Foreign Acquisitions of U.S. Companies: State Cybersecurity and Privacy Laws Expand the Scope of Due Diligence by a Geometric Factor by George H. Wang and Kenneth N. Rashbaum, Barton LLP

George H. Wang and Kenneth N. Rashbaum are partners in the New York office of Barton LLP.

In an age in which digital information is one of a company's most valuable assets, a growing share of due diligence time and effort is being devoted to compliance with laws and regulations governing the privacy and security of such assets. All businesses with a website may be said to have reach into, and presence in, every state—therefore due diligence into information management compliance of a U.S. target company requires cognizance of the laws of at least 52 separate jurisdictions comprising the 50 states, the District of Columbia, and Puerto Rico. This article discusses the need to expand due diligence into privacy laws beyond U.S. federal privacy laws to cover the breadth of U.S. state and territorial jurisdictions.

Federal Preemption Does Not Apply

Privacy law exemplifies the complexity of due diligence into acquisitions of U.S. companies. There is no all-encompassing national privacy or cybersecurity law in the United States, but federal legislation or regulations impose safeguards in the protection of digital information, particularly in the areas of financial services (including publicly traded companies), healthcare, and education. Additionally, M&A attorneys should be aware that 47 states have statutes governing notification of breach of personal financial or healthcare information. There is no standardization among these provisions—some states permit those aggrieved by the failure to receive breach notifications to sue in state court, while others only allow for complaints to state agencies which, in turn, can investigate and assess civil monetary penalties.

State laws that are stricter than federal legislation or regulations in the protection of federally regulated data (e.g., personally identifiable health information, subscriber or accountholder data and certain information on students created by educational institutions) are not preempted by federal law. In addition, certain state laws impose requirements not found in federal laws, such as requiring documented information management policies and adoption of protocols for notification of data breaches. Therefore, an acquirer must be cognizant of both the federal statutes pertinent to the industry of the target company and the applicable requirements of the states in which the target does or may transact business. If the target company conducts business over the Internet, it may be deemed to transact business in all 50 states and, therefore, a 50-state review may be advisable. The U.S. Supreme Court in J. McIntyre Machinery, Ltd. v. Nicastro, 564 U.S. 873 (2011), limited jurisdiction of state courts to companies that "purposefully avail themselves" of the markets in that state. But jurisdiction for litigation purposes is not the same thing as statutory or regulatory compliance, and so an acquirer would be well advised to consider the laws of all U.S. states in which the company has done or may do business, either by physical presence or over the Internet. In Pablo Star Ltd. v. Welsh Government, No. 16-CV-1167, 2016 U.S. Dist. LEXIS 33846, *19–*20 (S.D.N.Y. Mar. 16, 2016), the court held that Internet presence alone would not provide a basis for personal jurisdiction, but the question remains open as to how much more is required for "purposeful availment" of a state market by electronic commerce.

Health Information: Strong Federal Regulation, but Ignore State Law at Your Peril

Most non-U.S. acquirers, particularly those from European Union countries, are familiar with the U.S. health privacy regulations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Regulations under HIPAA provide requirements for privacy and security safeguards regarding medical treatment, condition, or payment that can be traced to an identifiable individual by one or more of 18 specified identifiers. These regulations affect not only healthcare providers and health insurance plans, but also, since the adoption of the Omnibus Final Rule in 2013, certain mobile health IT developers, consultancies and other entities that access identifiable patient information in order to provide a service to a healthcare provider or plan now fall under the jurisdiction of the HIPAA regulations. For the rules updated through March 26, 2013, see HIPAA Administrative Simplification Regulation Text.

While HIPAA regulations are enforced by the Office for Civil Rights of the United States Department of Health and Human Services (OCR), the Omnibus Final Rule provides that state attorneys general may bring HIPAA violation proceedings if OCR declines to do so; therefore, acquirers need to conduct diligence about pending state health privacy actions as well. Attorneys general in Connecticut, Illinois, and California have brought such proceedings and, with the ongoing epidemic of healthcare breaches, more state attorneys general will undoubtedly do so. In addition, states that permit claims based on a common law right of privacy may use the standards

in the HIPAA regulations as a metric for standard of care. In 2014, the Connecticut Supreme Court, in Byrne v. Avery Center for Obstetrics and Gynecology, 102 A.3d 32, 49 (Conn. 2014), held that "HIPAA and its implementing regulations may be utilized to inform the standard of care applicable to such claims arising from allegations of negligence in the disclosure of patients' medical records." The reach of state privacy laws, which would cover health information, may also extend beyond traditional healthcare organizations. In Pierre-Paul v. ESPN, Inc., 2016 U.S. Dist. LEXIS 119597 (S. D. Fla. Aug. 29, 2016), a federal court in Florida recently allowed a claim in negligence for violation of medical privacy brought by New York Giants football player Jason Pierre-Paul against the sports television network ESPN, which had released medical records photographed and tweeted by a reporter that described Pierre-Paul's treatment for a fireworks-related accident.

State litigation, though, may not be the most significant exposure for an acquirer of a healthcare entity. A number of states have explicit medical privacy regulations that are enforced by administrative agencies. State attorneys general may commence litigation or investigations, but state departments of health may also commence proceedings for violations against patient or health insurance plan subscribers. Florida recently passed an Information Protection Act, under which the Florida Attorney General may bring violation proceedings and California's Confidentiality of Medical Information Act (CMIA) has been extant for many years and has been enforced in proceedings by the Office of the Attorney General of the State of California.

