Mergers and Acquisitions Trends: What You Need to Know about Data Privacy & Security

Presented by
Brett Roberts and Sten Hoidal
May 31, 2019

Fredrikson & BYRON, P.A.

Agenda

- Introduction to F&B M&A
- Continued Trend in M&A: Rep & Warranty Insurance
- Data Privacy Security as Critical Issues
- Questions?

Introduction to F&B M&A

Fredrikson & BYRON, P.A.

Fredrikson Overview

Our Firm	Our Practices

• 290 attorneys
• Office locations:
  • Minneapolis, Minnesota
  • Bismarck, North Dakota
  • Des Moines, Iowa
  • Fargo, North Dakota
  • Mankato, Minnesota
  • Saltillo, Mexico
  • Shanghai, China
• "Where Law and Business Meet" approach to the practice of law
	• 30+ practice areas with depth and expertise in:
	  • Mergers & Acquisitions
	  • Private Equity
	  • Tax & Business Planning
	  • Corporate Governance
	  • Corporate Finance
	  • Employment & Labor
	  • Life Sciences & Healthcare
	  • FDA/Regulatory
	  • Intellectual Property/Trademarks
	  • Compensation Planning
	  • Litigation

Mergers & Acquisitions Group

- Completed over 275 M&A assignments in 2018 totaling over $7 billion in deal value
- Comprehensive range of transactions in a variety of structures, sizes, and industries

Continued Trend in M&A: Rep & Warranty Insurance

Purpose of R&W Insurance

- Seller makes representations (and warranties) about business (e.g., ownership, financial statements, compliance with laws, litigation, required consents, change in control fees, etc.).

- If a representation is untrue:
  - Traditionally: Buyer's indemnification rights would be secured by a portion of the purchase price (10-20%) being held back for a period of time (12 – 24 months) plus buyer's ability to sue seller.
  - Under R&W Insurance: Buyer may have a claim under insurance policy instead of against seller's escrow or against seller directly.

Increased Use of R&W Insurance

- Not as common 6 or 7 years ago.
- 29% of acquisitions of lower to middle-market private targets by public companies during 2016 and first half of 2017 used R&W insurance.[1]
  - Almost certainly higher now. Why?
    - Deal studies lag
    - Familiarity with R&W insurance is increasing
    - R&W insurers are selling better and cheaper products
    - M&A markets remains competitive and sellers prefer R&W insurance since it increases proceeds at closing and mitigates contingent liabilities.

[1] Source: ABA M&A Private Target Deal Points Study – 2017 Update.

Cons of R&W Insurance

- Moral Hazard?
  - Absent fraud, seller has little (or no) skin in the game. As a result, seller has less of an incentive to make sure representations are accurate.
    - But note: Since R&W insurance results in seller having little (or no) skin in the game, representations and warranties are typically easier to negotiate.
- Adequate Remedy?
  - Coverage limit is typically only 10% of purchase price
  - Pursuing claim can be a distraction (from post-closing strategy, e.g.)
  - Reputational harm
- **What to watch for: Representations for which seller might not know accuracy but if inaccurate will cause buyer reputational harm.**
  - **Examples: Data Privacy and Security reps**

