NH-ISAC.

Again, devices that require a periodic report must still disclose changes when they file that report. Manufacturers should also notify users about potential temporary fixes for the issue until the vulnerability is fully remediated. Further, if a manufacturer fails to address uncontrolled risks to a device's essential clinical performance, the FDA will assess the risk posed to patient health in evaluating whether a violation of the FDCA has occurred.

An example of an uncontrolled risk is a vulnerability that allows unauthorized users to reprogram a medical device in a way that could impair its medical function. Even assuming the device is not a Class III medical device, such a risk would require notification to the FDA unless no serious adverse events or deaths occurred, the manufacturer remediated and notified users within 30 days, and the manufacturer participates in an ISAO.

Implementing the NIST Framework for a Medical Device Manufacturer

An appendix to the guidance includes recommendations to medical device manufacturers on implementing the NIST Framework. These recommendations are based on the concept of "essential

clinical performance" detailed in the guidance. Rather than offering a discrete set of recommendations for each principle, the FDA offers general guidance spanning several principles at once.

For example, the guidance urges manufacturers to **identify** the essential clinical performance of their devices and any signs of cybersecurity or quality problems with their devices, at least in part by incorporating into the device design some capability to detect attacks and capture forensic evidence.

To address both principles of **protect** and **detect**, manufacturers should assess vulnerabilities with tools such as CVSS, characterize identified threats and vulnerabilities in order to triage the issues to be remediated, generate summary reports on each identified vulnerability that include a risk analysis and threat report, and implement a process to assess cybersecurity issues both horizontally, *i.e.*, across all devices in their portfolio, and vertically, *i.e.*, on specific device components.

In **protecting**, **responding**, and **recovering** from cybersecurity incidents, manufacturers should establish mechanisms for communicating with users about vulnerabilities, remediate incidents in a way that is proportional to the magnitude of the problem, and validate remediation to ensure risks were properly mitigated.

This guidance on NIST implementation is not meant to cover all considerations that should inform use of the NIST Framework, but shows how the FDA's specific guidance for device manufacturers should fit within their use of NIST. In providing these recommendations, the FDA provides concrete examples of how it expects NIST will be used in the healthcare industry.

IMPACT OF THE GUIDANCE

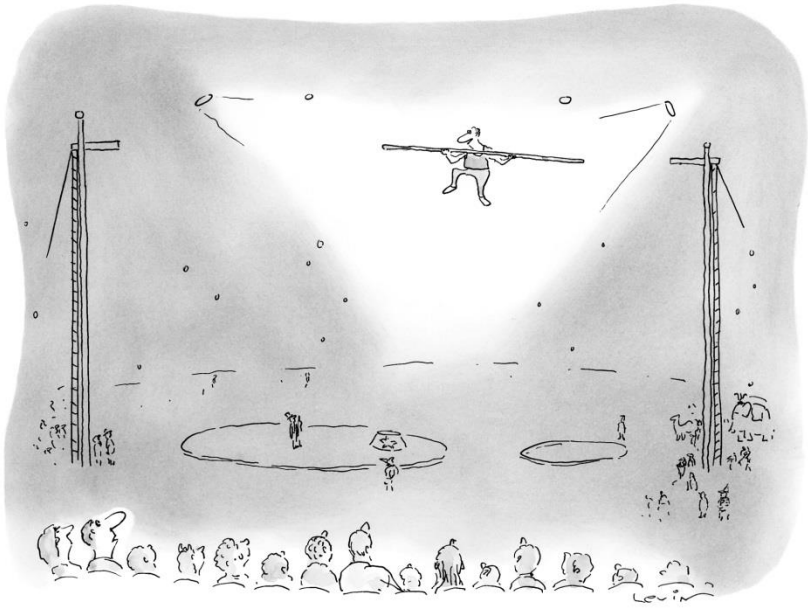
With the Postmarket Guidance, the FDA takes direct aim at imposing standards on medical devices, but it is a safe bet that neither the FDA nor other regulators will stop there.

The guidance itself emphasizes the shared responsibility of all healthcare stakeholders to address cybersecurity on an ongoing basis. Adopting the NIST Framework and participating in ISAOs seem wise steps for any business subject to FDA scrutiny.

Going forward, other regulators, the plaintiffs' bar and courts may also point to the FDA guidance as contributing to an emerging standard of care that could, in time, support legal liability under various theories.

Reproduced with permission from Bloomberg BNA Health IT Law & Industry Report™, April 25, 2016. The Bureau of National Affairs, Inc. (800-372-1033) www.bna.com.

Cross Border Issues



"It appears to be some kind of wireless technology."

Cybersecurity and data privacy are issues of transnational concern. In this section, we focus primarily on developments coming out of the European Union that have far-reaching effects. First, we provide an analysis of the scope of the new European General Data Protection Regulation ("GDPR") which will come into force in May 2018, including what companies can do now to ensure they don't run afoul of the GDPR.

We also examine ongoing developments in the transfer of personal data between the U.S. and the EU following the European Court of Justice's ruling late last year that the Safe Harbour Protocol was invalid, including the new EU-U.S. "Privacy Shield" which recently was given a conditional nod of approval by EU privacy regulators.

European Union General Data Protection Regulation:

Not Just an EU Issue

The EU General Data Protection Regulation ("GDPR"), entering into force in May 2018, significantly changes the EU's data protection landscape. EU businesses of course cannot ignore the GDPR – but neither can U.S. businesses, as the GDPR expands the territorial scope of EU data protection law to businesses that target EU residents. This includes businesses without a physical footprint in the EU. Substantively, the GDPR expands individuals' rights and imposes heightened obligations on data controllers (*i.e.*, those who decide how and why an individual's personal data is processed) and data processors (*i.e.*, those who obtain, record or hold data on a data controller's behalf).[1]

The GDPR promises to be more than a paper tiger – a business that doesn't meet the GDPR's expanded and more onerous obligations will face fines up to the higher of €20 million or 4% of the business's worldwide annual turnover. Businesses can minimize their risk by implementing a structured, committed and adequately resourced data protection program.

[1] Both concepts retain the same meaning as in the existing EU Data Protection Directive. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L281), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

THE GDPR'S SCOPE – TIME TO ASSESS AND RE-ASSESS

The GDPR will replace the existing EU Data Protection Directive (the "Directive") which, at over 20 years old, is widely regarded as showing its age. Since the Directive's inception, the volume of data that businesses produce, collect, store and process has increased exponentially. The GDPR seeks to address this new frontier in a harmonized manner and put data protection front and center for businesses that operate in or deal with the EU.

With the GDPR's text now finalized[2] and some jurisdictions already introducing equivalent laws ahead of the GDPR's formal implementation,[3] businesses may well want to consider now whether the GDPR applies to their current (or future) activities. If so, they might wish to consider conducting a GDPR readiness review sooner rather than later.

Come May 2018, a business will have to comply with its provisions if it:

1. is an EU-based data controller or processor; or

2. is based outside the EU and:

---

2 Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, 2016 O.J. (L119), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

3 France, for example, has taken steps to introduce a number of GDPR provisions early by tabling amendments to its existing data protection act. These include implementation of GDPR's higher sanctions for breach and the right to be forgotten, amongst others.

a. processes EU residents' personal data in connection with goods or services provided in the EU; or

b. monitors EU residents' behavior in the EU.

Unlike today, then, businesses that target EU consumers from outside the EU *and* process their data outside the EU will be covered by the EU's data protection laws once the GDPR is in force. Even for businesses already subject to and fully compliant with EU data protection law, the additional requirements in the GDPR are likely to take time to implement.

A GDPR READINESS REVIEW – HOW TO PREPARE

The GDPR is designed to ratchet up protection for consumers in a host of ways, including:

1. an obligation for certain businesses to appoint a data protection officer;

2. new direct obligations on data processors, including to notify the data controller of data breaches without undue delay;

3. heightened requirements to obtain consumers' free, unambiguous, specific and informed consent to data processing;

4. breach notification obligations, both to data protection authorities and affected individuals;

5. a codified "right to be forgotten," *i.e.*, the right to have your personal data erased without undue delay;

6. risk management obligations, including requirements to maintain certain documentation and to conduct impact assessments; and

7. dramatically increased penalties for breaches of data protection law.

For those businesses considering whether to conduct a GDPR readiness review, the following checklist may be helpful:

First, ***familiarize***. All relevant decision-makers within a business should be aware of the GDPR, its requirements and the impact it will have on their organization. "Tone from the top" is undoubtedly key to any data protection program's success. Businesses also might consider identifying key employees who have a particular impact on their business's data protection risk profile and informing them of, training them on and monitoring them for GDPR compliance. Pervasive engagement is key.

Second, ***identify***. While not a GDPR-specific exercise, mapping a business's data architecture, what personal data the business holds and how the business stores and uses the data could help businesses prepare for the GDPR.

Third, ***assign accountability***. The GDPR specifically requires some businesses to designate a data protection officer *e.g.*, those whose core activity is data processing and engage in systematic, large-scale monitoring of individuals' personal data. Whether or not subject to that requirement, any business can benefit from a robust accountability framework and a culture of continuous assessment of data protection risk and compliance. Clear reporting lines that reach up to senior management and the board can be helpful, not only if

there is a data breach (where the new notification requirements will add significant pressure), but also when considering strategically important data protection issues (*e.g.*, how to lawfully effect cross-border transfers of personal data).

Fourth, ***protect data by design***. Businesses may find it easier to comply with GDPR if they treat data protection as integral to all processes and products involving personal information. As a general matter, processes and products that are conceived and deployed with data protection in mind from the outset will lend themselves to compliance more readily than processes and products where data protection considerations are "bolted on" at the back end. As a practical matter, this means that internal lawyers or others with GDPR compliance responsibility may wish to review processes and products as early in the development cycle as is practicable.

Fifth, ***review, revisit and revise***. Consider the business's existing policies and procedures in light of the GDPR and whether they address individuals' rights under the GDPR effectively and efficiently. Key areas include ensuring that the business's privacy policies are easily accessible and that consent for personal data processing is GDPR-compliant. Ongoing assessment of policies and procedures is one way to help ensure that a business is compliant not just on paper but also in practice.

CONCLUSIONS

As the GDPR breathes new life into EU data protection law, early engagement will help affected businesses to cope. With less than two years to prepare for GDPR's entry into force, businesses have the opportunity to plan carefully for compliance.

Client Update:

Transfers of Personal Data to the United States: European Court of Justice Rules the Safe Harbour Protocol Is Potentially Invalid

In a decision that could have significant implications for the transfer of personal data from the European Union to the United States, the Court of Justice of the European Union (the "CJEU") ruled that the approval previously granted by the European Commission (the "Commission") to the EU-US Safe Harbour protocol ("the Safe Harbour") is not valid. The Safe Harbour has been one of the ways in which personal data may be transferred from countries within the EU to the United States in conformity with the EU Data Protection Directive 95/46/EG (the "Directive"). As a consequence of this decision, companies that have registered under the Safe Harbour can no longer be certain of their ability to rely on that protocol as a lawful method to make such transfers.

BACKGROUND

The Directive and the legislation implemented by Member States of the EU[1] and the other members of the European Economic Area (the "EEA"), which comprises the EU, Iceland, Liechtenstein and Norway, allow transfers of personal data from EU countries to countries outside the EEA only under limited circumstances. Either the destination country must provide an "adequate level of protection" to personal data, or one of a specific set of other conditions must apply to the transfer.

---

[1] Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the UK.

The Commission has made determinations that a number of individual third countries ensure an adequate level of protection, allowing transfers to those countries subject only to the same restrictions on transfers within the EEA. Although the United States is not among those countries, the United States Department of Commerce and the European Commission agreed upon the Safe Harbour framework in 2000, to enable the transfer of personal data to the Safe Harbour registrants in conformity with the Directive.

