Dechert LLP

ATTORNEY-CLIENT PRIVILEGED COMMUNICATION
ATTORNEY WORK PRODUCT

MEMORANDUM

DATE February 21, 2017

TO Tim Andrews
Director, The ID Register

FROM Timothy C. Blank
Hilary Bonaccorsi

RE Analysis of The ID Register's Data Privacy and Cybersecurity Practices Under U.S. Law

---

I. Facts

The ID Register is a digital platform hosted on the Microsoft Cloud ("Azure"). It is designed to streamline customer due diligence processes and regulatory reporting. The ID Register enables institutional and natural person applicants to create a profile, fill out a Universal Questionnaire for Funds and publish that profile on the ID Register at no cost. Applicants may then authorize the sharing of their profiles with any subscriber who pays to access the ID Register. Subscribers may include banks, legal firms, fund managers and other counterparties worldwide. Applicant profiles are kept up-to-date by the ID Register to ensure that each profile remains compliant with certain regulatory requirements.

The ID Register is a trading name of, and is owned and operated by, The ID Register (Guernsey) Limited. All agreements entered into by the ID Register are entered into by The ID Register (Guernsey) Limited.

II. Overview

We have been asked to review whether the ID Register complies with U.S. data privacy and information security laws. Because most of the ID Register's subscribers are financial institutions, our analysis focuses on data privacy and information security laws and regulations that apply to financial institutions, which include the following:

- Title V of the Gramm-Leach-Bliley Act of 1999 (the "G-L-B Act"), 15 U.S.C. § 6801 *et seq.*;
- The Security and Exchange Commission's ("SEC") Regulation S-P ("Reg. S-P" or the "SEC Regulations"), 17 CFR § 248 subpt. A, and the related guidance issued thereunder;

- Section 5 of the Federal Trade Commission Act of 1914 (the "FTC Act"), 15 U.S.C. § 45, prohibiting "unfair and deceptive trade practices;" and

- Standards for the Protection of Personal Information of Residents of the Commonwealth (the "Massachusetts Standards"), 201 Mass. Code Regs. 17.00.

We have also considered the ID Register's use of Azure to host the ID Register platform under applicable laws and guidance in a separate section entitled "Special Note Regarding Third Party Vendors."

III. Basis for Analysis

We have reviewed the ID Register Written Information Security Program (the "WISP"), the ID Register Incident Response Plan (the "IRP"), the ID Register Privacy Statement (the "Privacy Statement") and the ID Register's description of its security practices which appear under the "Security" tab (the "Security Statement" and together with the WISP, the IRP and the Privacy Statement, the "Policies") on www.theidregister.com. We have also reviewed Microsoft's description of the security, privacy and compliance features that Azure provides and which are available at https://azure.microsoft.com/en-us/support/trust-center/.

The ID Register represents that it is actually implementing the WISP and IRP. The ID Register also represents that it complies with the statements made in its Privacy Statement and Security Statement. We have not conducted testing to confirm that the ID Register is actually implementing the Policies. We also have not received or reviewed the results of any penetration testing conducted on the ID Register. Furthermore, we have not reviewed any policies associated with Azure and we have not conducted any testing on Azure or reviewed the results of any such testing. We also have not reviewed any agreements entered into between Apex, The ID Register, and Microsoft regarding the use of Azure. The ID Register represents that such agreements exist and that they contain adequate provisions related to data privacy and information security.

Accordingly, our analysis of the ID Register's compliance with U.S. privacy and data security laws rests on the ID Register's representations that:

- The ID Register fully complies with its WISP and IRP and actually implements the policies and procedures described in those documents;

- The ID Register fully complies with the statements made in its Privacy Statement and Security Statement;

- Apex, on behalf of the ID Register, has entered into an agreement or a series of agreements with Microsoft regarding the ID Register's use of Azure and the agreement(s) contain adequate provisions related to data privacy and information security; and

- The description of Azure that is provided at https://azure.microsoft.com/en-us/support/trust-center/ is accurate.

IV. Compliance with U.S. Law

A. G-L-B Act

The G-L-B Act addresses the collection, storage, use, disclosure and protection of "nonpublic personal information"[1] ("NPI") by "financial institutions."[2] 15 U.S.C. § 6801(a). In it, Congress directed various federal agencies that regulate financial institutions to establish "appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical and physical safeguards 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 such records; and (3) protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer." 15 U.S.C. § 6801(b).

