AN A.S. PRATT PUBLICATION
OCTOBER 2015
VOL. 1 • NO. 2

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

EDITOR'S NOTE: COMBATING RISKS
Steven A. Meyerowitz

DEALMAKERS IGNORE CYBER RISKS AT THEIR OWN PERIL
Aaron P. Simpson and Adam H. Solomon

CYBERSECURITY AND GOVERNMENT "HELP" – ENGAGING WITH DOJ, DHS, FBI, SECRET SERVICE, AND REGULATORS – PART I
Alan Charles Raul and Tasha D. Manoranjan

THE DEFEND TRADE SECRETS ACT OF 2015: ATTEMPTING TO MAKE A FEDERAL CASE OUT OF TRADE SECRET THEFT – PART I
David R. Fertig, Christopher J. Cox, and John A. Stratford

FTC LAUNCHES "START WITH SECURITY" INITIATIVE: RELEASES DATA SECURITY GUIDANCE AND ANNOUNCES NATIONWIDE CONFERENCE SERIES
James S. Talbot

FFIEC RELEASES VOLUNTARY CYBERSECURITY ASSESSMENT TOOL
James S. Talbot and Cristina Vasile

JEEP HACK DRIVES CYBER, CRISIS, LIABILITY, AND SUPPLY CHAIN COVERAGE ISSUES
Joseph F. Bermudez

Pratt's Privacy & Cybersecurity Law Report

VOLUME 1 | NUMBER 2 | OCTOBER 2015

Editor's Note: Combating Risks
Steven A. Meyerowitz 43

Dealmakers Ignore Cyber Risks at Their Own Peril
Aaron P. Simpson and Adam H. Solomon 46

Cybersecurity and Government "Help" – Engaging with DOJ, DHS, FBI, Secret Service, and Regulators – Part I
Alan Charles Raul and Tasha D. Manoranjan 53

The Defend Trade Secrets Act of 2015: Attempting To Make a Federal Case Out of Trade Secret Theft – Part I
David R. Fertig, Christopher J. Cox, and John A. Stratford 60

FTC Launches "Start With Security" Initiative: Releases Data Security Guidance and Announces Nationwide Conference Series
James S. Talbot 66

FFIEC Releases Voluntary Cybersecurity Assessment Tool
James S. Talbot and Cristina Vasile 70

Jeep Hack Drives Cyber, Crisis, Liability, and Supply Chain Coverage Issues
Joseph F. Bermudez 74

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3000
Fax Number .... (518) 487-3584
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3000

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Aaron P. Simpson and Adam H. Solomon, *Dealmakers Ignore Cyber Risks at Their Own Peril*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [46] (LexisNexis A.S. Pratt)

An A.S. Pratt™ Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2015–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 718.224.2258. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report,* LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Dealmakers Ignore Cyber Risks at Their Own Peril

By Aaron P. Simpson and Adam H. Solomon*

With cyber attacks pervasive in commerce today, it is imperative for businesses engaging in corporate transactions to consider the cybersecurity and privacy risks of their investments prior to purchasing, merging with, or financing a company. Dealmakers can mitigate these risks and prevent the incurrence of unanticipated costs and criticism from unforeseen information security and privacy issues that may emerge after the closing of a deal through thoughtful due diligence efforts. The authors of this article discuss the cybersecurity and privacy due diligence process.

In today's commercial environment, it is imperative for businesses engaging in corporate transactions to consider the cybersecurity and privacy risks of their investments prior to purchasing, merging with or financing a company. Cyber attacks across industry are rampant, and purchasers face significant risks of data breaches and privacy violations occurring before or arising after the closing of a deal. These events can increase liability and ultimately harm the value of the investment. Through thoughtful due diligence efforts, dealmakers can mitigate these risks and prevent the incurrence of unanticipated costs and criticism from unforeseen information security and privacy issues that may emerge after the closing of a deal.

There are many liabilities that may arise from the collection, use, disclosure and security of company data. The most significant liabilities result from cyber attacks compromising sensitive information maintained by the company. As a starting point, companies experiencing a breach incur potentially hefty costs investigating, remediating and responding to breaches, including the cost of conducting a forensic examination and fixing, rebuilding, upgrading or altogether replacing impacted computer systems. On top of these expenses, data breaches pose liability risks associated with regulatory enforcement, fines and assessments levied by payment card brands or regulators, private litigation such as consumer class actions and shareholder derivative suits and congressional inquiries, as well as losses of sales, goodwill, intellectual property, information assets and shareholder value. Similar liability risks may arise for companies in data-intensive fields from the use of consumer information in violation of privacy laws or company privacy policies that are treated as actionable public representations under state and federal consumer protection laws.