Under the Safe Harbour, companies subject to the jurisdiction of the US Federal Trade Commission or the US Department of Transportation could, by registering with the Department of Commerce, self-certify that they apply the following protections to EU-originating personal data: (i) they agree to notify individuals about the purposes for which they collect and use information about them; (ii) individuals are given the opportunity to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorised; (iii) they take reasonable precautions to protect personal information from loss, misuse, and unauthorised access, disclosure, alteration, and destruction; and (iv) individuals have access to personal information about them that an organisation holds and be able to correct, amend, or delete that information where it is inaccurate.[2]

CLAIM

The CJEU came to consider the validity of the Safe Harbour as a result of a claim relating to Facebook brought by Maximilian Schrems, an Austrian citizen. As with the Facebook data of other

[2] For additional information about the substance of the Safe Harbour protocols, see https://safeharbor.export.gov/list.aspx.

users within the EU, some or all of the data provided by Mr. Schrems to Facebook are transferred from Facebook's Irish subsidiary – its main operating arm in the EU – to the United States using the Safe Harbour, to which Facebook subscribed. Mr. Schrems complained to the Irish data protection regulator that the revelations made by Edward Snowden in 2013 concerning the activities of the US intelligence services meant that the United States did not offer sufficient protection against surveillance over his transferred personal data. The Irish regulator rejected his complaint, primarily on the ground that Facebook had self-certified that it complied with the Safe Harbour protocols, which had been approved by the Commission, and the regulator had no power to make a finding contrary to the Commission's determination. Mr. Schrems pursued the issue in the Irish courts, as a result of which the CJEU was called on to consider the issue.

DECISION

In the decision, the CJEU ruled that that the Commission decision endorsing the Safe Harbour protocol does not limit the powers available to a national data protection supervisory authority. As a result, national regulators are able and required to examine whether the transfer of data to a third country complies with the applicable legal requirements, regardless of any previous determinations by the Commission.

Therefore, it ruled that the Irish regulator should have made a ruling on whether data transferred under the Safe Harbour would receive an adequate level of protection.

As a next step, the CJEU stated that if a regulator did find that transfers under the Safe Harbour – or pursuant to a different Commission determination – provided inadequate protection, then

legal proceedings must be commenced, as only the CJEU has jurisdiction to declare a Commission decision invalid.

Consequently, the CJEU went on to consider whether the Commission's decision relating to the Safe Harbour was valid: it determined that it was not.

The CJEU determined that the Safe Harbour no longer offers adequate protection for two reasons.

First, the CJEU noted that companies subject to US law are bound to disregard the Safe Harbour's rules and protocols protecting data privacy if they conflict with the national security, public interest, and law enforcement requirements of the United States. As a result, the Safe Harbour does not prevent, and indeed enables, interference by US public authorities with the fundamental rights of individuals, as guaranteed by EU human rights law. The CJEU held that legislation allowing US authorities to have access on a generalised basis to the content of electronic communications, without regard for necessity and notwithstanding the Safe Harbour's protections, compromised the fundamental right to respect for private life as reflected in EU human rights law.

Second, the CJEU considered individuals' rights of redress against surveillance by US authorities. The court found that individuals subject to surveillance of their personal data could not pursue adequate legal remedies in order to access, rectify, or erase the data, and held that the absence of such rights compromised the fundamental right to effective judicial protection.

The CJEU is the highest court of the EU and there is therefore no appeal against its judgment to any other court within the EU. The

immediate consequence of the decision is that the Irish court (and possibly the Irish data protection authority at some stage) must consider Mr. Schrems's complaint and decide whether the transfer of the data of Facebook's European users to the United States should be suspended on the ground that the United States does not afford an adequate level of protection of personal data. It will need to do so by considering the factual and legal aspects of the treatment of personal data in the United States.

The wider implications remain to be seen, but may be significant. On the one hand, because the CJEU ruled that data protection authorities must be allowed to review and challenge any previous determinations of the Commission, it is possible that there may be challenges not only to the Commission's findings of adequacy in respect of other third countries, but also to the other currently accepted methods of transferring data from the EU to the United States and elsewhere, such as the use of data transfer agreements (which may, however, also come under some scrutiny in the wake of the CJEU's decision).

On the other hand, companies that have registered under the Safe Harbour regime are not prohibited from transferring personal data to the United States. Nonetheless, the arrangements by which they transfer data, and the adequacy of protection in the United States for such data, may be reviewed by the Member States' data protection authorities. The CJEU's decision confirms the authorities' right and ability to review data transfer arrangements, even those subject to the Safe Harbour framework, but the authorities and courts of the Member States may well view the protections offered by the Safe Harbour in different ways. At a minimum, it can be expected that there will be an ongoing dialogue within each Member State as to the adequacy of the Safe Harbour protection standards and whether

personal data is otherwise adequately protected when it is transferred by companies to the United States.

Almost certainly, the discussions between the United States and the EU regarding the Safe Harbour will now be reinvigorated, including with respect to developing other means by which data could be transferred to the United States.

Entities that transfer data from the EU to the United States, whether on a regular or *ad hoc* basis, will need to review and assess the meaning of the ruling of the CJEU, and its consequences, whether they rely on the Safe Harbour or on other mechanisms, such as model contracts, that have been sanctioned by the European Commission.

This client update was originally issued on October 6, 2015.

Client Update:

EU-U.S. Privacy Shield Open for Self-Certification on August 1

On August 1, 2016, U.S. organizations can finally begin to submit self-certification requests to the U.S. Department of Commerce under the new EU-U.S. "Privacy Shield." This opens a new era for the lawful transfer of personal data from the European Union westward across the Atlantic. The Commerce Department has published a practical guide, "How to Join Privacy Shield: Guide to Self-Certification," that sets out the steps to participation.[1]

WHAT CLEARED THE WAY FOR THE PRIVACY SHIELD TO BECOME OPERATIONAL?

On July 12, 2016, the European Commission adopted an "adequacy decision"[2] ("Decision") under the EU Data Protection Directive,[3] approving the final form of the Privacy Shield. The Decision entered into force the same day.[4]

The adequacy decision ended, at least for now, a process of negotiation and debate that began after the Snowden revelations in 2013 and culminated in the October 2015 European Court of Justice ("CJEU") *Schrems* decision striking down the Privacy Shield's

---

1 *See* http://tinyurl.com/jpm3zm6.

2 *See* http://tinyurl.com/hc26oqs.

3 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

4 *See* EU Commission press release dated July 12, 2016, http://tinyurl.com/jeg3doq.

predecessor, the Safe Harbor.[5] The Privacy Shield, too, could yet face challenges in the CJEU or elsewhere. Subject to that possibility, however, the adequacy decision means that EU personal data can now flow freely from the 28 EU Member States (and the three European Economic Area members, Norway, Liechtenstein and Iceland) to U.S. organizations that self-certify adherence to the Privacy Shield Principles. The Privacy Shield framework will be published in the Federal Register, and the self-certification process with the U.S. Department of Commerce will start on August 1, 2016.[6]

WHAT ARE THE PRIVACY SHIELD PRINCIPLES AS FINALLY ADOPTED?

The following Privacy Shield Principles ("Principles") form the cornerstones of EU data protection compliance for transatlantic data transfers:

- Notice. A participating U.S. organization handling EU personal data must inform individuals about the scope of the organization's participation in the Privacy Shield, the type of personal data collected, the purpose of processing that data and the individual's access to legal redress.
- Choice. The organization must offer the individual the opportunity to opt out of having their personal information either disclosed to third parties or used for a materially different

[5] *See* the Debevoise Client Update "Transfers of Personal Data to the United States: European Court of Justice Rules the Safe Harbour Protocol Is Potentially Invalid," dated October 6, 2015, http://tinyurl.com/hvad4zm, and Debevoise FCPA Update November 2015, http://tinyurl.com/hjzxklk.

[6] *See* the U.S. Department of Commerce press release dated July 12, 2016, http://tinyurl.com/zh26mvj.

purpose than that for which the data was originally collected. In the case of sensitive information (medical or health conditions, racial or ethnic origin, etc.), organizations generally must obtain opt-in consent.

- Security. The organization must take reasonable and appropriate security measures to protect personal information from loss, misuse, unauthorized access, etc. Specific security measures are not dictated by the terms of the Privacy Shield.
- Data Integrity and Purpose Limitation. Personal information collected must be limited to that which is relevant for the purposes of the processing. The organization must take reasonable steps to ensure that the personal data collected is reliable for its intended use, accurate, complete and current. Personal information can only be retained as long as it serves the purpose for which it was collected.
- Access. Individuals have the right to access their personal information held by the organization and the right to correct, amend or delete information that is inaccurate or has been processed in violation of the Principles.
- Accountability for Onward Transfer. In case of an onward transfer from the self-certifying organization to a third-party controller or an agent, the organization has to contract with the data recipient to provide the same level of protection as under the Shield.
- Recourse, Enforcement and Liability. The organization must provide for a mechanism that assures compliance with the Principles. In the case of human resources data collected in the context of an employment relationship, the organization must commit to cooperate with European data protection authorities and to comply with those authorities' advice.

The Privacy Shield also includes a set of Supplemental Principles, which flesh out the above Principles by specifying such detailed steps as the performance of due diligence and audits, the means of processing of human resources data and the terms of data processing contracts for onward transfers.

WHAT ROLE WILL THE U.S. GOVERNMENT PLAY?

To obtain the protections of the Privacy Shield, a U.S. organization must self-certify adherence to the U.S. Department of Commerce. Participants must (a) subject themselves to the investigatory and enforcement powers of the U.S. Federal Trade Commission or the U.S. Department of Transportation; (b) publicly declare their commitment to comply with the Principles; (c) publicly disclose a privacy policy consistent with the Principles and (d) fully implement the Principles. The certification must be renewed annually.

The Principles provide for several carve-outs, providing that a U.S. organization may limit adherence to the Privacy Shield to the extent necessary (a) to meet U.S. national security, public interest, or law enforcement requirements or (b) to comply with U.S. statutes, government regulations, or case law. The organization must indicate in its privacy policy if it expects that exceptions under (b) will apply on a regular basis.

A self-certifying organization's failure to comply can lead to enforcement measures under Section 5 of the Federal Trade Commission Act,[7] which prohibits unfair and deceptive acts, or under other laws or regulations prohibiting such acts.

[7] 15 U.S.C. § 45(a).

The Department of Commerce will maintain a public list of U.S. organizations that have self-certified. Privacy Shield protections are assured from the date that the Department places the organization on the list. The Department will remove an organization from the list if it voluntarily withdraws from the Privacy Shield or if it fails to complete its annual re-certification. The Department will also remove organizations that persistently fail to comply with the Principles. Such organizations must return or delete any personal information of European data subjects they received under the Privacy Shield.

WHAT LEGAL REDRESS WILL BE AVAILABLE TO EU DATA SUBJECTS?

EU data subjects who believe that their data has been misused will have several redress possibilities:

- Filing of a complaint with the self-certified organization. Organizations must respond within 45 days of receiving a complaint.
- Use of a free Alternative Dispute Resolution process through an independent ADR provider. The organization will be required to include information in its published privacy policies about the independent dispute resolution body to which European data subjects may address complaints.
- Filing of a complaint with the U.S. Department of Commerce.
- Filing of a complaint with the data subject's "home" data protection authority. The authority will refer the complaint to the U.S. Department of Commerce, which will respond within 90 days, or the Federal Trade Commission, if the Department of Commerce is unable to resolve the matter.
- If a case is not resolved by other means, there will be an arbitration mechanism. Individuals may file a notice to the U.S.-

seated Privacy Shield Panel, a dispute resolution body that can issue binding decisions against U.S. self-certified organizations, providing non-monetary equitable relief.

- Individual complaints based on a fear that personal information has been accessed in an unlawful way by U.S. authorities in the area of national security will be handled by an Ombudsperson independent from the U.S. intelligence services.

WHAT ARE THE MAIN DIFFERENCES COMPARED TO SAFE HARBOR?

The Privacy Shield was drafted against the backdrop of perceived shortcomings in the Safe Harbor regime, especially the perception that the Safe Harbor had left European data subjects unduly exposed to U.S. government surveillance. The Privacy Shield addresses these concerns by requiring companies to disclose certain mandatory content in their privacy policies and by adding obligations for U.S. data importers, including tightened conditions and stricter liability provisions for onward transfers to third parties outside the framework. The Federal Trade Commission is expected to increase its enforcement efforts against participating companies to counter the argument of prior lax Safe Harbor oversight. The new variety of EU data subjects' accessible and affordable avenues to individual redress also promises greater scrutiny and compliance under the Privacy Shield as compared to Safe Harbor.

IS THE PRIVACY SHIELD STILL SUBJECT TO REVIEW AND CHALLENGE?