Many federal agencies have adopted privacy rules (which require financial institutions to disclose to their customers how they collect and share customers' NPI and to limit that information sharing) and some have adopted safeguards rules (which require financial institutions to put in place programs to protect customers' NPI). *See, e.g.*, Reg. S-P, 17 CFR § 248.30; *but see* Consumer Finance Protection Bureau Privacy of Consumer Financial Information Rule (Regulation P), 12 CFR pt. 1016 (omitting safeguards rule provisions). Two of those federal agencies—the SEC and the FTC—are primary regulators of companies that will likely subscribe to the ID Register. The SEC adopted Reg. S-P in response to the G-L-B Act, under which it has jurisdiction over SEC registered investment advisers, SEC registered broker-dealers and SEC registered investment companies. Reg S-P, 17 CFR § 248.1(b). Similarly, the FTC adopted its Privacy Rule, 16 CFR pt. 313, and Safeguards Rule (together, The "FTC Regulations") 16 CFR pt. 314, under which it has authority over other "financial institutions," which include funds that that are exempt from SEC registration (*i.e.*, private funds and hedge funds).

The regulations promulgated by the SEC and FTC under the authority granted to them by the G-L-B Act are substantially similar. There are four reasons for which we only address Reg. S-P in this analysis. First, the regulations themselves are nearly identical from a substantive standpoint. Second, the SEC has issued significantly more guidance regarding the meaning behind the confusing

---

[1] The G-L-B Act defines "nonpublic personal information" as "personally identifiable financial information—(i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution." 15 U.S.C. § 6809(4)(A).

[2] The G-L-B Act defines a "financial institution" as "any institution the business of which is engaging in financial activities as described in section 1843(k) of title 12." 15 U.S.C. § 6809(3)(A).

and often contradictory terms used in Reg. S-P. *See, e.g.*, Staff Responses to Questions about Regulation S-P (SEC, January 2003), available at https://www.sec.gov/divisions/investment/guidance/regs2qa.htm. Third, via its enforcement division which is known as the Office of Compliance Inspections and Examinations ("OCIE"), the SEC has issued risk alerts that provide best practices for how investment advisers and broker-dealers should comply with the safeguards provisions of Reg. S-P. *See, e.g.*, 4 OCIE Nat'l Examination Program 8, 2015 Cybersecurity Examination Initiative (Sept. 15, 2015), available at https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf (hereinafter, the "OCIE Risk Alert"). And fourth, the SEC has brought enforcement actions for violations of the Rule 30(a) of Reg. S-P (the "Safeguards Rule"). *See, e.g.*, R.T. Jones Capital, Investment Advisers Act Release No. 4204 (September 22, 2015). The enforcement actions give further insight into the SEC's expectations.

The ID Register would not likely be considered a "financial institution" under the G-L-B Act and thus would not itself subject to the G-L-B Act, the SEC Regulations, or the FTC Regulations as a result. However, many of the ID Register's potential subscribers are subject to the G-L-B Act and the SEC and/or FTC regulations. The SEC and FTC Regulations hold financial institutions responsible for the "downstream protection" of the NPI they receive. Reg. S-P Limits on Disclosures, 17 CFR §§ 248.10-248.12. As a result, SEC and FTC regulated entities are focusing intensely on the third party vendors who store their customers' NPI. Those entities frequently seek representations from third party vendors (like the ID Register) that they themselves comply with the G-L-B Act and the related regulations and guidance issued thereunder. We have therefore analyzed whether the ID Register complies with the relevant portions of Reg. S-P.

1. *Reg. S-P: Privacy Rule*

The "Privacy Rule" provisions of Reg. S-P require financial institutions to provide their customers with a privacy notice at the outset of the customer relationship and, subject to certain exceptions, on an annual basis thereafter. 17 CFR §§ 248.4-248.5. The privacy notice must disclose: the categories of NPI that the financial institution collects from its customers; how it shares NPI with non-affiliated third parties; and how it safeguards and protects that information. 17 CFR § 248.6(a). Reg. S-P also requires financial institutions to provide customers with the opportunity to "opt out" of some, but not all, types of information sharing. 17 CFR § 248.7. Customers are not entitled to opt-out of having their information shared with nonaffiliated third parties when that information is shared for everyday business purposes (such as when it is shared with nonaffiliated service providers like the ID Register). 17 CFR § 248.13. However, under Reg. S-P, customers can still expect that when their NPI is held with a third party service provider, the third party must limit its disclosure in the same ways as the financial institution. 17 CFR § 248.11.

