WILLKIE FARR & GALLAGHER LLP

BRUSSELS CHICAGO FRANKFURT HOUSTON LONDON LOS ANGELES MILAN NEW YORK PALO ALTO PARIS ROME SAN FRANCISCO WASHINGTON

Cybersecurity & Data Privacy Issues In Transactions – Corporate Training Seminar

Daniel Alvarez | Michelle Bae
July 13, 2022

WILLKIE FARR & GALLAGHER LLP

Agenda

- What Are The Risks?
  - Three High-Profile Examples of Privacy/Cyber Issues In M&A
  - Enforcement and Regulatory Trends in Privacy and Cybersecurity
- Identifying and Protecting Against Risk
  - Risk Considerations in Diligence
  - Risk Allocation – Reps, Covenants, and Specific Indemnities
- Questions

Privacy & Cybersecurity in M&A: What Are The Risks?

Case Studies – Three High-Profile Examples

Verizon/Yahoo!

- July 2016, Yahoo and Verizon enter into a merger agreement, under which Verizon would acquire Yahoo's operating business for $4.83 billion.
- September 2016, Yahoo discloses two major breaches for the first time, despite allegedly knowing of the breaches earlier.
  - The breaches occurred in 2013 and 2014.
  - Affected approximately 3 billion user accounts, and compromised names, email addresses, telephone numbers, birth dates, encrypted passwords and, for some users, unencrypted answers to security questions.
- February 2017, Verizon announces new terms to the deal, including $350 million reduction in price, and Yahoo! retaining certain liabilities.
  - Regulatory ($35 million) and litigation ($117.5 million) penalties on top.

Marriott/Starwood

- November 2016, Marriott International acquires Starwood Hotel and Resorts for $13.6 billion.
- September 2018, Marriott detects a breach in Starwood's guest reservation system that had been ongoing since 2014
  - Removes the unauthorized users, but the damage has been done: ~340 million customers (including millions of UK and EU residents) had personal information exposed
  - Compromised data included payment card info and passport numbers.
- July 2019, the UK's Information Commissioner's Office announces its intention to fine Marriott $124 million for GDPR violations, including for failing to keep customers' personal data secure.
  - ICO concludes that Marriot failed to undertake sufficient due diligence when it bought Starwood, so it retained liability associated with the breach.
  - In October 2020, ICO announced fine for Marriot of ~$22 million (reduction likely due to COVID impact on hotel industry).

RadioShack

- April 2015, RadioShack proposed a bankruptcy sale of certain assets, including personally identifiable information (PII) of 67 million customer contacts – name, physical address, email address, phone number, and other transaction data.
  - But RadioShack's privacy policy told customers "**we will not sell or rent your PII to anyone at any time**" and offline stores had similar language.
- 38 state AGs, supported by FTC, opposed the sale, arguing it would violate RadioShack's privacy policy and state and federal consumer protection laws, including FTC Act.
- Resolution – limited data available to purchaser, purchaser notified individuals about the deal, provided individuals chance to opt-out prior to transfer/use of PII, and promised no further sale or transfer of PII.

Enforcement and Legal/Regulatory Trends

Privacy & Cyber Regulatory Landscape

The privacy and cyber regulatory landscape is growing increasingly complex, particularly for entities that operate across national borders.

- U.S. state and federal Laws
  - Federal privacy law compromised mainly of FTC using Section 5 authority, plus sectoral/activity-based laws, e.g., GLBA (financial institutions), HIPAA (healthcare providers/insurers), CAN-SPAM/TCPA (advertising)
  - Comprehensive state privacy laws: California (already in effect), Virginia, Colorado, Utah, Connecticut (all coming into effect in 2023)
  - Growing number of state-level sector- and data-specific laws: e.g., NY DFS Cyber rules, Illinois Biometric Information Privacy Act, etc.
  - New federal privacy law or rules coming down the pike?
- Non-US laws
  - Many countries borrowing from GDPR to some degree with new privacy laws – Brazil, China, India, others.
  - Data localization and cross-border data transfer restrictions becoming more prominent.

Privacy Liability and Enforcement Trends (EU)

- DPAs in Europe have used the authority granted in GDPR to impose significant penalties. Some examples include:

Company	Settlement/Fine	DPA/Regulator
Amazon (2021)	€746 million	CNIL (France)
WhatsApp	€255 million	Ireland
Google (Ireland)	€90 million	Ireland
Facebook	€60 million	CNIL (France)
H&M	€35 million	Hamburg (Germany)

- *Reports out of Ireland suggest Irish DPA is considering an order that would prohibit Facebook/Meta from sending EU data to the US, an order that Facebook has said would force Facebook out of Europe.*

Privacy Liability & Enforcement Trends (US)

- Recent notable settlements and fines highlight just how expensive data privacy and data security violations (or allegations thereof) can be.