Yes, in a number of ways. The European Commission will continuously monitor the functioning of the Privacy Shield. There will also be an annual joint review by the European Commission and the U.S. Department of Commerce, focusing in particular on the safeguards relating to national security access – *i.e.*, the Snowden-

inspired concerns, regarding arguably excessive U.S. intelligence access to personal information, that drove the *Schrems* decision. If U.S. organizations or public authorities do not abide by their commitments, then the European Commission can suspend, amend or repeal the Privacy Shield or limit its scope.

The *Schrems* decision leaves open the possibility that a similar legal challenge to the Privacy Shield could emerge in the CJEU. *Schrems* also leaves open that an individual country's data protection authority may seek to question or limit the application of the Privacy Shield to its country's citizens' data. The Article 29 Working Party – a group of representatives of national data protection authorities within the European Union, which has been notably skeptical towards the Privacy Shield thus far – has advised that it will conduct a coordinated analysis of the final form of the Privacy Shield, and will publish a statement as soon as possible.[8]

Also relevant is the new General Data Protection Regulation ("GDPR"),[9] which will replace the current Data Protection Directive on May 25, 2018 as the overall privacy law directly binding within the European Union. Adequacy decisions issued during the life of the Directive will be respected once GDPR comes into force.[10] Nonetheless, the Article 29 Working Party has advised that, once the GDPR enters into force, it will review the adequacy decision

---

8 *See* Article 29 Working Party press release dated July 1, 2016, http://tinyurl.com/jmyqr7d.

9 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

10 *See* Article 45 paragraph 9 GDPR.

regarding the Privacy Shield with a view to the higher level of data protection that the GDPR offers.[11]

Time will tell how robust the Privacy Shield proves to be in the face of any of these potential reviews and challenges. For today, the headline news is that U.S. organizations finally have a specific new option for data transfers to replace the Safe Harbor.

This client update was originally issued on July 26, 2016.

[11] *See* Article 29 Working Party statement dated April 13, 2016, http://tinyurl.com/h9hbd2o.

Private Litigation Developments

"It's very important that you try very, very hard to remember where you electronically transferred Mommy and Daddy's assets."

In this section, we address recent trends in private litigation arising from data breaches. In particular, we offer tips for maintaining privilege over cybersecurity assessments and investigations; consider the potential increase of post-data breach litigation in the United Kingdom and address recent developments in how courts have addressed standing in class action cases.

Over the last year, a number of courts have considered whether consumer class actions following a data breach can withstand a

motion to dismiss. As set forth in our client updates regarding the recent *Neiman Marcus* and *Case v. Miami Beach Healthcare Group* decisions, courts have taken varying approaches to determining whether consumers have standing to bring claims in the wake of a data breach. The Seventh Circuit recently doubled down on its *Neiman Marcus* holding in *Lewert v. P.F. Chang's China Bistro, Inc.*, allowing consumer claims to proceed. Courts outside of the Seventh Circuit, however, appear to treat the *Neiman Marcus* approach as the minority position, finding that plaintiffs who have not been victims of fraud resulting from a data breach do not have Article III standing because they have suffered no actual injury. Recently, federal courts in Nevada and Maryland have underscored the importance of these pleading requirements in class action suits arising from data breaches.

- The District of Nevada in *In re Zappos.com, Inc. Customer Data Security Breach Litigation* dismissed the amended complaint of plaintiffs who alleged that their email accounts were accessed by hackers and used to send unwanted advertisements to their contacts, finding that such allegations did not constitute an injury. Plaintiffs who had alleged specific instances of fraud resulting from the breach, including fraudulent credit and debit card purchases, were permitted to pursue their claims. The court also granted Zappos' motion to strike the class allegations from the complaint because the proposed class definition, which included any person whose PII was compromised during the breach, was overbroad.
- In *Chambliss v. Carefirst, Inc.*, the District of Maryland granted Carefirst's motion to dismiss a putative class action, finding that none of the plaintiffs' alleged injuries were sufficient to establish Article III standing. In *Chambliss*, only the plaintiffs' names, birth dates, email addresses and subscriber identification numbers

had been subject to unauthorized access as a result of the data breach, rather than social security numbers or credit card numbers. No actual fraud was alleged to have resulted from these breaches, and the court ruled that allegations of an increased risk of fraud were mere speculation. The plaintiffs have appealed, and thus it will be important to watch for a decision from the Fourth Circuit in the coming months.

Cybersecurity Vendors and the Attorney-Client Privilege

As cybersecurity threats have increased, so has regulatory scrutiny of the steps companies take to address those threats. In the face of that scrutiny – which, as described elsewhere in this book, ranges from a continued focus on cybersecurity in examinations to increasingly frequent enforcement actions by the SEC, the CFPB and others against companies whose cyber policies and procedures are viewed as inadequate – companies and their counsel frequently turn to third parties with technical expertise. For purposes of this article, we'll refer to those third parties as "Cyber Vendors."

Cyber Vendors may provide any number of valuable cybersecurity-related services to companies, and, as with any other non-legal service provider, the ordinary expectation is that their work is not privileged. But in certain limited circumstances, companies may seek to assert privilege over the work of their Cyber Vendors. This comes up most frequently in two contexts: first, when a company seeks legal advice about whether its cybersecurity practices and policies comply with legal and regulatory requirements; and second, when a company's counsel requires forensic assistance in investigating a breach. In those situations, counsel often needs a Cyber Vendor's technical expertise in order to effectively render legal advice. When a Cyber Vendor is retained for that purpose, if managed properly, its work should be privileged. This article explains the basic rules on applying the privilege to non-lawyers, discusses two recent cases in which courts have found that privilege applied to the work of Cyber Vendors, and outlines the steps that

companies and their counsel should consider taking to maintain privilege over the work Cyber Vendors do to assist counsel.

BACKGROUND RULE ON NON-ATTORNEY AGENTS

Non-attorney agents and subordinates working under the direct supervision of an attorney are ordinarily included within the scope of the attorney-client privilege.[1] This rule is not limited to agents like paralegals who perform ministerial or clerical tasks; the privilege may also apply to those who provide subject-matter expertise to facilitate or enable legal advice.

In one leading case, *United States v. Kovel*[2], the United States Court of Appeals for the Second Circuit extended the attorney-client privilege to cover communications with an accountant hired to facilitate tax-related legal advice. The court analogized the accountant to a foreign language interpreter: accounting concepts "are a foreign language to some lawyers in almost all cases, and to almost all lawyers in some cases. Hence the presence of an accountant, whether hired by the lawyer or the client, while the client is relating a complicated tax story to the lawyer, ought not destroy the privilege." The application of privilege in this circumstance, however, is qualified: the client must be pursuing legal advice, not accounting advice, and the accountant's presence and involvement with the client must be "necessary, or at least highly

---

1 *E.g. Zenith Radio Corp. v. Radio Corp. of Am.*, 121 F. Supp. 792, 794 (D. Del. 1954) (privilege applied to "general office clerks and help, law clerks, [and] junior attorneys…under the personal supervision of the attorney through whom the privilege passes"); *United States v. United Shoe Mach. Corp.*, 89 F. Supp. 357, 358 (D. Mass. 1950) (noting that the privilege applies to communications with "a member of the bar of a court, *or his subordinate*" (emphasis added)).

2 296 F.2d 918 (2d Cir. 1961).

useful, for the effective consultation between the client and the lawyer which the privilege is designed to permit."

Kovel laid the groundwork for extending privilege beyond the walls of the law firm. Since *Kovel*, courts have extended the privilege to a number of other subject-matter experts, including public relations consultants,[3] financial advisors,[4] and medical experts.[5] But these decisions are fact-specific, and courts have frequently pointed out the important caveat to the *Kovel* rule: "the advice rendered must be that of the attorney, not the agent."[6]

A straightforward application of these rules suggests they ought to apply to Cyber Vendors when they are retained to provide technical advice to counsel so that counsel, in turn, can provide legal advice to its clients. The early case law in this area suggests that courts agree.

PRIVILEGE IN CYBER CASES

Two cases demonstrate in practice the extension of privilege to Cyber Vendors.

Genesco Inc. v. Visa U.S.A., Inc.

Between December 2009 and December 2010, Genesco, a Nashville-based apparel retailer with more than 2000 stores in the United States, Canada, the United Kingdom and Ireland, was the victim of a cybersecurity breach. The company's computer systems were

---

3 *In re Grand Jury Subpoenas Dated Mar. 24, 2003*, 265 F. Supp. 2d 321, 330 (S.D.N.Y. 2003).

4 *Goldstein v. F.D.I.C.*, 494 B.R. 82, 89-90 (D.D.C. 2013).

5 *Sprague v., Dir., Office of Workers' Comp. Programs*, 688 F.2d 862, 869-70 (1st Cir. 1982).

6 *Gucci Am., Inc. v. Guess?, Inc.*, 271 F.R.D. 58, 70-71 (S.D.N.Y. 2010).

attacked by cyber criminals, who used malware to gain access to payment card data transmitted by Genesco to its payment processors.

Genesco publicly announced the breach in December 2010, and as a result, Visa assessed Genesco's merchant banks more than $13 million in fines and reimbursement expenses for their failures to ensure that Genesco complied with Payment Card Industry Data Security Standards ("PCI DSS"). As is typical, the banks passed these fines on to Genesco. Genesco, in turn, sued Visa to challenge its decision to levy the fines.

Genesco had retained two separate Cyber Vendors in connection with the breach. First, it retained the PCI forensic investigator Trustwave to investigate the breach and prepare a report. (Genesco did not assert privilege over that report, which was shared with Visa and the merchant banks.) Second, the company – through its general counsel – retained the cybersecurity firm Stroz Friedberg to assist in-house and outside counsel in rendering legal advice to Genesco about the breach and the Trustwave report. Visa sought discovery into Stroz's work, and Genesco asserted attorney-client and work product protection privileges.

The court agreed with Genesco, holding that the requested materials were protected from discovery by the attorney-client privilege, because "attorneys' factual investigations fall comfortably within the protection of the attorney-client privilege," and "[t]his privilege extends to the Stroz firm that assisted counsel in its investigation." The court reasoned that, in principle, cybersecurity consultants are no different than accounting consultants, whose work product and communications have traditionally been held to be subject to the attorney-client privilege. Similarly, the court held that the forensic

reports constituted protected attorney work product because "work product privilege also attaches to an agent's work under counsel's direction."

In re Target Corp. Consumer Data Security Breach Litigation
In the aftermath of Target's December 2013 data breach, involving the theft of millions of credit card numbers and the personal information of millions of its customers, Target engaged two separate teams from Verizon Business Network Services as Cyber Vendors. One team was retained by Target to conduct an investigation into the breach on behalf of several credit card companies. The second team was retained jointly by Target and its outside counsel, to "enable counsel to provide legal advice to Target, including legal advice in anticipation of litigation and regulatory inquiries."

The plaintiffs in a multi-district class action heard in the U.S. District Court for the District of Minnesota sought to discover documents that were the product of the second track of Verizon's investigation. The Court reviewed a number of the relevant documents in camera and determined that they were covered by the attorney-client privilege. This decision was grounded largely on Target's representation that Verizon's work on the second track was "focused not on remediation of the breach…but on informing Target's in-house and outside counsel about the breach so that Target's attorneys could provide the company with legal advice and prepare to defend the company in litigation that was already pending and was reasonably expected to follow."

BEST PRACTICES FOR MAINTAINING PRIVILEGE OF CYBER VENDORS' WORK

These cases collectively point to some common sense steps that companies and their counsel can take to ensure that the attorney-client privilege applies to certain work performed by Cyber Vendors where maintaining privilege is desirable.

- **Appearances matter**. Courts will consider whether the company, its counsel and its Cyber Vendors take steps that demonstrate the belief that Cyber Vendor work is covered by privilege.
  - Counsel should formally retain Cyber Vendors. Whether in-house counsel retains the Cyber Vendor (as in *Genesco*), or outside counsel, the company and the Cyber Vendor sign a three-party engagement letter (as in *Target*), Cyber Vendors should be retained by counsel and the agreement or engagement letter should make clear that the purpose of the engagement is to facilitate the provision of legal advice.
  - Materials prepared by Cyber Vendors working on behalf of counsel should make that fact abundantly clear and should include privilege headers ("Privileged"; "Prepared For and Delivered to Counsel"; "At the Request/Instruction of Counsel").