The ID Register would not likely be considered a "financial institution" under the G-L-B Act and Reg. S-P. As a result, the ID Register would not be required to provide a Reg. S-P privacy notice to applicants. However, the ID Register should still limit the ways in which it shares

applicants' information so that its information sharing practices are consistent with Reg. S-P. This is the case even though applicants provide their NPI directly to the ID Register rather than to a "financial institution" as defined by Reg. S-P.

The ID Register represents in its Privacy Statement that it does not share applicants' NPI in a way that would violate Reg. S-P. The ID Register specifically states, "We will not disclose or transfer personal information to third parties for the purposes of marketing or profiling, however we may disclose or transfer such information to agents or third parties authorized to act on our behalf or to third parties (including Apex Investor Services (UK) Limited, Apex (Ireland) Limited] and Apex Investor Services (Jersey) Limited) only for the purposes of providing the Services."

2. *Reg. S-P: Safeguards Rule*

The Reg. S-P Safeguards Rule requires financial institutions to "adopt written policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information." 17 CFR § 248.30. Specifically, the Safeguards Rule states that the "policies and procedures must be reasonably designed to: (a) Insure the security and confidentiality of customer records and information; (b) Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (c) Protect against unauthorized access to or use of customer records and information that could result in substantial harm or inconvenience to any customer." *Id.* at § 248.30(a).

The SEC Division of Investment Management and OCIE have both issued guidance for SEC registered investment advisers and broker dealers regarding cybersecurity practices. IM Guidance Update No. 2015-02 (SEC, April 2015), available at https://www.sec.gov/investment/im-guidance-2015-02.pdf; *see also* OCIE Risk Alert. Based on enforcement actions the SEC Staff has brought for violations of the Safeguards Rule, this guidance should be considered mandatory. OCIE's Risk Alert focuses on six key areas with respect to cybersecurity: (i) Governance and Risk Assessment; (ii) Access Rights and Controls; (iii) Data Loss Prevention; (iv) Vendor Management; (v) Training; and (vi) Incident Response.

As mentioned, the SEC Staff has also brought enforcement actions against investment advisers and broker-dealers for alleged violations of the Safeguards Rule. Among other issues, those enforcement actions have focused on the requirement that financial institutions actually implement their written policies and procedures regarding privacy and information security,[3] the importance of conducting "data mapping" to determine where customers' personal information is located within a

[3] *See* Morgan Stanley Smith Barney, Investment Advisers Act Release No. 4415 (June 8, 2016).

financial institution and how it is protected,[4] and the SEC's expectation that the entities it supervises have incident response plans.[5]

As drafted, the ID Register's WISP complies with the Reg. S-P Safeguards Rule. It addresses the six key areas of focus laid out in the OCIE Risk Alert. Based on the assumptions outlined in Part II infra, the ID Register is therefore compliant with the Reg. S-P Safeguards Rule.

B. Section 5 of the FTC Act

The FTC's authority to use the prohibition on unfair practices in Section 5[6] of the FTC Act to challenge companies' data security lapses has been upheld in federal court. *FTC v. Wyndham*, 799 F. 3d 236 (3d Cir. 2015). The FTC has used its "Section 5" authority to enforce companies' privacy promises, explaining that "[w]hen companies tell consumers they will safeguard their personal information, the FTC can and does take law enforcement action to make sure that companies live up to these promises." *See* FTC Media Resources, Enforcing Privacy Promises, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises. For example, after the data breach that affected the website AshleyMadison.com, the FTC filed a complaint charging that the website operators misrepresented that they had taken "reasonable steps to ensure AshleyMadison.com was secure," "that Ashley Madison.com had received a "Trusted Security Award," and that using the "Full Delete" service offered on the website would remove consumers' profiles from the website completely." Complaint For Permanent Injunction and Other Equitable Relief at 47, 53, and 51, *FTC v. Ruby Corp.*, No. 1:16-cv-02438 (D.D.C. filed Dec. 14, 2016), available at https://www.ftc.gov/system/files/documents/cases/161214ashleymadisoncmplt1.pdf. The website operators agreed to settle these and other related charges. FTC Press Release, Operators of AshleyMadison.com Settle FTC, State Charges Resulting From 2015 Data Breach that Exposed 36 Million Users' Profile Information (Dec. 14, 2016), available at https://www.ftc.gov/news-events/press-releases/2016/12/operators-ashleymadisoncom-settle-ftc-state-charges-resulting. As a result, under U.S. law, it is important that companies make accurate representations to their consumers with respect to consumers' privacy and data security.