M&A Trends:
Data Privacy Security as Critical Issues

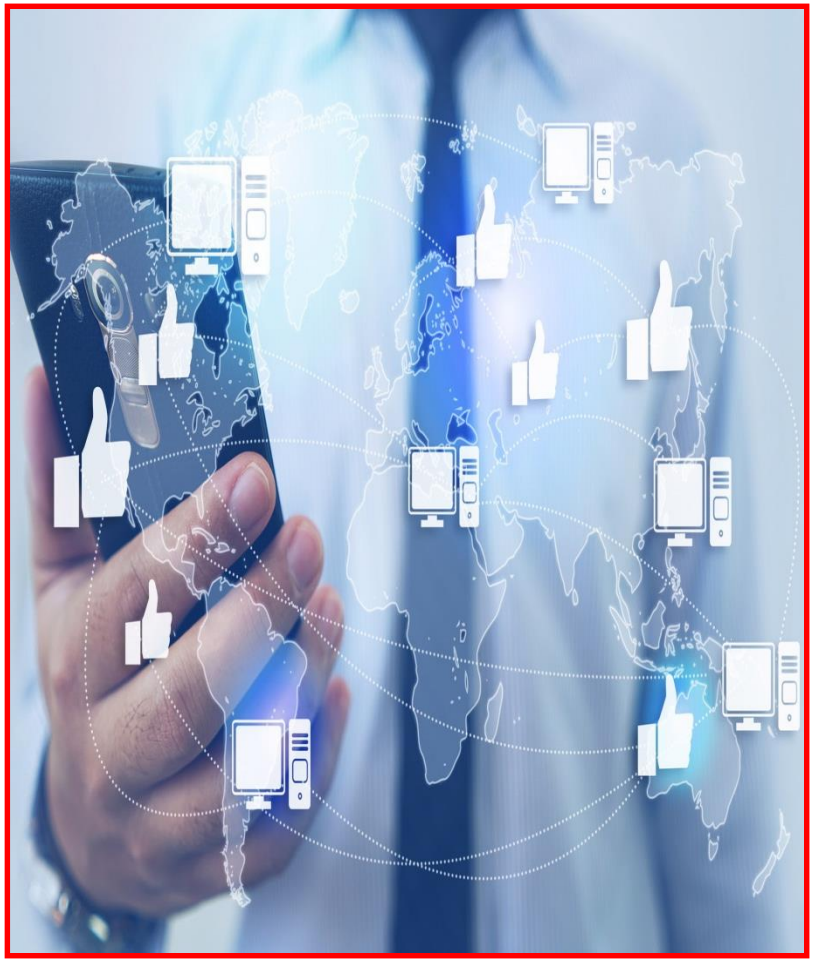
Why is it an emerging trend?

- Potential headline making issue (just ask Marriot and Yahoo)
- Complex legal landscape
- Consequences can be significant
  - Inability to use target's data assets as desired
  - Loss in value of acquired assets
  - Civil and criminal sanctions, fines, and penalties
  - Significant potential reputational harm

Consequences – Facebook

FTC to Facebook & WhatsApp: "The FTC has made clear that, absent affirmative express consent by a consumer, a company cannot use data in a manner that is materially inconsistent with promises made at the time the data was collected, and that such use of data could be an unfair practice under Section 5."

"Hundreds of millions of users have entrusted their personal information to WhatsApp. The FTC staff will continue to monitor the companies' practices to ensure that Facebook and WhatsApp honor the promises they have made to those users."



Cybersecurity Issues Can Take a Long Time to Manifest…

Hackers Spend Over 200 Days Inside Systems Before Discovery ...

https://www.info**security**-magazine.com/news/hackers-spend-over-200-days-inside/ ▼

Feb 24, 2015 - ... drop in average detection time but plenty to keep **security** teams busy. ... when they've been **breached**, despite the average time taken to **detect** an ... firms hoping adoption **will** make them less attractive to cyber-criminals.

Client Vision for Transaction

- Client needs to understand how it intends to use target's data assets
- Client needs to understand what it intends to do with target's IT assets
- Attorney needs to become steeped in target's data assets, legal obligations, IT systems and operations