---

* Aaron P. Simpson, a member of the Board of Editors of *Pratt's Privacy & Cybersecurity Law Report*, is a partner at Hunton & Williams LLP, advising clients on a broad range of privacy and cybersecurity matters, including state, federal, and international privacy and data security requirements as well as the remediation of data security incidents. Adam H. Solomon is an associate at the firm, focusing his practice on privacy and cybersecurity law. Resident in the firm's New York office, the authors may be contacted at asimpson@hunton.com and asolomon@hunton.com, respectively.

Faced with the seeming inevitability of cyber attacks and potentially massive liability that ensues, companies and management are increasingly judged by how well they have prepared for and responded to these types of events. When purchasing, merging with or investing in a company, conducting due diligence of the target company's information assets has become a critical step in protecting investments, limiting liability and mitigating operational, financial and reputational risk arising from the target company's privacy and information security practices.

THE CYBER AND PRIVACY DUE DILIGENCE PROCESS

To manage these risks and liabilities, companies must be proactive. Even if the target company makes representations that it has never suffered a breach, it is undoubtedly only a matter of time before a cyber attacker exploits potential vulnerabilities or a third party identifies ongoing misuse of company information. Moreover, an attack may already be underway. In 2014, an Israeli security firm discovered an ongoing hacking operation targeting banks, governments, research labs and critical infrastructure facilities in Europe that began over 12 years before it was discovered.[1] With network intrusions becoming more persistent, the risk of acquiring a company experiencing an ongoing breach (perhaps unknowingly) has increased.

Potential post-closing integration difficulties also up the ante on diligence associated with information assets. Following a merger or acquisition, companies often face difficulties in integrating their information assets, which can lead to cyber intrusions and privacy mishaps. For example, the merging of the networks or databases of different entities may introduce security weaknesses, induce privacy violations or result in coverage gaps in the company's cyber insurance policy, all of which can be managed more effectively if the companies go into the deal with their eyes wide open.

By conducting cybersecurity and privacy due diligence, purchasers can proactively identify incidents and issues that give rise to concerns regarding the adequacy, reasonableness and appropriateness of the target company's privacy and information security practices. In doing so, the purchaser can develop a roadmap for remediating any material gaps post-closing so that it is well-equipped to manage the cybersecurity and privacy risks of its new investment efficiently and appropriately. Due diligence requests for privacy and cybersecurity-related materials can, however, become overly burdensome and inefficient if the right issues are not identified and the wrong questions are asked. Each due diligence approach should be tailored to the deal and companies at issue. The process should begin with a comprehensive privacy and information security due diligence questionnaire that asks specific questions to the target company and should end with an agreement that contains the appropriate

[1] *See* Liat Clark, *Decade-long Cybercrime Ring Hacked European Banks and Labs*, Wired.Co.UK (Sept. 16, 2014), http://www.wired.co.uk/news/archive/2014-09/16/harkonnen-operation.

representations and covenants concerning privacy and security. As described below, this diligence process should account for the following key areas of risk.

Incident History

There are an assortment of actors threatening corporate information assets today, including cyber criminals, hacktivist organizations and nation states. These threat actors routinely infiltrate corporate networks to steal proprietary information, including customer and employee personal data, payment card information, sensitive financial and strategic information, trade secrets and intellectual property. These parties are not acting alone. To the contrary, they are supported by a sophisticated supply chain of vendors, including software developers, infrastructure providers and money launderers. While some of these attacks are targeted and bespoke, many are carried out using toolkits purchased on the black market that enable non-technical actors to hack corporate networks on a scalable basis using sophisticated malware and other automated methods. As a result of the commodification of hacking, the frequency and volume of cyber attacks has increased.

With the rise in cyber attacks, there is a growing risk of a data breach going undetected or undisclosed prior to closing a deal. Cyber attacks have impacted several deals in recent years. For example, Australian telecommunications provider Telstra reported that it recently became aware of a customer data breach at a subsidiary acquired in the Asia-Pacific region just weeks after closing a $697 million deal to purchase the company in April 2015.[2] Nearly 10 months after acquiring a data broker subsidiary in 2012, Experian was reportedly notified by the U.S. Secret Service that its new subsidiary was being exploited by identity thieves to steal the personal information of allegedly over 200 million individuals.[3] The incident resulted in congressional and regulatory inquiries, a consumer class action brought against Experian, and Experian suing the former owner of its subsidiary for breach of warranty and contract, express contractual indemnification and various tort claims arising from its acquisition. Similarly, in the midst of BNY Mellon acquiring the asset management subsidiary of MBIA in October 2014, a data researcher reportedly discovered sensitive information of the subsidiary exposed on the Internet, including customer account numbers, balances and account access credentials.[4]

---

[2] Mike Burgess, *Pacnet Security Breach*, Telstra Exchange (May 20, 2015), http://exchange.telstra.com.au/2015/05/20/pacnet-security-breach/.