- **But appearances are not *all* that matter**. When a company seeks ordinary-course cybersecurity advice from a Cyber Vendor, courts will not permit the company to circumvent the usual discovery rules merely by structuring the engagement through counsel. Cyber Vendors should be made aware of <u>when</u> and <u>why</u> their work is considered privileged. The Court in the *Target* case placed significant weight on the fact that the company's chief legal officer represented that the Cyber Vendor's work was done to support counsel, and that all involved understood that their

work was for the purpose of facilitating the provision of legal advice.

- **Where feasible, consider segregating investigations from other technical advice**. Where possible, clients should consider separately retaining teams of Cyber Vendors, with one assisting counsel and investigating at its direction and the other doing non-privileged technical remediation work.
- **When assigning work to a Cyber Vendor, be mindful of the purpose of the work**. The privilege analysis turns, in significant part, on whether the Cyber Vendor is working in order to permit the attorney to render legal advice or in order to provide its own technical advice. Courts often require that the non-lawyer provide services that are necessary for the lawyer to render advice in order for the privilege to apply.
  - *Gathering facts*: if the facts will be transmitted and explained to the lawyer, so that the lawyer can give advice, the privilege should apply. If the facts will be analyzed so that the Cyber Vendor can offer advice or take action itself, the privilege may not apply.
  - *Generating work product*: if the work product will be transmitted to the lawyer, so that the lawyer can use it to advise the client, the privilege should apply. If the work product is directed to the client, or offers technical rather than legal advice, it may not be privileged.

Into the Breach:
The UK Litigation Landscape

INTRODUCTION

In the UK, the regulatory implications of breaches of privacy have garnered much attention, and will likely continue to do so as the EU General Data Protection Regulation enters into force.[1] By contrast, comparatively little attention has been devoted to the civil litigation that can erupt following a data breach involving sensitive information. The increasing prevalence of such incidents, frequently the result of criminal hacking, means that the litigation risks to which data breaches give rise are likely to increasingly come into the spotlight.

A 2015 survey conducted by PWC found that 90% of large UK businesses and 74% of small UK businesses suffered a data breach in the previous year (up from 81% and 60% respectively in the year prior to that). In circumstances where 9 out of 10 large businesses are suffering a data breach of some sort, many of which involve enormous quantities of data, it is almost inconceivable that litigation arising out of such incidents will not soon become a regular feature in UK courts, as they are increasingly becoming in the United States, discussed elsewhere in this section.

The contours of the litigation landscape are beginning to emerge in the United Kingdom as a result of cybersecurity breaches. While some features of this landscape are uniquely creatures of English

[1] This remains the case notwithstanding the uncertainty which has been created by the Brexit referendum in which a majority of UK voters opted to leave the EU. The UK will almost certainly need to impose comparable standards in any subsequent legislation even if the GDPR is not directly applied, within the context of any future broader trade deal with the EU.

law, as is often the case, the majority of them are directly foreshadowed by legal developments in United States.

THE LITIGATION LANDSCAPE IN THE UK

English law provides three primary avenues for suit following a data breach:

- ***Common-Law Privacy Actions***. There are a variety of causes of action available to potential Plaintiffs under English law principles governing the protection of information. These common-law claims range from actions for breach of confidence (which derive their origins from equitable obligations to safeguard confidential information), to the more novel tort of misuse of private information (explicitly recognized most recently by the Court of Appeal in the case of *Google Inc. v. Vidal-Hall & Ors*, [2015] EWCA Civ 311).[2] Both types of actions can be pursued by those who suffer tangible losses as a result of a data breach.
- ***Statutory Privacy Actions***. In addition to common-law claims, there are statutory rights of action under section 13 of the UK Data Protection Act 1998 (DPA 1998), which provide a cause of action for damages against data custodians for losses that victims of a data breach may suffer due to a failure to comply with certain security standards provided for in DPA 1998. As of this writing (subject to reversal by the UK Supreme Court in the *Google* case), plaintiffs suing under this statutory action may bring a claim on the basis of mere distress, without having to demonstrate any

[2] The Court of Appeal is the second most senior court in the English judicial hierarchy. This case is presently under appeal to the UK Supreme Court. However the Supreme Court refused permission to appeal the findings of the Court of Appeal in relation to the existence and extent of the tort of the misuse of private information.

monetary losses. A further element of uncertainty on the scope of this statutory right of action is created by the recent 'Brexit' vote in the UK, as the arguments its enlargement were based on were derived from various provisions of the European Convention on Human Rights – which the UK may ultimately choose to opt out of in the event of an exit from the EU.

- ***Common-Law Breaches of Duty Actions***. Another, potentially significant, cause of action available to potential plaintiffs are a range of general claims for breach of duty, such as negligence, which may be brought by those who suffer tangible losses as a result of a leak of sensitive data.

In addition to these causes of action, English law also provides for actions to be brought by a class of individuals, which has already been leveraged in the context of a data breach. The UK High court recently granted a Group Litigation Order to approximately 2,000 employees of the UK supermarket chain Morrisons whose personal information had been leaked by a disgruntled former employee, demonstrating the litigation risk that a breach of data security poses to UK companies.

There is legal uncertainty as to the applicable standard of care expected of data custodians, and the contours of liability are still being determined by the courts. There are already clues as to what standards data custodians will be tested against in England, such as the requirements and procedures set out in guides published by the UK Information Commissioner's Office. It is also likely that UK courts will look across the pond at what standards are being applied in the United States.

WHAT TO EXPECT AHEAD

The sheer quantity of data which has been in issue in recent high-profile breaches in the UK (*e.g.*, 2.4 million customers' details were compromised in the cyber-attack on the UK retail chain Carphone Warehouse in 2015) – coupled with the fact that the right to sue in respect of emotional harm or distress may not require direct proof of any pecuniary damage – increases the likelihood of consumer litigation in the UK.

Developments in the United States are also strong indicators of what lies on the horizon in the UK in this respect. Derivative actions have been pursued by shareholders against boards of directors in the wake of large data breaches involving alleged failures by management to put in place and maintain proper systems for the protection of sensitive data. Comparable principles governing derivative actions by shareholders exist in English corporate law, and the losses to a business that result from breaches can be astronomical. For example, following a large and highly publicized data breach, the UK-based telecoms group TalkTalk warned that the cost of dealing with the breach could be up to £35 million. It is easy to see how similar claims might well be pursued by aggrieved investors in England if they feel a company hasn't done enough to safeguard what is increasingly understood to be a critical asset.

The recent publicity surrounding the breach involving the Panamanian law firm Mossack Fonseca, and the more general efforts that hackers have been exerting to target law firms, including some of the largest UK-based practices, raises the specter of negligence or breach of contract claims raised by clients and business partners against data custodians.

CONCLUDING THOUGHTS

The litigation landscape in the UK is likely to develop rapidly in the coming years as increasing numbers of lawsuits arise out of data breaches. English law is both developing new causes of action, as well as applying traditional principles in a fresh context, to provide redress for victims of data breaches, and the UK may well become an increasingly popular forum for the litigation of such disputes.

Client Update:

Florida Court Dismisses Data Breach Lawsuit for Lack of Standing

Addressing a key issue in consumer data breach class action litigation, a federal court in the Southern District of Florida has dismissed a lawsuit against a Florida hospital for lack of Article III standing because there was no allegation that the individual plaintiff's personal information had actually been misused. *See Case v. Miami Beach Healthcare Group, Ltd., et al.*, Case No. 14-24583-CIV (S.D. Fla.) (Feb. 26, 2016). This reinforces the requirement of a plaintiff's ability to plead actual harm with some specificity – a daunting task in most consumer data breach cases. Though some courts have taken a more plaintiff-friendly view of the pleading standard, Case pushes those decisions further toward the margins.

WHERE THE COURTS HAVE BEEN SO FAR

The starting point for most recent judicial discussion of the standing issue in data breach cases is the Supreme Court's 2013 decision in *Clapper v. Amnesty International USA*. There, the Court rejected a challenge by alleged victims of federal surveillance who could not plead that they were actually surveilled or injured: "[T]hreatened injury must be *certainly impending* to constitute injury in fact," the Court said, and "[a]llegations of *possible* future injury" are not sufficient. (emphasis in original). The Court acknowledged that, in some prior cases, it had upheld standing based on a "substantial risk" that the harm would occur. The Court went on to state in 2014, in *Susan B. Anthony List v. Driehaus*, that "[a]n allegation of future injury may suffice if the threatened injury is 'certainly impending,' or there is a 'substantial risk' that the harm will occur."

Many lower courts have relied on *Clapper* in dismissing data breach consumer class actions at the pleading stage, holding that the alleged theft of personal information does not, by itself, establish an imminent risk of concrete injury. Even before *Clapper*, in *Reilly v. Ceridian Corp.*, the Third Circuit held that "[i]n data breach cases where no misuse is alleged, . . . there has been no injury – indeed, no change in the status quo."

Reilly involved a security breach at a payroll processing firm. A hacker gained access to the personal information of about 27,000 of the firm's customers' employees, including their names, addresses, Social Security numbers, dates of birth and bank account information. The court held that the mere accessing of that data by a hacker, and the plaintiffs' allegations of possible future injury, were not sufficient to satisfy Article III because the alleged injury was not "certainly impending."

Last year, however, the Seventh Circuit ruled in *Remijas v. Neiman Marcus Group, LLC* that "an increased risk of future fraudulent charges and greater susceptibility to identity theft" was sufficient to confer standing at the pleading stage. The data breach that Neiman Marcus experienced potentially exposed approximately 350,000 credit card numbers. Approximately 9,200 credit cards were used fraudulently, although the victims were later reimbursed for the charges. The court declined to assume that future charges would be reimbursed, and found that, in any case, there are "identifiable costs associated with the process of sorting things out."

The *Neiman Marcus* decision went against the clear trend post-*Clapper* of dismissing data breach class actions in the absence of unreimbursed economic harm that could demonstrably be

connected to the particular breach in question. As we noted at the time, it remained an open question whether *Neiman Marcus* would in time be seen as a minority view or as a sign of reversal in the trend.

THE CASE DECISION

Case involved a data breach at a Florida hospital that allegedly exposed the names, dates of birth and/or Social Security numbers of over 85,000 of the hospitals' patients. Because the plaintiff in *Case* did not claim that her information "was actually misused, or that the unauthorized disclosure of her sensitive information caused her any type of harm, economic or otherwise," the district court last week held that she lacked standing.

The *Case* court distinguished other decisions, such as the consumer class action that followed the data breach of Target stores, on the basis that the plaintiffs in those cases alleged actual injuries, "including unlawful charges, restricted or blocked access to back accounts, inability to pay other bills and late payment charges or new card fees."

The court also rejected the plaintiff's argument that she was injured because she did not receive the full value of the services for which she paid, which purportedly included data protection services. The court concluded that the hospital's charges to the plaintiff for medical care did not "explicitly or implicitly include[] the cost of data protection."

SIGNIFICANCE FOR DATA BREACH LITIGATION

The *Case* decision joins a number of other post-*Neiman Marcus* decisions where consumer class actions following a data breach have

failed at the motion to dismiss stage. *See, e.g., In re SuperValu, Inc.*, No. 14-MD-2586, 2016 WL 81792 (D. Minn. Jan. 7, 2016); *Whalen v. Michael Stores Inc.*, No. 14-CV-7006, 2015 WL 9462108 (E.D.N.Y. Dec. 28, 2015); *Fernandez v. Leidos, Inc.*, No. 2:14-CV-02247, 2015 WL 5095893 (E.D. Cal. Aug. 28, 2015). Certain cases have gone the other way at least in part, making it important to watch for additional cases as this area of the law continues to develop. *See, e.g., In re Anthem, Inc. Data Breach Litig.*, No. 15-MD-02617, 2016 WL 589760 (N.D. Cal. Feb. 14, 2016); *Walker v. Boston Med. Ctr. Corp.*, No. SUCV20151733BLS1, 2015 WL 9946193 (Mass. Super. Nov. 20, 2015). But it seems fair to say that the directional arrow is pointing toward treating the *Neiman Marcus* approach as the minority position.

The *Case* decision underscores the importance of scrutinizing the specific allegations relevant to the issue of future harm to individual consumers – *e.g.*, what type of data is at issue, whether it is certain that a third party accessed the consumers' data, whether the data has been made available to identity thieves, whether fraudulent charges have been made and whether those charges have been reimbursed to the consumers. By rejecting the argument that a data breach means the promised services have not been delivered at full value, *Case* also rejects a theory that – if accepted – potentially could have allowed for a much more liberal approach to standing.