Defendant	Settlement/Fine	Notes
Facebook	$5 Billion	Record-breaking monetary penalty re violation of 2012 FTC privacy order
Facebook	$650 Million	Largest settlement under Illinois BIPA
Equifax	$575 Million	Included massive injunctive reqs
Home Depot	~$200 Million	Still paying 7+ years after breach.
Yahoo!	~$150 Million	Does not include reduced enterprise value of $350 million.
Uber	$148 Million	Consumer class action settled 2018
Capital One	$80 Million	Regulatory fine only, not litigation

Identifying and Protecting Against Privacy/Cyber Risk in M&A

Privacy/Cyber Issues in M&A

- Changes in EU, U.S., and global privacy/data protection laws have raised the profile and broadened the issues covered by privacy/cybersecurity diligence.
- Importance of data and cybersecurity issues in M&A increasing.
  - Major breaches, and rise in frequency, size, and cost of ransomware incidents have heightened concerns re: potential exposure.
  - More risk around data increases importance of diligence to identify potential areas of liability.
  - Target company's compliance (or not) with privacy and data security laws and/or usage or transfer of data post-close can be a deal breaker.
- In a representations and warranties insurance (RWI) deal, external parties such as carriers/insurers have an interest in the privacy/cyber compliance posture of the target company.
  - Exclusions/carve-outs in coverage on data privacy and security due to potential exposure.

Risk Considerations and Diligence

Key Diligence Questions – Identifying Scope

- Some of the key diligence questions that we and other parties regularly ask to help understand the scope of the target's data privacy activities and risk include:
  - What data is being collected? (personal data, material business data)
  - Where is the data being collected from – US, EU, China, Russia, etc.?
  - How is the data being used or shared? Used for electronic marketing, processing payments, etc?
  - Is the data being processed for the target's benefit or on behalf of the target's customers? Are there any significant contractual limitations on the use of certain data?

The answers to these questions help us understand what privacy and cybersecurity laws and other requirements may apply:

- Jurisdiction-specific laws depending on the company's operations
- Industry-specific issues (GLBA, HIPAA, CAN-SPAM/TCPA)
- State-specific issues (e.g., CCPA, BIPA, NAIC Model Laws)
- Other requirements (e.g., PCI-DSS)

Key Diligence Questions – Assessing Compliance

- Understanding scope allows us to assess the extent to which the target is complying with applicable laws, regulations, and requirements and/or behaving consistently with similar companies we've seen.
- Key questions include:
  - Does the company maintain a compliance program and organization?
  - Does the company have documented policies on the proper use of personal information it collects? Are employees trained?
  - How sophisticated and effective are the company's security measures? Are they documented?
  - Does the Company perform diligence on vendors that it uses for various tasks that involve sharing data?
  - Any historical data breaches or security incidents?
  - Cyber insurance policy?

Key Diligence Questions – Third Party Help?

- Clients involved in bigger, more prominent deals with significant data assets may want to engage a third party forensic or IT consultant to conduct penetration tests, vulnerability assessments, or dark web scans.
  - A vulnerability assessment is a high-level, often automated test or series of tests that aims to identify potential vulnerabilities in the target system.
  - A penetration test involves both identification and attempted exploitation of vulnerabilities in the target system.
  - Dark web scan attempts to find evidence in the dark web that a target's systems may have been compromised.
- Every deal is different, and the right mix of legal, technical, and operational diligence will likewise be different for every deal.
- We work with various companies to perform these and similar activities during the diligence process and present to the client a comprehensive technical, operational, and legal picture of the company's privacy and security efforts.

Risk Allocation –
Reps, Covenants, and Specific Indemnities

Risk Allocation – Reps and Warranties

- Risk mitigation through strong reps and warranties can be an important part of overall risk allocation strategy.
  - Robust privacy reps becoming the norm, even for deals where data is not central.
  - RWI deals – need to balance strong reps against concerns re: disclosures or exclusions.
- Deals involving "sensitive" sectors (e.g., healthcare, financial data) or involving significant amounts of data (e.g., lead generation, data brokers) include even more robust and detailed reps.