[3] Gerry Tschopp, *The Facts on Court Ventures and Experian*, Experian News Blog (Mar. 30, 2014), http://www.experian.com/blogs/news/2014/03/30/court-ventures/; Jim Finkle & Karen Freifeld, *Exclusive: U.S. States Probing Security Breach at Experian*, Reuters, http://www.reuters.com/article/2014/04/03/us-experian-databreach-idUSBREA321SL20140403.

[4] Edward Krudy & Hilary Russ, *Update 1: Data Breach at Bond Insurer MBIA May Affect Thousands of Local U.S. Governments*, Reuters (Oct. 7, 2014), http://www.reuters.com/article/2014/10/08/mbia-cybersecurity-idUSL2N0S22LB20141008.

To help evaluate the target company's cybersecurity posture and obtain appropriate representations and warranties, the purchaser should investigate the target company's history of cybersecurity incidents, including those related to the company's network, service providers, Web sites, and customers. The clear objective of this inquiry should be to uncover circumstances in which the target company has discovered or been notified of an actual or suspected information security incident, and receive appropriate representations regarding how the company responded to the matter, assessed and satisfied its applicable legal obligations, and remediated the incident. To gain a complete picture of the target company's history of privacy and security incidents, the review also should ascertain the process by which the company monitors, detects, investigates and responds to information security incidents. A lack of appropriate incident response mechanisms increases the likelihood that a breach has gone undetected or undisclosed to management.

Regulatory Compliance

Legal compliance is another key risk to evaluate during the due diligence process. The obligation to comply with privacy and information security laws and standards can raise the integration costs of the acquisition. To remediate deficiencies, the purchaser may need to incur expenses such as updating or replacing computer systems, hiring additional staff, purchasing new services and retaining outside experts to provide assessments. While all companies have compliance challenges, the risk of noncompliance with applicable legal requirements is especially prevalent with startups and midsize companies, which often have less robust, formal and well-funded compliance, legal and information security programs. This can lead to the existence of gaps between such a target's privacy and information security practices and its legal obligations. In these cases, the cost of noncompliance can be significant.

In addition to incurring potentially substantial expenses to remediate privacy and information security issues and align the target company's practices with the purchaser's policies, a regulatory violation could result in fines or civil penalties and extensive settlement agreements that impose onerous information security and privacy requirements on not only the target company but also the purchasing entity. As a historical matter, Federal Trade Commission ("FTC") settlements in the information security arena have been broad, typically enjoining future misconduct and imposing continuing obligations related to the company's information security practices, including third-party audits, for over 20 years. Given how privacy and information security issues were regulated just five years ago, 20 years is a virtual eternity in the data space.

There are many sources of privacy and information laws in the United States and abroad. In the U.S., information privacy and security laws constitute a complex mélange of sectoral-based state and federal laws. Depending on the nature of the target's business, a variety of federal and state laws concerning privacy and information security could apply to the target company's information, including laws regulating

healthcare entities, telecommunications providers, utilities and financial institutions. The FTC has been the primary regulator overseeing privacy and information security practices in the U.S. by using its core consumer protection authority to enforce against unfair or deceptive practices of unregulated entities such as retailers. Industry standards also may impose privacy and security requirements on the target company. Most notably, to the extent the target company receives or processes payment card information, it will have contractual obligations to comply with the comprehensive security requirements of the Payment Card Industry Data Security Standard.

Given the variety of legal mandates applicable to privacy and information security issues, the due diligence process must include an evaluation of the applicable requirements set forth in federal, state and foreign laws, regulatory enforcement actions, and important industry standards concerning privacy, information security and data protection. Based on the applicable requirements, the review should in turn identify and assess areas in which the target's privacy and information security practices fall short of its legal obligations. The target company's privacy and information security policies and procedures serve as key sources of information for conducting such an assessment. To gain a further understanding of the company's privacy and security posture, the compliance review also should evaluate reports prepared by or on behalf of the target company documenting the findings and recommendations from prior risk assessments, privacy and security assessments, or audits or evaluations, including any associated corrective action plans related to those reports. Through these materials, the purchaser can identify red flags and compliance gaps such as out-of-date policies and procedures, inaccurate descriptions of the target's practices or lack of legal compliance, all of which can create significant issues post-closing.