The ID Register makes adequate representations regarding consumer privacy and information security in its Privacy Statement and Security Statement. The ID Register has provided assurances that it fully complies with the statements it makes in the Privacy Statement and Security

---

4 *See* Craig Scott Capital, Exchange Act Release No. 77595 (April 12, 2016).

5 *See* R.T. Jones Capital, Investment Advisers Act Release No. 4204 (September 22, 2015).

6 15 U.S.C. § 45(a)(2) (stating that "The [FTC] is hereby empowered and directed to prevent persons, partnerships, or corporations... from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce").

Statement. Therefore, it is unlikely that such statements would be found to be "false and misleading" under Section 5 of the FTC Act.

C. Massachusetts Standards

There is no generally applicable federal data protection law in the U.S.[7] Data protection requirements are therefore often addressed at the state level. *See e.g.*, the Massachusetts Standards; *see also* the Rhode Island Identity Theft Protection Act of 2015, R.I. Gen. Laws § 11-49.3. The Massachusetts Standards represent the high-water mark for U.S. companies that are not subject to separate, industry-specific regulations.[8] Therefore, even companies that do not have customers who are Massachusetts residents generally draft their written information security programs to comply with the Massachusetts Standards. To be compliant with U.S. law and related best practices, the ID Register should do the same.

The Massachusetts Standards require companies that collect "personal information"[9] about residents of the Commonwealth of Massachusetts to "develop, implement and maintain a comprehensive information security program." 201 Mass. Code Regs. 17.03(1). The information security program must be "written" and must contain "administrative, technical and physical safeguards that are appropriate to (a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive written information security program; (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information." *Id.*

---

[7] The G-L-B Act is a federal law that has data protection provisions; however, it only applies to "financial institutions" and is therefore not generally applicable to all companies.

[8] The New York Department of Financial Services ("NY DFS") recently proposed a comprehensive cybersecurity regulation that becomes effective March 1, 2017 and applies to entities that come within its jurisdiction. Cybersecurity Requirements for Financial Services Companies, 23 NYCRR 500.00 (2016) (hereinafter, "NY DFS Regulations"). The NY DFS Regulations are stricter than the Massachusetts Standards. Although NY DFS has not made it clear, it appears that the NY DFS Regulations do not apply to SEC registered investment advisers. Therefore, we have not analyzed the ID Register's compliance with the NY DFS Regulations.

[9] The Massachusetts Standards define "personal information" as "a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public." 201 Mass. Code Regs. 17.02.

The Massachusetts Standards lay out a series of specific requirements. For example, companies must place "reasonable restrictions upon physical access to records containing personal information," 201 Mass. Code Regs. 17.03(2)(g), "encrypt all data containing personal information to be transmitted wirelessly," 201 Mass. Code Regs. 17.04(3), and conduct "ongoing employee (including temporary and contract employee) training and compliance with policies and procedures." 201 Mass. Code Regs. 17.03(2)(b).

As drafted, the ID Register WISP complies with the provisions in the Massachusetts Standards. The Security Statement also indicates compliance with specific provisions in the Massachusetts standards such as those related to access to personal information and encryption of data at rest and in transit. Further, the ID Register represents that it has entered into an agreement with Microsoft to use the Azure program and has provided assurances that the agreement addresses all important information security safeguards. Based on these facts and representations, the ID Register is compliant with the Massachusetts Standards.