This client update was originally issued on February 29, 2016.

Client Update:

Data Breach Plaintiffs' Suit Reinstated; Court Holds Affected Customers Have Standing

A new decision from the Seventh Circuit Court of Appeals holds that consumers of a hacked retailer had standing to sue on the basis of the costs they incurred in responding to the breach, even if their accounts had not suffered any fraudulent charges. The Court held that even consumers that had not experienced actual identity theft had standing to sue, given the costs allegedly associated with "sorting things out" in the wake of a data breach.

The Seventh Circuit's ruling bucks a longtime trend of post-data breach consumer class actions failing at the pleading stage in the wake of the Supreme Court's 2013 decision in *Clapper v. Amnesty International*. *Clapper* held, in the context of allegations of unlawful electronic surveillance, that an imminent risk of concrete injury is required for a plaintiff to have standing to sue in federal court. Many district courts have relied on *Clapper* to grant motions to dismiss data breach class actions, holding that the mere theft of information does not establish an imminent risk of concrete injury.

THE DECISION

The new decision in *Remijas v. Neiman Marcus Group, LLC* departs from that trend, reversing the decision of the district court to toss out the suit based on *Clapper*. Neiman Marcus suffered a data breach in 2013 that potentially exposed up to 350,000 credit cards, but according to the company, only 9,200 consumers actually suffered fraudulent transactions. Neiman Marcus paid for a year of identity theft monitoring for all 350,000 accounts. Plaintiffs in *Neiman Marcus* sued on a number of theories, arguing that they had standing

because of the lost time and money spent protecting against future identity theft.

The district court held that the plaintiffs lacked standing under *Clapper* because the harm was inchoate. The Seventh Circuit held that this interpretation of *Clapper* was too broad and did not appreciate the likelihood of future harm – "the Neiman Marcus customers should not have to wait until hackers commit identity theft or credit card fraud in order to give the class standing."

IMPACT AND ANALYSIS

The *Neiman Marcus* analysis, if adopted by other courts, could give consumers standing in data breach cases because of the costs associated with protecting against identity theft and fraud. As the Seventh Circuit noted: "the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." In light of that reasoning, the Court held *Clapper's* requirement of imminent future injury satisfied.

Another significant aspect of the *Neiman Marcus* decision relates to the oft-asserted defense, in the wake of data breaches, that affected consumers' information could have been obtained from any number of hacked companies. Neiman Marcus noted the breadth of the Target hack, and asserted that Plaintiffs could not show that the breach at Neiman Marcus was the source of their problems. The Seventh Circuit held that this showing was not required: the fact that other companies might have exposed Plaintiffs' information was for defendants to prove, not for plaintiffs to allege.

Although the *Neiman Marcus* decision generally provides a boost to consumer suits, it is worth remembering that it deals only with

whether plaintiffs can survive a motion to dismiss. The Court's opinion repeatedly referenced the standard that requires courts to credit plaintiffs' allegations at this stage of the litigation, and noted all that is required to establish standing is a non-speculative assertion of injury.

Whether *Neiman Marcus* portends a paradigm shift remains to be seen. The new decision is particularly significant in light of the relatively recent decisions in the class action litigation stemming from Target's data breach. Two class actions against Target – one by consumers and one by financial institutions – survived motions to dismiss in December 2014. There, as in *Neiman Marcus*, the court found plaintiffs had standing given allegations of injury based on fraudulent charges and the time and costs involved in dealing with breach-related issues. Target ultimately settled the consumers' claims for $10 million. The financial institution class action remains pending after a proposed $19 million settlement fell apart when not enough banks signed on. Given that a circuit court has now adopted reasoning similar to the *Target* class action cases in refusing to dismiss class action claims stemming from a data breach, there is little doubt that the plaintiffs' class action bar will continue to bring post-breach damage cases.

This client update was originally issued on July 28, 2015.

Federal Legislation Update

In this section, we analyze the new federal Cybersecurity Information Sharing Act, or CISA. CISA establishes a legal safe harbor, for sharing with the government information about cybersecurity incidents, threats and defenses. The Department of Homeland Security has established an online portal to receive such reports. Homeland Security also has issued implementing regulations and guidance documents.

More recently, President Obama signed into law the Defend Trade Secrets Act, or DTSA, which will now provide private entities with a federal cause of action and civil remedies for "a trade secret that is misappropriated" – a field of civil litigation that has until now remained largely governed by state trade secret laws within state

courts. The DTSA provides powerful remedies, including ex parte seizure provisions, double damages and attorney fee shifting for willful trade secret misappropriations, in addition to more traditional damages and injunctive relief.

Client Update:

The Cybersecurity Information Sharing Act

Significant new cybersecurity legislation was signed into law by President Obama late in 2015. The Cybersecurity Information Sharing Act, or CISA ("SEE-sa") for short, is a revised version of a bill that passed the Senate last fall. Notably, CISA provides a safe harbor from liability to companies for the voluntary sharing of "cyber threat indicators" and "defense mechanisms" with the federal government. CISA is not industry-specific and thus has implications for a wide range of companies.

BASICS OF THE BILL

The premise of CISA is that we are all generally better off when companies engage in robust monitoring of cyberthreats and robust sharing of threat information. If Company A shares what it knows, the argument goes, then Company B (and Companies C and D . . .) can use that information to improve their own defenses. Sharing also may help law enforcement and other public-sector players to take action against the threat. Yet there is a perception that concerns such as confidentiality, trade secrets and privacy historically may have made companies reluctant to monitor and share.

CISA aims to break down that reluctance. Specifically, the new statute:

- Requires that the Department of Homeland Security ("DHS") establish a portal for collection of threat information, and a system for dissemination of the information to private- and public-sector entities.

- Provides that a private entity may, for cybersecurity purposes, monitor (i) information systems of its own; (ii) information systems of other private entities (upon receiving authorization and written consent); (iii) information systems of the U.S. government (upon receiving authorization and written consent); and (iv) information that is stored on, processed by, or transmitted via an information system monitored by such private entity.
- Provides that private entities may establish certain cyber defenses, such as firewalls or other intrusion prevention systems, provided the measures do not "destroy[], render[] unusable, provide[] unauthorized access to, or substantially harm[]" an information system of another (or information stored thereon) without prior consent.
- Protects private entities from liability from causes of action based on the monitoring of an information system or the sharing or receipt of threat information. CISA also guarantees the prompt dismissal of any such causes of action. To receive protection, the monitoring, sharing or receipt, must be conducted in accordance with all other requirements of CISA.

CISA includes belt-and-suspenders privacy safeguards: A private entity must remove personally identifying information about individuals before sharing with DHS, and DHS must confirm removal of all such information before making any subsequent disclosure. Information shared in accordance with CISA is exempt from Freedom of Information Act requests. CISA expressly creates no "duty to share a cyber threat indicator or defensive measure," and no "duty to warn or act based on the receipt" of the same.

Important details remain to be filled in. Within 60 days after enactment, the Director of National Intelligence, in consultation

with the heads of the appropriate federal agencies, must submit to Congress procedures for facilitating and promoting the sharing of information by the federal government. DHS and the Department of Justice ("DOJ") must within 60 days of enactment jointly develop (i) interim policies and procedures relating to the receipt of cyber threat indicators and defensive measures by the federal government and (ii) interim guidelines relating to privacy and civil liberties; each of these must be finalized within 180 days of enactment. Within 90 days after enactment, DHS, in coordination with other relevant agencies, must develop and implement the portal for accepting cyber threat indicators and defensive measures.

CONSIDERATIONS FOR COMPANIES

Over time, CISA likely will have many implications for organizations of all kinds. Here are a few initial thoughts on its practical effects.

Adjustments to Policies and Procedures

Companies likely will want to build at least three new mechanisms into their cybersecurity policies and procedures: (i) a mechanism for considering when to report a threat to the DHS portal; the statute provides no specific guidance on what constitutes a reportable event; (ii) a mechanism for actually submitting information to the portal with care - the safe harbor does not apply if, for example, a company fails to strip out personally identifiable information; (iii) and a mechanism for acting on threat information that DHS shares. CISA itself imposes no substantive standards for cybersecurity, and (as noted) imposes no duty to act on information shared by DHS. But neither does it bar courts, regulators and enforcement agencies from seeking to impose liability on companies for their cybersecurity failings. The CISA safe harbor applies only to the acts of monitoring and sharing.

Disclosure Issues

Longstanding SEC guidance calls for public companies to disclose "cybersecurity risks and cyber incidents," as well as the costs and other consequences of those risks and incidents, to their investors to the extent such disclosure would be material. No specific level of detail is mandated, but the SEC cautions that "generic 'boilerplate' disclosure" is to be avoided. Companies will want to keep an eye on any evolving interplay between this disclosure obligation and their CISA disclosures. Depending upon the particular facts and circumstances, disclosure of a risk to the DHS portal could be seen as an indicator of materiality necessitating disclosure of the same risk to the market.

Vendor Relationships

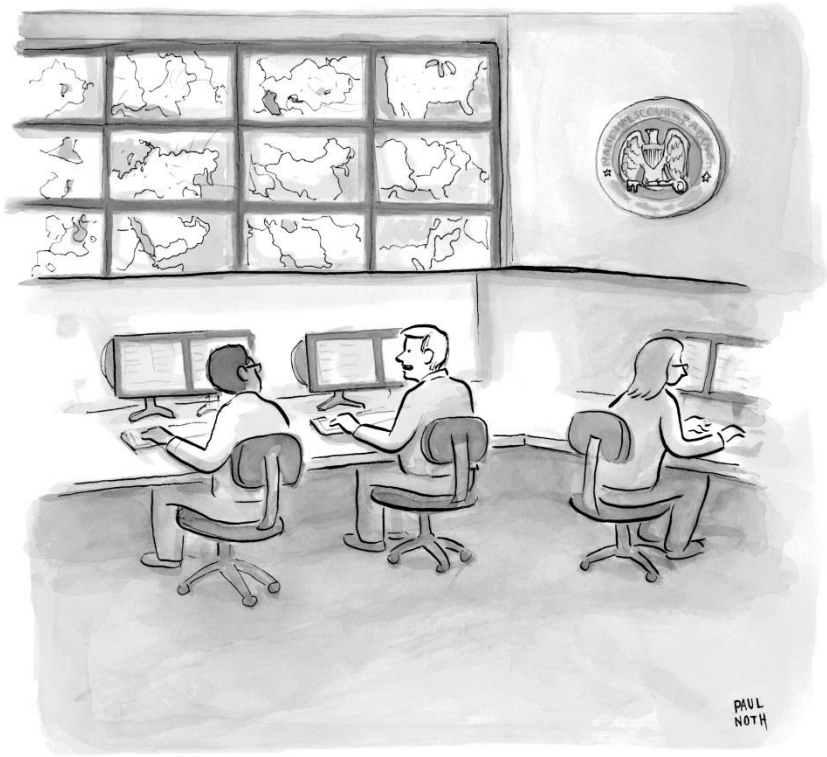
Companies also will want to monitor how CISA affects their relationships with key vendors. For example, companies that outsource the storage of sensitive information might inquire with vendors about their own CISA compliance practices. In some cases, it might be appropriate to contractually mandate that vendors participate in CISA information sharing, or that the same information a vendor shares with DHS must also be shared with the contract counterparty.

Privacy

Companies should pay particular attention to the DOJ/DHS privacy procedures as they are developed and promulgated, and should consider taking advantage of any opportunity that is provided to comment on such procedures.

This client update was originally issued on January 6, 2016.

Cyber Threat Trends



"After we read every e-mail ever written, I'm gonna start on that new Dan Brown novel."

In this section we take a look at current threat trends that have cropped up in a variety of industries and contexts. Malvertising – or the use of online ads as a means to deploy malware and infect a victim's computer, is increasingly a threat vector to be wary of, and

may pose litigation risks to those in the advertising sector. Ransomware, on the other hand, is malware that locks users out of their own electronic data. Both appear to be on the rise, and ransomware, in particular, is increasingly threatening large institutions.

In these two articles, we describe these threats and explore practical ways to prepare for and mitigate their effects.

Malvertising: When Advertisements Strike

Malvertising is the injection of malware onto a user's computer through online advertising. It is on the rise. Malvertising is particularly threatening because, unlike other cyberthreats that savvy Internet users can easily avoid (sketchy email solicitations, dodgy links and attachments), these malicious ads appear to the user as safe and legitimate.