Privacy Representations

To the extent the target company makes privacy representations to its customers, for example, through an online privacy notice or Health Insurance Portability and Accountability Act ("HIPAA") privacy notice, the due diligence review should assess the target's privacy practices and policies representing the way in which it may collect, retain, use, share and process the personal information of consumers. The representations in the target's privacy notices will place limits on the purchaser's ability to use and share this information after the acquisition. Notably, the FTC has issued guidance and sent letters to companies engaging in acquisitions, most recently a letter to Facebook prior to its acquisition of WhatsApp in 2014,[5] regarding its expectation that following a merger or acquisition, the purchaser must honor the prior promises made to consumers by the purchased entity regarding how it may use or share consumer information, or otherwise get express permission from consumers to

[5] Letter from Jessica Rich, Director, Bureau of Consumer Protection, to Erin Egan, Chief Privacy Officer, Facebook, Inc. and Ann Hoge, General Counsel, WhatsApp Inc. (Apr. 10, 2014), https://www.ftc.gov/system/files/documents/public_statements/297701/140410facebookwhatappltr.pdf.

materially change how their previously collected information will be collected, used or shared after the corporate transaction.[6] For many companies this would be a gargantuan and entirely impractical exercise that should only be taken on with full knowledge of the possibility before closing. The acquisition or merger also might require the company to provide consumers with notice of any change to how it plans to use information collected after the transaction and a choice whether to agree to such changes.

Contractual Liability

The due diligence process also should include an assessment of the target company's contractual relationships with vendors, customers and business partners. Besides assessing the company's risk and legal posture, this review will help identify the next steps for managing the company's vendor and customer relationships after closing in cases where existing contractual language could be enhanced or revised, or ongoing monitoring may be appropriate.

With respect to the target company's vendors, the purchaser should identify third-party privacy and security risks associated with the target outsourcing IT functions to data centers, software developers and other types of service providers. The focus of this review should be on the agreements in place with vendors that host, maintain, receive or transmit the target company's sensitive information. It also is important to ascertain how the target selects, reviews and monitors its vendors. If the target does not take reasonable measures to retain appropriate vendors, include strong contractual protections in its agreements with vendors and monitor its vendors' compliance, then the possibility of a data breach at one of those vendors, known or unknown, increases. Issues commonly found in vendor contracts include agreements with insufficient contractual specifications, broad sharing and usage rights related to the target's information, or a lack of privacy, confidentiality and information security obligations altogether. The review also may uncover that the agreements do not adequately comply with applicable laws, such as when the vendor constitutes a business associate under HIPAA, which requires specific contractual obligations in the business associate agreement.

In addition to vendor agreements, in most cases it will be necessary to evaluate the target company's customer and business partner agreements. These agreements may include additional privacy and information security obligations over and above the target's legal obligations. If such agreements contain terms that establish additional privacy requirements and security specifications such as adherence to information security standards, limitations on data de-identification or restrictions on outsourcing,

---

[6] *See e.g.*, Jamie Hine, *Mergers and Privacy Promises*, Fed. Trade Comm'n (Mar. 25, 2015), https://www.ftc.gov/news-events/blogs/business-blog/2015/03/mergers-privacy-promises.

the company may have additional compliance-related challenges and costs associated with meeting such obligations.

Furthermore, in this day and age it is necessary to assess the target's cyber insurance coverage as part of this contractual review. This assessment should analyze both companies' insurance portfolio, including current policies covering cybersecurity, directors and officers, errors and omissions, fidelity and crime, and general commercial liability, to assess potential coverage in the event of a cyber incident and the ramifications the corporate transaction may have on the coverage.

CONCLUSION

Given the pace of technological change we have seen in the recent past and the potential for scalable privacy and information security abuses, the cyber-stakes are at an all-time high. Businesses making investments in data-intensive targets overlook diligence in these key areas at their own peril. Those who take appropriate precautionary measures to assess the privacy and cybersecurity implications of their investments will continue to fare far better than those that fail to do so. By performing due diligence of the target company's privacy and information security practices, businesses will identify key risks to their investment and gain critical knowledge of how potential liabilities may impact their investment.