State Financial Information Safeguard Requirements Multiply

The media reports of attacks on financial services organizations, from banks as large as JPMorgan Chase to one and two-person broker-dealers, are too numerous to list here. The recent financial information breaches have led the Financial Industry Regulatory Authority (FINRA), the Commodities Futures Trading Commission, and the Securities and Exchange Commission to promulgate or update regulations concerning protection of financial data. The Gramm-Leach-Bliley Act, which mandates certain confidentiality controls for consumer financial information, has not been updated in recent years, but in 2016 the Federal Trade Commission, which enforces this statute, sought comments to its draft revision of the FTC Safeguards Rule that would require measures to keep customer information secure (https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/safeguards-rule). Yet, if the acquirer only asks about compliance with regulation by these federal agencies, the acquirer may be missing a potentially significant risk of exposure to state proceedings.

As in the case of healthcare data, financial data protection has been the subject of numerous investigations by state attorneys general. Attorneys General of Maryland, New York, California, and several other states launched investigations in the wake of the massive breach of credit card information from Home Depot in 2014. The New York Attorney General participated in a multi-state settlement with TD Bank over a breach of the data of 260,000 customers, 31,407 of whom were from New York (http://www.ag.ny.gov/press-release/ag-schneiderman-announces-multi-state-settlement-td-bank-over-data-breach). California's experience with data breaches led to a comprehensive breach report released in February, 2016 (https://oag.ca.gov/breachreport2016) and the promulgation of minimum security standards cited in the previous paragraph.

The New York Department of Financial Services (NYDFS) has conducted audits of financial services organizations under its jurisdiction since March of 2015, initially with a cybersecurity questionnaire (available at http://www.bartonesq.com/wp-content/uploads/2015/04/4.2.2015-NYDFS-letter-to-cybersecurity-insurers.pdf). Organizations under the jurisdiction of NYDFS include banks, investment companies, credit unions, insurers, and upwards of 2,200 other companies (http://www.dfs.ny.gov/about/whowesupervise.htm).

In September 2016, New York's Governor Andrew Cuomo announced that the NYDFS proposed cybersecurity regulations would go into effect following a 45-day comment period unless modified. They would require covered financial services organizations to:

- Prepare and implement a written information security plan and train the work force on that plan;
- Establish a clear breach response protocol and report certain breaches to NYDFS;
- Designate a Chief Information Security Officer;
- Prepare detailed policies and procedures to monitor the security safeguards of third-party service providers;
- Implement multi-factor authentication;
- Perform quarterly vulnerability assessments and annual penetration analyses; and
- Maintain an audit trail system that would log access to critical systems and system events including alterations to the audit trail systems. (http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf)

General Information Safeguards at the State Level Continue to Evolve

Privacy and information security requirements in many states cover regulated information in categories beyond healthcare and financial information and may, in fact, be stricter than federal information safeguards. In the case of healthcare, following the 2013 effective date of the Omnibus Final Rule, state attorneys general may decide whether to proceed under these state provisions or to bring proceedings for violations of the HIPAA Privacy or Security Rules. The Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth (201 CMR 17.03), discussed in further detail below, mandates precise safeguards for the protection of sensitive personal information that falls into several categories, including financial data. The Office of the Massachusetts Attorney General has brought a number of proceedings under these regulations.

In February 2016, the Office of the Attorney General of California, a state that has long been a leader in security and privacy safeguards, adopted the 20 security controls of the Center for Internet Security's Critical Security Controls as "a minimum level of information security that all organizations that collect or maintain personal information should meet." These safeguards provide more comprehensive security safeguards than the CMIA (which comprises mostly privacy protections). The Attorney General's February 2016 report states that these controls are a standard for information protection in California: "The failure to implement all the controls that apply to an organization's environment constitutes a lack of reasonable security." It is possible that the Attorney General may bring actions for failures to meet these standards; however, as the promulgation of these standards is relatively recent, it is unclear whether courts will consider them as a metric for standard of care under California's privacy laws.

Acquirers interested in target companies in, or that do business in, Massachusetts or California, or states with similar laws, should consider incorporating inquiries regarding compliance with such laws and regulations in their due diligence questionnaires and review.

Conclusion

Dire economic consequences may await the acquirer who does not follow through on comprehensive due diligence of cybersecurity risks. On September 22, 2016, Yahoo announced that 500 million Yahoo accounts were hacked in late 2014 by what Yahoo believed was a state-sponsored actor. The Yahoo breach of information was announced publicly after the parties entered into a definitive Stock Purchase Agreement earlier in July for the sale of all of the outstanding shares of Yahoo, as reorganized, to Verizon. This timing raises questions regarding what information may or may not have been appropriately disclosed by Yahoo in due diligence with regard to Verizon's offer to purchase certain assets, as well as whether Verizon asked and followed up on responses that could have revealed the existence of that massive breach. At best, Yahoo is likely to face a request for a significant purchase price adjustment, or Verizon may seek to terminate the transaction completely.

Foreign acquirers of target companies in the United States should be cognizant of, and appropriately conduct their due diligence procedures in a thorough manner given, the increasing promulgation of complex regulations and laws related to privacy and cybersecurity issues at the state level, as well as federal regulations that have expanded dramatically in recent years. Conducting an appropriately expansive due diligence review of a target's compliance with federal and state regulations could avert potential enforcement actions or litigation by state attorneys general, federal and state agencies, and individuals under a private right of action, as well as potentially expensive market fallout.