This article discusses how cybercriminals exploit the mechanics of the online advertising ecosystem, followed by a discussion of legal considerations for companies operating in this rapidly evolving space.

THE TECHNICAL 411

Let's start by imagining how a typical advertising-supported website looks to the user. There's a content window showing, say, video clips or news articles from the site publisher. There's also an advertising window, showing marketing messages. The two windows may look to the average user like an integrated whole.

In fact, only the content window is under the site publisher's technical control. Likely as not, the "feed" to the advertising window does not go through the publisher – but, rather, through a variety of ad networks, ad exchanges, resellers and other third parties. On average, each online ad goes through five to six such intermediary companies before it is displayed to the end user.[1]

---

[1] STAFF OF S. COMM. ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS, 113TH CONG., REP. ON ONLINE

Like a highway with multiple on-ramps, the online advertising system offers various points of entry for criminals to exploit. Cybercriminals may place malvertising by creating fictitious identities and "fronts", *i.e.*, by purporting to be legitimate advertisers or intermediary companies. The bad guys also may hack into legitimate advertisers or ad companies, stealing employee credentials and using those to replace legitimate ads with malvertising.

Once in the system, malvertising is notoriously difficult to track, and cybercriminals continue to develop clever strategies to avoid detection, such as by removing the malware from the host ad after a few hours, by only serving the malware to every tenth or twentieth user who views the ad, or by configuring the malvertising so that it only begins to function days after the ad has been approved to run.

The malware implanted via malvertising likewise may function in various ways: for example, to capture users' personal information, to turn users' devices into bots (in order, *e.g.*, to distribute DDos attacks), or to distribute ransomware. The goal of the cybercriminals may be identity theft, account takeover, corporate espionage, or financial fraud. Malware may also be used to inflate and distort click-through rates or other measures that affect the cost of advertising.

Malvertising attacks have increased dramatically in recent years. Google reports that it disabled more than 780 million malicious ads in 2015, an almost 50% increase from 2014.[2] The cybersecurity firm

---

ADVERTISING AND HIDDEN HAZARDS TO CONSUMER SECURITY AND DATA PRIVACY 14 (Comm. Print 2014).

[2] *See* Paul Sawers, *Google blocked 780 million 'bad ads' in 2015, up 50% from 2014*, VENTURE BEAT (June 20, 2016),

Cyphort Labs estimates that 2016 will see a 131% increase in malvertising attacks over 2014 levels.[3]

Malvertising attacks have been launched through popular mainstream websites, including those published by *The New York Times*, the BBC, MSN and AOL.[4] In the past two months, for example, the gossip website PerezHilton.com, which has over 500,000 daily visitors, was used to host two separate malvertising campaigns, potentially affecting millions of visitors.[5]

LEGAL CONSIDERATIONS

It is early days in the development of malvertising as a legal issue. We are not aware of any civil lawsuits arising out of malvertising to date. Nor are we aware of any investigations or enforcement actions relating to malvertising by any of the many government agencies that police the civil cyber beat.

One notable criminal prosecution involved an Estonian crime syndicate – known as Rove Digital – that altered DNS settings on computers in order to hijack their ad clicks. Dubbed the "doomsday virus" by the media for the potential risk of catastrophic internet

---

http://venturebeat.com/2016/01/21/google-blocked-780-million-bad-ads-in-2015-up-50-from-2014/.

3 *See* Aldrin Brown, *'Malvertising' Attacks on Record Pace*, MSPMENTOR (May 12, 2016), http://mspmentor.net/msp-mentor/malvertising-attacks-record-pace.

4 *See*, Dan Goodin, *Big-name sites hit by rash of malicious ads spreading crypto ransomware*, ARS TECHNICA (Mar. 15, 2016), http://arstechnica.com/security/2016/03/big-name-sites-hit-by-rash-of-malicious-ads-spreading-crypto-ransomware/.

5 *See*, Jane McCallion, *Perez Hilton malware strikes millions of users*, ITPRO (May 12, 2016), http://www.itpro.co.uk/malware/26525/perez-hilton-malware-strikes-millions-of-users.

outages (which didn't materialize) the virus ultimately netted Rove Digital $14 million, according to the FBI. Vladimir Tsastsin, a key figure in the syndicate, was sentenced to seven years' imprisonment by a New York Federal Court in April 2016. [6]

Although it is early days, it is not too early for companies involved in the online advertising world to weigh a number of considerations as they consider how to protect themselves and their customers:

- **Warranties and Indemnification**: Through contracts, parties may seek to protect themselves from any liability that might stem from malvertising campaigns. For example, Google's DoubleClick Ad Exchange, a marketplace for the buying and selling of ad space, requires parties placing ads through its service to warranty that the ads provided will not contain "malware, spyware or any other malicious code."[7] Similarly, Condé Nast's contracts with advertisers and ad agencies include a warranty to Condé Nast that the ads will not "cause the download or delivery of any software application, executable code, malware, any virus or malicious or social engineering (*e.g.*, phishing, etc.) code or features . . ." as well as a warranty that the ads will not be "harmful to any person, corporation or other entity."[8]

---

[6] Debevoise Partner James Pastore, formerly an Assistant U.S. Attorney in the Southern District of New York, was part of the prosecution team that obtained indictment and extradition of Mr. Tsastsin.

[7] Google DoubleClick Ad Exchange Buyer Terms, DOUBLECLICK AD EXCHANGE BY GOOGLE, https://www.google.com/doubleclick/adxbuyer/terms.html (last visited June 20, 2016).

[8] Epicurious Contract and Regulations, CONDÉ NAST, http://www.condenast.com/brands/epicurious/media-kit/contracts-and-regulations (last visited June 20, 2016).

Indemnification is another contractual option. The same Condé Nast contract, for example, requires that advertisers or ad agencies "defend, indemnify and hold harmless" the publisher against any liability or damages arising from "the linkage of any advertisement . . . to other material" or a "breach or alleged breach" of any warranties, including the warranty, referenced above, that the ad will not cause the delivery of malware.

- **Due Diligence**: There is much to be said for investigating one's counterparties. Due diligence might reveal that a particular exchange has been known to serve up malvertising, or even provide indicia that the counterparty is a front for cybercriminals. As part of continuing diligence efforts once a contract is entered into, parties might want to request audit rights in order to evaluate the systems in place for identification and removal of malvertising.
- **Evolving best practices**: In a world where "reasonable security" is increasingly cited as a legal standard, companies will be well advised to keep abreast of the latest technical and commercial measures to prevent malvertising.[9] For example, publishers may not fully control the flow of ads to that separate advertising window on their sites. But they may have the ability to set up a checkpoint – perhaps through a security vendor – that allows ads being served by third parties to be scanned for malware before they reach a site's users. The adoption of such tools may be increasingly favored as their technical sophistication and effectiveness increases. Similarly, the Online Trust Alliance has

[9] *See, e.g.*, Cal. Civ. Code § 1798.81.5 (West 2016) (requiring businesses that collect personal information to use "reasonable security procedures and practices"); *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3rd Cir. 2015) (discussing the requirement of "reasonable" cybersecurity measures).

promulgated an "Advertiser & Customer Risk Evaluation Framework," as an effort to encourage best practices.[10]

Malvertising is not going away anytime soon. Just as technological responses to the threat are continuing to develop, the legal implications remain in flux. Companies that operate in the online ad arena must remain alert to changes and be prepared to respond accordingly.

[10] Advertiser & Customer Risk Evaluation Framework, ONLINE TRUST ALLIANCE, https://otalliance.org/system/files/files/best-practices/documents/advertising_risk_evaluation_framework.pdf (last visited June 20, 2016).

Client Update:

New Federal Ransomware Guidance

The U.S. Department of Health and Human Services (HHS) has just issued significant new guidance on ransomware. The guidance makes clear that entities subject to the data security provisions of federal healthcare law now have specific responsibilities both to guard against ransomware attacks and – in a departure from existing breach notification requirements – to report such attacks when they happen. Given that ransomware attacks are spiking sharply across corporate America, the HHS guidance is instructive not just for healthcare entities but for enterprises in all sectors.

RANSOMWARE FAQ

What is ransomware? Ransomware is a form of attack where the hacker does not steal your files, but encrypts them so you cannot access them. Then the hacker offers to sell you the encryption key, typically payable in the online currency Bitcoin. The usual demand comes with a deadline – after which time, the hacker threatens, the key will be discarded and your files will remain forever inaccessible.

If a low-tech metaphor helps: Think of the ransomware attacker as a sort of reverse "burglar," who doesn't break in to your house, but locks you out of it and demands payment to let you back in.

Why is the government taking action? Ransomware attacks are way, way up. There have been an estimated 4,000 attacks a day in 2016 to date, representing a 300% increase over 2015. Historically, ransomware attacks tended to be petty crimes directed at individuals and mom-and-pop organizations. But these attacks are now being directed more often, and with more success, at larger enterprises.

How do ransomware attacks happen? Ransomware gets onto an enterprise's system like any other kind of malware. "Phishing" attacks, where users unwittingly click on a malware-laden link or attachment in a seemingly innocent email, are a common vector. Hackers also may steal system credentials or exploit software vulnerabilities to install ransomware.

Hackers who successfully launch their ransomware then typically post threatening messages on the screens of users at the victim entity. In one example cited by the Department of Justice, the hacker asserted that the users themselves had engaged in illegal activity and must pay a "fine." In another, the hacker stated that a ransom must be paid within a certain time period or "all your files will be permanently encrypted and nobody will be able to recover them."

Do victims pay the ransom? Often, yes. No comprehensive metrics are publicly available, but at least one study reports a 40% pay-up rate. It is a matter of public record that, earlier this year, Hollywood Presbyterian Hospital in Los Angeles paid its hacker 40 bitcoin, or about $17,000. Even law enforcement is not immune; a Massachusetts police department has admitted that it paid a ransom to retrieve its work files.

Why pay? In that memorable line from the movie "Argo," payment of the ransom may be the victim's "best bad option." Enterprises face a tough choice when the encryption is not defeatable and the padlocked files are business-critical. (How long can a modern hospital, for example, be offline before devastating consequences occur?) Compounding these difficulties, law enforcement agencies generally cannot find the cybercriminal fast enough to satisfy business demands, if they can find the criminal at all. (He may be

overseas.) Moreover, the bad guys frequently set the ransom at or about nuisance-value levels. And at least until now, there has been no disclosure requirement.

Add it all up, and payment of the ransom – however frustrating – can seem to be a reasonable cost-benefit calculation. As one FBI official has said, "To be honest, we often advise people just to pay the ransom." (To be clear, the FBI's official policy is that victims should contact law enforcement. The new HHS guidance calls for reporting of ransomware attacks to the local FBI or Secret Service field office.)

Do hackers who are paid actually supply the encryption key? Often, yes. Again, metrics are hard to come by – but an FBI source has said that typically, "You do get your access back." Some ransomware attackers even ask you to rate them, like an Uber driver, so they can advertise to future victims that they have a track record of supplying the encryption key once paid.

There is not always honor among thieves. Published reports indicate that just this spring, a hospital in Wichita paid a ransom – but in return got only partial access to its files, together with a demand for an additional payment.

Isn't ransomware a crime? You bet. At a minimum, ransomware schemes run afoul of the federal computer crime statute, 18 U.S.C. § 1030, and particularly subsection (a)(7), which forbids hacking intended to extort something of value from the victim.

Up to now, what have been the legal obligations of ransomware victims? Few, if any:

- Most states have laws requiring disclosure of data breaches, but these laws ordinarily kick in only when data containing personal information is exposed or stolen – not when the data is simply made inaccessible.
- In specific situations, companies may be contractually required to give notice to their counterparties of certain cybersecurity events, including ransomware attacks.
- The U.S. Federal Trade Commission generally takes the position that maintaining poor cybersecurity can be an unfair business practice under Section 5 of the FTC Act. But the FTC has not yet applied this theory to try and hold a ransomware victim culpable. Informally, the FTC has indicated that it is focused on hacking cases that cause large-scale consumer impact – a description that does not fit the classic historical ransomware case, but might fit the emerging breed of enterprise-level ransomware attack.

THE NEW HHS GUIDANCE

The federal Health Insurance Portability and Accountability Act (HIPAA), has long imposed cybersecurity standards on covered entities and their business associates via the HIPAA Security Rule. The new July 11 guidance makes clear that HIPAA's cybersecurity standards will now be construed to apply to ransomware.