D. Special Note Regarding Third Party Vendors

The ID Register should pay particular attention to regulatory requirements and guidance regarding reliance on third party vendors. First, the ID Register itself will be considered a third party vendor to any subscriber, and second, the ID Register will rely heavily on its own third party vendor, Azure, to store and safeguard customer information. The Massachusetts Standards specifically require the ID Register to enter into agreements with third-party service providers who have access to Massachusetts residents' "personal information" in order to require them to agree to appropriately protect that information. 201 Mass. Code Regs. 17.03(2)(f)(2). Reg. S-P also includes "downstream" obligations that require SEC-registered entities to protect their customers' NPI when that information is in the possession of a third party service provider such as the ID Register. 17 CFR § 248.11. In addition, the OCIE Risk Alert includes "Vendor Management" as one of its six areas of focus; recommending, for example, that SEC registered investment advisers conduct due diligence on third party vendors and engage in ongoing monitoring of those vendors.

In addition, the Financial Industry Regulatory Authority ("FINRA")[10] has focused on proper oversight of third party service providers. In November 2016, FINRA fined member firm Lincoln Financial Securities Corp. ("Lincoln") for its alleged failure to implement security policies to protect confidential information after its web-based customer account database was hacked in violation of NASD Rules 3010(a) and 3010(b) (for conduct before December 1, 2014) and FINRA Rules 3110(a)

[10] FINRA is a self-regulatory organization that supervises member brokerage firms and brokers.

and 3110(b)[11] (for conduct after December 1, 2014).[12] Lincoln Fin. Sec. Corp., FINRA Letter of Acceptance, Waiver and Consent No. 2013035036601 (Nov. 14, 2016) (hereinafter "Lincoln AWC"). In the related settlement order, FINRA explained that while Lincoln had adopted written supervisory procedures ("WSPs") that addressed the storage of customer data on a cloud-based-server, FINRA found that Lincoln's WSPs did not provide adequate guidance on how those policies should be implemented. *Id.* at 3-4. FINRA found that Lincoln "failed to ensure that its registered representatives, or the third-party vendors retained by its representatives, adequately applied Lincoln's Data Security Policy." *Id.* at 3. For example, FINRA explained that "Lincoln failed to take adequate steps to monitor or audit the vendors' performance" by, in part, failing to "adequately test and verify the security of information stored on cloud servers at Lincoln's branch offices." *Id.* As some of the ID Register's potential subscribers may be FINRA member firms, the ID Register should be aware of FINRA's actions with respect to information security requirements and take active steps to test and verify the ID Register platform.

The ID Register represents that it has an agreement in place with Microsoft regarding its use of Azure and that the agreement addresses the security, compliance and transparency items detailed on the Azure website. We have not been asked to review the agreement. In addition, the ID Register represents that it takes advantage of various services offered via Azure such as the Microsoft Antimalware Service. The ID Register does not request audit reports from the third parties that certify Azure's compliance with its stated security controls, but the ID Register has the ability to view those reports when they are published by Microsoft and represents that it does so. Based on these representations, the ID Register is compliant with the provision in the Massachusetts Standards that relate to third party services providers and is taking appropriate steps that are consistent with the SEC's guidance on third party vendors.

---

11 FINRA Rule 3110 requires member firms to "establish and maintain a system to supervise the activities of each associated person that is reasonably designed to achieve compliance with applicable securities laws and regulations, and with applicable FINRA rules." The applicable underlying regulation Lincoln violated was Rule 30 of Reg. S-P.

12 NASD Rule 3010 was superseded by FINRA Rule 3110 effective December 1, 2014. *See* Lincoln AWC at n. 1. The FINRA settlement with Lincoln was related to conduct that occurred from at least 2011 to 2015, which importantly included a breach of a Lincoln office's computer server in January 2012 which affected the confidential records and information of approximately 5,400 Lincoln customers. Lincoln AWC at 3.

V. Conclusion

Based on the ID Register's Representations, The ID Register is compliant with the U.S. laws and regulations regarding privacy security and information security that are discussed in this memorandum and the ID Register is taking appropriate steps to comply with the guidance issued by various financial industry regulators.

THIS ANALYSIS IS SOLELY RENDERED FOR THE BENEFIT OF THE ID REGISTER (GUERNSEY) LIMITED. IT IS NOT TO BE RELIED UPON BY ANY THIRD PARTY AND DOES NOT CREATE AN ATTORNEY-CLIENT PRIVILEGE BETWEEN DECHERT LLP AND ANY SUCH THIRD PARTY.