Risk Allocation – Example Rep

(a) The Company complies with, and has at all times complied with, all Data Protection Requirements, which means, collectively, (i) Data Protection Laws; (ii) Privacy Policies; (iii) any Contracts and/or codes of conduct relating to the collection, access, use, storage, disclosure, transmission, or cross-border transfer of Personal Data; and (iv) the Payment Card Industry Data Security Standard; and (vi) advertising self-regulatory requirements.

(b) The Company established and maintains, and has maintained, physical, technical, and administrative security measures and policies, compliant with applicable Data Protection Requirements, that (i) identify internal and organizational risks to the confidentiality, integrity, security, and availability of Personal Data and/or business data and Data Systems taking into account the sensitivity of the data or systems; (ii) protect the confidentiality, integrity, security, and availability of the Company's software, systems, and websites that are involved in the collection and/or processing of Personal Data and/or business data and Data Systems; and (iii) maintain notification procedures in compliance with applicable Data Protection Requirements in the case of any breach of security compromising Personal Data and/or business data and Data Systems.

(c) The Company has not experienced any failures, crashes, security breaches or incidents, unauthorized access, use, modification, or disclosure, or other adverse events or incidents related to Personal Data and/or business data and Data Systems that would require notification of individuals, other affected parties, law enforcement, or any Governmental Authority.

(d) The Company has not received any subpoenas, demands, or other notices from any Governmental Authority investigating, inquiring into, or otherwise relating to any actual or potential violation of any Data Protection Law and, to the Company's Knowledge, the Company is not under investigation by any Governmental Authority for any actual or potential violation of any Data Protection Law. No notice, complaint, claim, inquiry, audit, enforcement action, proceeding, or litigation of any kind has been served on, or initiated against the Company or any of its officers, directors, or employees (in their capacity as such) by any private party or Governmental Authority, foreign or domestic, under any Data Protection Requirement.

(e) The execution, delivery, and performance of this Agreement shall not cause, constitute, or result in a breach or violation of any Data Protection Requirement or other standard terms of service entered into by the users of the Company's service(s).

Risk Allocation – Pre-Closing Covenants

- Pre-closing covenants can be a useful tool to address specific, concrete issues identified during diligence that can be mitigated prior to completion of transaction (typically at the expense of the seller).
- Examples include:
  - Updating non-compliant contracts with vendors or customers.
  - Publishing a website privacy notice that complies with applicable law.
  - Remediating specific issues identified in a penetration test.
- If not done properly, buyer has potential flexibility to take steps to protect itself.
  - Only an option if parties not doing simultaneous sign and close.

Risk Allocation – Post-Closing Covenants

- Certain risks that do not require immediate remediation prior to completion or cannot be remediated pre-closing given the transaction timeline.
- Including milestones or conditions to be met prior to closing (and after) gives the buyer some indication as to whether progress is being made.
- Some important considerations:
  - What is the risk and does it merit the effort of pushing for a covenant/condition?
  - How does an identified risk carry forward and how much is that risk actually mitigated by the pre-closing changes?
  - Do you trust the target to do it properly?

Risk Allocation – Specific Indemnities

- Specific indemnities can be used if there are known risks or if specific circumstances are discovered during diligence.
- The terms of the indemnity (e.g., scope, financial caps) will depend on the nature of the issue.
  - An obligation to reimburse the buyer with respect to loss suffered as a result of non-compliance issues known to the parties.
- Issues:
  - The target will generally push back, especially to an open-ended indemnity.
  - Potential liability can be difficult to assess.

Risk Mitigation – Post-Closing Integration

- Post-closing integration may be the most important component of the risk mitigation plan, and should be calibrated to both the buyer's goals and the current posture of the target.
- Three keys:
  - Amend policies to bring them up to your standards.
  - Install and deploy security measures on IT systems.
  - Train employees on new policies, security measures, etc.
- Important considerations:
  - What are the primary risks identified during diligence?
  - What is the legal regime that applies? Does it impose any restrictions, requirements, or obligations for which you are not currently compliant?
  - What are your goals for the target? Is the data a strategic asset?
  - What are the practical considerations and how do they match to any legal/compliance issues?

Questions?

Presenters

Daniel Alvarez
Partner, Communications & Media Department
Co-Chair, Cybersecurity & Privacy Practice Group
dalvarez@willkie.com
202-303-1125

Michelle Bae
Associate, Cybersecurity & Privacy Practice Group
ebae@willkie.com
212-728-3166