First, the guidance makes clear that those subject to HIPAA must "implement policies and procedures that can assist an entity in responding to and recovering from a ransomware attack."

These policies and procedures should include "maintaining frequent backups" and conducting periodic "test restorations," *i.e.*, measuring the enterprise's ability to actually function from backups if a ransomware attack were to limit access to regular systems. HHS also counsels organizations to "consider maintaining backups offline

and unavailable from their networks." This is because of the propensity of ransomware attackers to target the backup files themselves – in effect, padlocking the garage door as well as the front door.

The HHS guidance specifies that all this is part of the larger obligation, under the Security Rule, to maintain a "data backup plan" that includes provisions for disaster recovery planning, emergency operations, analyzing the criticality of applications and data, and periodically testing contingency plans.

The long-standing HIPAA mandate to maintain "security incident procedures" will now be construed to require processes that will allow an organization to detect, analyze, contain, eradicate and recover from a ransomware attack. Ransomware attacks are now explicitly defined as "security incidents" triggering the obligation to deploy these procedures. Likewise, the long-standing requirement that a covered organization's workforce must receive appropriate security training now includes a requirement that the workforce be trained in how to detect and report malware so as to help ward off ransomware attacks.

Second, breach notification obligations may well now kick in under HIPAA even if other notification triggers, such as the states' notification statutes, are not implicated. The guidance is quite clear that "the presence of ransomware . . . is a security incident" for purposes of the Security Rule, and qualifies as a breach because unwanted encryption of personal health information (PHI) by the ransomware attacker amounts to "acquisition" of that data by the attacker within the meaning of the Rule. Until now, ransomware and the payment of a ransom typically did not trigger breach disclosure obligations, and the guidance marks a significant

departure from prior practice which may be a harbinger of change in other sectors.

Whether HIPAA disclosure procedures must be followed will be a case specific determination. But the general rule is that disclosure must occur unless the enterprise can show a "low probability" that PHI has been compromised. Traditional factors in this analysis include the nature and extent of PHI involved, whether the PHI was actually acquired or viewed, and the extent of risk mitigation. Under the new guidance, a "high risk of unavailability of the data, or high risk to the integrity of the data" is to be considered an indicator of compromise.

If the data encrypted by the ransomware attacker was previously encrypted by the data holder, that may cut against disclosure being required. Even then, though, the determination is case-specific – for example, a ransomware attack on an encrypted laptop could still result in a breach, for purposes of the Security Rule, if "the file containing the PHI was decrypted and thus 'unsecured PHI' at the point in time that the ransomware accessed the file."

WHAT'S AN ENTERPRISE TO DO?

Organizations subject to HIPAA of course must sit up and take notice of the new HHS requirements, and review their training programs, technical protections, backup systems and incident response protocols for compliance with the new guidance.

Organizations in all sectors of the economy can learn from the HHS requirements, however, and by doing so can reduce both their business and legal risks associated with ransomware. For it seems safe to say that once a major agency like HHS defines an obligation

to detect, prevent, combat and report ransomware attacks, then other legal authorities may converge around similar views.

The Department of Justice, the Secret Service and other federal agencies have joined with HHS to issue best-practices guidance for all enterprises. The interagency guidance is not limited to healthcare entities, and it closely resembles the new HHS mandates for HIPAA-covered organizations.

Also part of the chorus is the federal Computer Emergency Response Team (US-CERT), a technical expert entity based at Carnegie-Mellon University that recently issued its own guide, Ransomware and Recent Variants. CERT's guidance on risk mitigation closely resembles the interagency recommendations and HHS mandates.

Ransomware thus joins the growing list of cybersecurity threats that, under the law, potential victims are well advised to take specific measures to prevent, detect and mitigate.

This client update was originally issued on July 19, 2016.

Client Update:

Cyber Crime Gets Back to Basics: Two New Examples of How Cyber Criminals Are Monetizing Stolen Information Through Well-Worn Criminal Strategies, and How You Can Respond

BACKGROUND

News of how cyber criminals have been able to monetize the information they steal typically has been harder to come by, and less scary, than news of data breaches themselves. This week brought two counter-examples, in which cyber criminals were able to grab over $75 million in ill-gotten gains.

The Schemes and How They Worked

Insider Trading. On August 11, 2015, the Department of Justice and the SEC jointly announced charges against a criminal group who combined hacking and insider trading in a remarkably simple way: by gaining access to earnings announcements on wire services' computer systems before they were released to the market.

News releases announcing earnings reports are typically released simultaneously by various wire services shortly after the market close. But for practical reasons, the information is uploaded to the wire services' computers earlier in the day. The criminals here used SQL injection, credential theft and other familiar hacking techniques to get access to the earnings reports before they were released publicly. Then they traded on the information, often shorting a stock just before negative news hit the street. Authorities estimated that this scheme netted the attackers more than $30 million over several years.

Impersonating the Boss. Separately, a California maker of network equipment, Ubiquiti, reported in its securities filings that it was the victim of an even more damaging cyber heist, through an even simpler means. The attackers spoofed emails that appeared to be from company executives, directing lower level employees to make funds transfers to overseas accounts, purportedly as payments to suppliers, something the company often does in the ordinary course. But these transfers were, of course, to accounts controlled by the hackers. The company reported that as a result of the spoofed emails, it transferred approximately **$46.7** million to the thieves' accounts. The company reported that, working with law enforcement and counsel, it has recovered approximately $8.1 million of the transferred funds, and believes it will recover more from funds that have been frozen in foreign accounts.

Lessons For Other Companies

First, encourage your IT security team to spend some time thinking like a common criminal. How would you attack your business, and what would be the weak links in your human defenses, business processes and controls against scams or frauds that come through your computer systems? Perhaps your existing program of penetration testing includes questions like this; if not, consider expanding the program.

Like the two examples discussed above, many of the most damaging cyber attacks are not necessarily innovative or novel, and exploit human relationship dynamics rather than technological security gaps. Where you find potential weak points, build in redundancy to your systems and controls. *And never allow funds transfers – particularly not international ones – through email alone.*

Second, if you are the victim of an attack, think seriously about reaching out to and cooperating with law enforcement. Corporate America has, with good reason, been concerned that civil regulators like the U.S. Federal Trade Commission will come after the victims of a data breach on the theory that their security was so inadequate as to be unlawful. But notably, in announcing the insider trading charges, the government did make any suggestion that the newswires had inadequate security defenses. Quite the contrary, the government focused on the "sophisticated" nature of the cyber intrusions and expressly thanked the newswires, which "cooperated with law enforcement over the course of the investigation."

This statement dovetails with a recent announcement by the FTC that, in assessing the reasonableness of a company's cyber defenses, it will consider "whether [a victim] cooperated with criminal and other law enforcement agencies in their efforts to apprehend the people responsible for the intrusion."[1] Indeed, the FTC noted that "a company that has reported a breach to the appropriate law enforcers and cooperated with them has taken an important step to reduce the harm from the breach," and one that will cause the FTC to "view that company more favorably than a company that hasn't cooperated."

Both of these statements – from law enforcement and the FTC – reflect an effort to assure wary victims that regulators will not follow a "no good deed goes unpunished" policy, and that, as in other areas of enforcement actions, genuine cooperation will be rewarded. It remains to be seen how much credit cooperation will earn

---

1 *See* "If the FTC Comes to Call," FTC Business Blog, available at https://www.ftc.gov/news-events/blogs/business-blog/2015/05/if-ftc-comes-call (last visited August 14, 2015).

companies, particularly where the breach was a result of obvious security failures, but the potential benefits of cooperation bear serious consideration in every case.

This client update was originally issued on August 17, 2015.

Insuring for Cyber Risk

"I feel like my best passwords are already behind me."

It is now cliché that there are only two kinds of businesses: those that have been hacked, and those that just don't know it yet. No set of cybersecurity measures – even the very best – can be sold as a panacea. For many companies, when an emergency arises, breaking the glass on insurance coverage is a critical part of cyber risk management strategy.

COVERAGE LITIGATION SO FAR

Most of the legal attention around insurance coverage for data breach costs has thus far centered around whether traditional Commercial General Liability ("CGL") policies provide coverage for some losses resulting from a data breach. CGL Carriers have been updating their policy forms to expressly exclude breach-related losses from coverage, and have fought, tooth and nail, claims of "personal and advertising injury" arising out of electronic publication of personal information. The interpretation of CGL policies in these disputes has been a game of linguistic gymnastics, turning on policy-specific questions such as whether data collection and storage could constitute "publication"[1]; whether unrecovered data tapes could constitute "publication"[2]; whether mere exposure of private data on the web over time, without any proof of actual access, could satisfy the "publication" requirement[3]; or whether the "publication" must be done by the insured itself, as opposed to hackers.[4]

The 7th Circuit's *Defender* case, as well as the similarly-decided *Aspen Way* out of the District Court of Montana, both from late 2015, are discussed in the following client update.[5] These cases are the continuation of a clear trend: notwithstanding the recent *Recall Total Information Management* policyholder win – suggesting a

---

1 *Defender Security Co. v. First Mercury Ins. Co.*, 1:13-CV-00245 at 5 (S.D. Ind. 2015).

2 *Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co.*, 83 A.3d 664, 672 (Con. App. Ct. 2015).

3 *Traveller's Indem. Co. of Am. v. Portal Healthcare Solutions, LLC.*, 35 F.Supp.3d 765, 771 (E.D. Va. 2014) *aff'd* 2016 WL 1399517 at *2.

4 *Zurich Am. Ins. v. Sony Corp. of Am.*, 2014 WL 3253541 (N.Y. Sup. 2014) (Trial Order).

5 *Defender*, *supra* n1; *Am. Econ. Ins. Co. v. Aspen Way Enterprises*, No. 14-cv-09 (D. Mont. 2015).

glimmer of coverage, at least in the 4th Circuit – companies seeking to insure their cyber risk must increasingly turn to standalone cyber liability insurance.[6]

THE BASICS OF CYBER INSURANCE

Cyber insurance is explicitly designed to cover privacy and/or security events, but the coverage components vary by carrier and policy form. The immediate costs associated with a data breach fall under the first rubric of "event management" coverage, or "first party" claims: forensic investigation to determine the fact and scope of the breach, as well as remedial steps; appointment of breach counsel and public relations firm; breach notification to affected third parties; and credit/identity theft monitoring services.

Any significant breach will also attract lawsuits, including the promise of attorneys' fees and discovery, as well as, potentially, civil judgments and settlements. Cyber "liability" coverage will respond to some subset of these "third party" claims. Some carriers may offer the chance to extend this coverage to include costs of responding to regulatory inquiries, as well as payment of any associated fines and penalties. Even more specific to data breaches, liability coverage might extend to contractual fines pursuant to agreements with credit card issuers for failure to comply with the payment card industry standards (PCI DSS).

While some combination of these two categories is the staple of most cyber policies, many insureds seek additional coverage for "business interruption" (sometimes "network interruption"), to insure for the lost profit and/or marginally increased operating expenses to get back up and running. This coverage is relatively new

---

6 *Recall*, *supra* n2.

and may be especially attractive to technology-dependent firms who do not hold vast amounts of sensitive payment card information or personal health information data, such as energy or infrastructure companies. Finally, insureds can seek coverage for "cyber extortion" or "ransomware" attempts, referring to threats to harm (or continue harming) a firm if payment demands are not met.

NAVIGATING NEW EXCLUSIONS

Layered on top of this is the added complexity of coverage exclusions. These are varied, but some of the key exclusions include "physical damage" or "bodily injury" (data is not considered tangible property); loss of company funds (normally covered under a crime policy, but increasingly at risk in light of the recent SWIFT network hacks); intellectual property; so-called "acts of war" or "terrorism"; and losses due to third–party acts or omissions.

Due to the relative immaturity of the market, there has been a dearth of coverage litigation over the scope and meaning of these exclusions in cyber insurance policies – that is, while parties dispute coverage every day, these have not percolated up to the courts. However, in one recent case, a carrier sought to deny coverage where the policyholder "failed to follow minimum required [contractual cybersecurity] practices," including "continuous implementation" of security procedures and controls listed in the insurance application. The carrier argued that the policyholder's failure to replace factory default settings and to ensure secure configuration of its systems allowed it to deny coverage. The carrier did not allege that its insured acted willfully, that it acted recklessly, or even that it was

grossly negligent. That case (*Cottage Health*, 2015) was dismissed without prejudice and sent to arbitration.[7]

In the first case we've found that actually interprets a cyber insurance policy, the District Court of Arizona ruled in favor of a Chubb affiliate in the *PF Chang's* coverage litigation.[8] While Chubb had reimbursed PF Chang's for $1.7M in breach-related claims, it resisted a claim for an additional $2M in fees and assessments by the credit card companies who had eaten the costs of fraudulent transactions and sought reimbursement from PF Chang's.[9] Finding that the policy did not provide coverage for contractual fees imposed by the card brands, the court relied on a technical reading of the policy, much in the vein of the CGL coverage cases.[10] However, the dispute might have been avoided if PF Chang's had fully understood this gap in its coverage in the first place: as PF Chang's described in their own summary judgment briefing, no Chubb policy to this day explicitly provides coverage for PCI-related contractual liabilities.[11]

CONCLUSIONS

Data breach-related costs can be far-reaching, and in this way *PF Chang's* is a cautionary tale for companies seeking to proactively "do the right thing" and manage their risk with standalone cyber coverage: as with any insurance, would-be policyholders need to know exactly what they are buying, and what risks they are willing

---

7 *Columbia Cas. Co. v. Cottage Health Sys.*, No. CV 15-0432 (C.D. Cal. 2015).

8 *PF Chang's China Bistro, Inc. v. Fed. Ins. Co.*, No. CV-15-01322-PHX-SMM (D. Ariz. 2016) (Order granting Summary Judgment).

9 *Id.* at 3.

10 *Id.* at 6.

11 Pl.'s Resp. Op. Def.'s Mot. Summ. J. 3.

to bear on their own. Once coverage is in place, companies should make sure their information security and technology teams stay up to speed on the policy and how it works, so that their incident response planning efforts are tailored to get the most out of the policy.

Client Update:

No Coverage Under Commercial General Liability Policies in Recent Data Privacy Suits

Two federal courts recently held that, under commercial general liability ("CGL") policies, insurance companies did not owe policyholders a duty to defend against consumer suits alleging electronic violations of privacy. Although specific to the facts and policies at issue, the decisions highlight the uncertainty in relying on traditional CGL policies for data privacy and breach coverage. The decisions also highlight the need for companies, their risk managers, insurance brokers and counsel to consider: Should a company have coverage specific to the privacy and cyber space, or is CGL coverage sufficient notwithstanding court decisions like these? If privacy- and cyber-specific coverage is desirable, what kind, and in what amounts?

WHAT HAPPENED?

Defender Security Company, a home security systems provider, allegedly recorded and stored all incoming and outbound phone conversations without notice or consent. Defender was hit with a state court class action in California, asserting violations of the California Penal Code. Sections 632 and 632.7 of the Code make it unlawful to record telephone and cellular communications without consent.

Aspen Way Enterprises, a franchisee of the Aaron's rent-to-own business, allegedly installed spy software on laptops that it leased to customers. The software allegedly allowed Aspen Way to access personal data such as images taken from webcams, keystrokes and screenshots. A federal class action filed on behalf of Aspen Way customers asserted claims under the Electronic Communications Privacy Act, 18 U.S.C. § 2511, and a common-law invasion of privacy

claim. The State of Washington also sued Aspen Way, asserting violations of state consumer protection and spyware laws.

THE COURT RULINGS: CGL COVERAGE DOES NOT APPLY

Defender and Aspen Way each sought coverage for these suits from various insurers under CGL policies. The insurers denied coverage.

Defender sought a declaratory judgment that its insurer owed it a duty to defend. Defender's insurer prevailed on a motion to dismiss in the trial court; that dismissal has just been affirmed by the U.S. Court of Appeals for the Seventh Circuit.

Aspen Way's insurers sued in separate actions seeking declaratory judgments that they did not owe a duty to defend the company. The U.S. District Court for the District of Montana ruled in favor of the insurance companies.

Both Defender and Aspen Way relied on policy provisions that provided for defense against suits alleging "personal or advertising injuries." Critically, the policies defined such injuries in part as those arising out of "oral or written ***publication*** of material that violates a person's right of privacy." (emphasis added)

With respect to Defender, the Seventh Circuit held that the mere recording and storage of information could not reasonably be construed as "publication." The carriers therefore did not owe a duty to defend.

With respect to Aspen Way, the district court determined that the Washington State suit did not allege facts amounting to publication of information, but that some claims in the underlying consumer

class action did sufficiently allege publication and therefore triggered possible coverage. This included transmission of captured customer data to the software developer and to Aspen Way. Even with such publication, however, the court ruled that Aspen Way's insurers did not owe a duty to defend given exclusions in the policies denying coverage for actions that may have violated statutes governing the recording and distribution of information. The district court concluded that the exclusions applied here because Aspen Way may have violated the Electronic Communications Privacy Act, 18 U.S.C. § 2511, when customers' personal information was captured and transmitted without their knowledge. The court also concluded that one of the insurance policies was not triggered because it expired prior to the alleged misconduct.

These decisions resonate with last year's decision by a New York trial court in the coverage dispute between Sony and its insurer regarding data breach claims arising from the 2011 cyberattack on Playstation. There too, the court concluded that the "publication" provision of a CGL policy could not be extended to cover cyber claims. The dispute was resolved by the parties before disposition of Sony's appeal.

WHAT NEXT?

In each of the Defender, Aspen Way and Sony matters, the courts declined to construe older CGL policies to cover privacy and cyber risks, at least where "publication" was the asserted basis for coverage. Although the outcomes of such cases necessarily hinge on the particular facts and policies at issue, the decisions underscore that relying on traditional CGL policies to cover privacy and cyber risks remains far from certain. Meanwhile, new CGL policies may expressly exclude privacy and cyber risks. Companies thus should

assess their privacy and cyber exposure, and consider the desirability of policies that expressly cover these risks.

Because actuarial data relating to data privacy issues and security breaches remains limited, it is difficult for underwriters to quantify risks. Insurers writing this coverage will rely on qualitative assessments of applicants' risk profiles. They also will look at how well a company can document its risk management procedures and risk culture. Companies considering or seeking such coverage will do best in the underwriting process if they understand and can articulate their risk management posture. A company's ticklist might include:

- Understanding the types of data collected and stored by the company;
- Assessing the volume and location of records that contain personally identifiable information or other sensitive confidential information;
- Preparing, testing and regularly updating an incident response plan for handling any actual breach, whether caused by an external hacker or internal missteps;
- Carefully measuring and documenting the company's privacy and cybersecurity posture in light of recognized benchmarks such as the Framework issued by the National Institute of Standards and Technology;
- Building the internal team and the roster of outside advisors (*e.g.*, cyberforensics consultants, crisis management firms and, yes, lawyers) necessary to assess and constantly improve the company's cybersecurity posture; and
- Ensuring that any outside vendors who have access to the company's network, or to whom the company outsources

sensitive data, are contractually bound to – and do – also follow robust security and privacy practices.

The decisions are *Defender Security Company v. First Mercury Insurance Company*, No. 1:13-cv-00245 (7th Cir. Sept. 29, 2015) and *American Economy Insurance Company v. Aspen Way Enterprises*, No. 14-cv-09 (D. Mont. Sept. 25, 2015).

This client update was originally issued on October 13, 2015.

Contributors

JEREMY FEIGELSON

Jeremy Feigelson, a litigation partner, leads the firm's Cybersecurity & Data Privacy practice and is a member of the firm's Intellectual Property and Media Group. He frequently represents clients in litigations and government investigations that involve the Internet and new technologies. His practice includes litigation and counseling on cybersecurity, data privacy, trademark, false advertising, copyright, and defamation matters. Mr. Feigelson has a broad and active practice in financial services matters, including securities litigation, investment management disputes and counseling of fund boards, the conduct of internal reviews, defense of government investigations, and complex commercial litigation.

DAVID A. O'NEIL

David A. O'Neil is a litigation partner and member of the firm's White Collar & Regulatory Defense Group. His practice focuses on white collar criminal defense, internal investigations, privacy and cyber security, congressional investigations, and AML/sanctions enforcement defense. Prior to joining the firm in 2015, Mr. O'Neil served for eight years in prominent positions within the Department of Justice, most recently in the Criminal Division where he was responsible for supervising more than 600 attorneys investigating and prosecuting the full range of federal crimes, including corporate malfeasance, cybercrime, fraud offenses and money laundering. Mr. O'Neil began his career as a federal prosecutor in the U.S. Attorney's Office for the Southern District of New York.

LUKE DEMBOSKY

Luke Dembosky is a litigation partner based in the firm's Washington, D.C. office and is a member of the Cybersecurity & Data Privacy practice and White Collar & Regulatory Defense Group. His practice focuses on cybersecurity incident preparation and emergency response, related civil litigation and regulatory defense, as well as national security issues. Prior to joining the firm in 2016, Mr. Dembosky served as Deputy Assistant Attorney General for National Security in the National Security Division of the U.S. Department of Justice and was the highest-ranking official at the Department of Justice focused primarily on cyber investigations and prosecutions. He previously served as Deputy Chief for Litigation in the Computer Crime and Intellectual Property Section and before that as the Department of Justice's representative at the U.S. Embassy in Moscow. Prior to his work at the Department of Justice, Mr. Dembosky was an Assistant U.S. Attorney in the Western District of Pennsylvania where he served in the Computer Hacking and Intellectual Property Unit.

JIM PASTORE

Jim Pastore is a litigation partner and a member of the firm's Cybersecurity & Data Privacy practice and Intellectual Property Litigation Group. His practice focuses on privacy and cybersecurity issues. Prior to rejoining Debevoise in 2014 as counsel, Mr. Pastore served for five years as an Assistant United States Attorney in the Southern District of New York. While he was with the Criminal Division of the U.S. Attorney's Office, Mr. Pastore spent most of his time as a prosecutor with the Complex Frauds Unit and Computer Hacking and Intellectual Property Section. From 2004 to 2009, Mr. Pastore was an associate at Debevoise focusing on IP litigation.

SARAH COYNE

Sarah Coyne is a partner in the firm's Litigation Department and a member of the White Collar & Regulatory Defense Group. She handles a variety of white collar matters and investigations, including those involving financial institutions. Prior to joining the firm in 2015, Ms. Coyne was a federal prosecutor for 14 years, starting in the District of New Jersey, then moving to the U.S. Attorney's Office in the Eastern District of New York, where she was Chief of the Business and Securities Fraud Section.

DAVID SARRATT

David Sarratt is a partner in the firm's Litigation Department. He is an experienced trial lawyer whose practice focuses on white collar criminal defense, internal investigations and complex civil litigation. Prior to joining the firm, Mr. Sarratt served as an Assistant United States Attorney in the Eastern District of New York from 2010 to 2014. As a federal prosecutor, Mr. Sarratt supervised and participated in a wide variety of investigations and prosecutions, involving, among other crimes, international terrorism, computer intrusions, export violations, fraud and racketeering.

JANE SHVETS

Jane Shvets, international counsel in the firm's London office, is a member of the Litigation Department. Ms. Shvets focuses on white collar defense, internal investigations, and compliance advice, with a particular emphasis on foreign corrupt practices legislation. She also focuses on international arbitration and litigation, with an emphasis on Eastern Europe and Russia. Ms. Shvets has represented a variety of U.S. and foreign corporate clients in white collar criminal, securities, intellectual property, cybersecurity and international arbitration matters. She has represented clients in various industries, including transportation, natural resources, food & beverage, retail, and construction.

Acknowledgements

The authors would like to thank Debevoise associates Johanna N. Skrzypczyk, Naeha Prakash, Charles W. Baxter, William Ward Bucher IV, Chris Garrett, Reneé Garrick, Anna Gressel, Alex Ginsberg, Richard T. R. Harper, Sean Heikkila, Robert Maddox, Jonathan Metallo, Jennifer Freeman Mintz, Ardil Salem, Max Shaul, Neelima Teerdhala, Joseph Weissman and Derek Wikstrom for their invaluable contributions to Breach Reading 2.0, including their research, drafting, and revising of the materials. A special thank you to Richard Fitch, Fred Loessel, Kate Zvonkovic, Brianna Linde and the rest of the production team for their work in pulling all of this together. We would also like to recognize the important contributions from Debevoise summer associates Adam B. Peck and Joshua Cameron Shirley. We appreciate all the hard work.