Privacy and Security Diligence

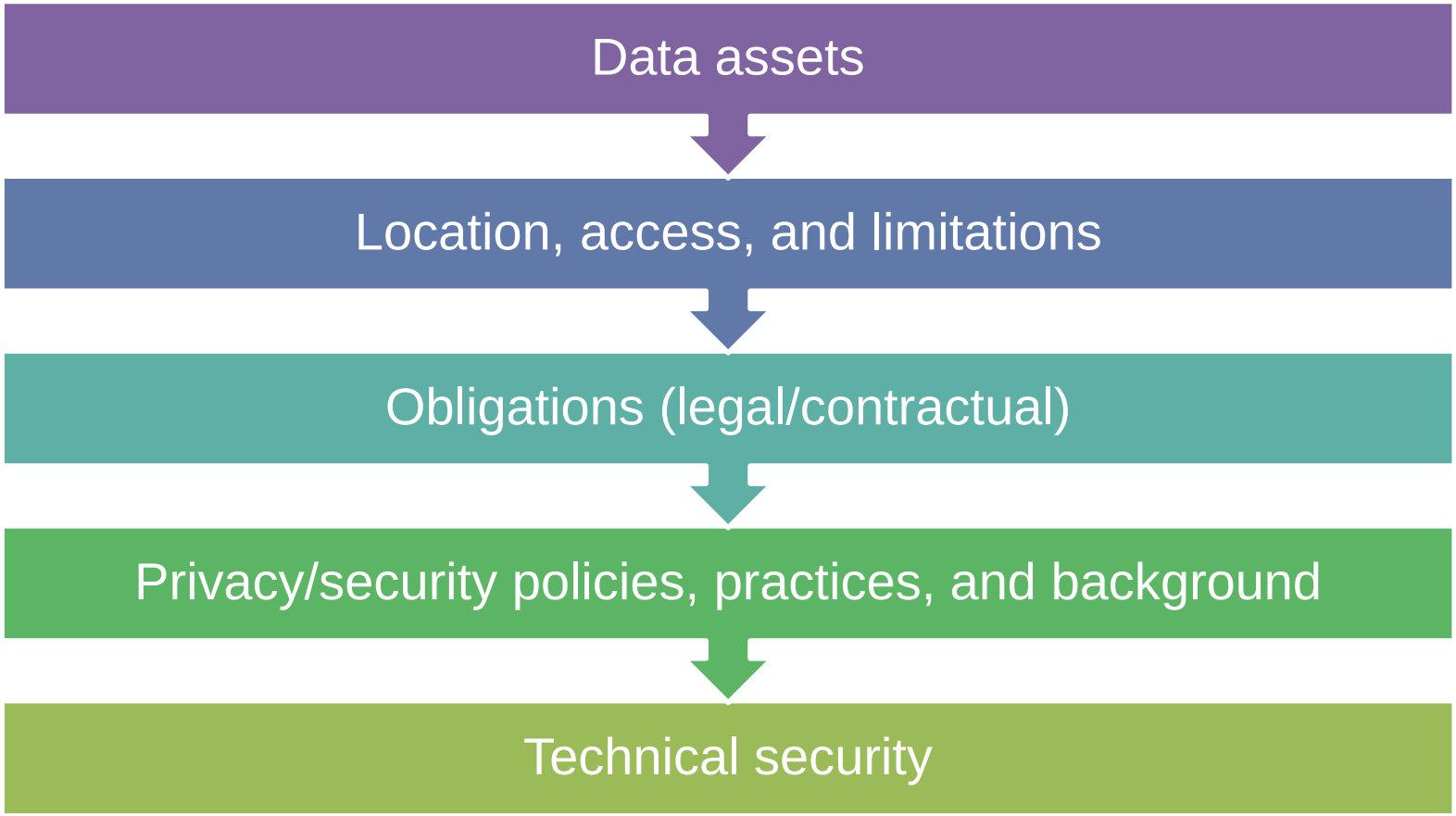
Diligence Goals/Purpose

- Identify limitations on ability to transfer/use target's data assets
- Reveal hidden/uncertain liabilities based on past failures to comply
- Determine hidden costs for integration of operations

Legal Diligence—General Considerations

- Incorporate data privacy and security questions into your larger diligence checklist
- Different ways to approach this
- See Sample checklist questions: Starts with identifying types and sources of PII that Company accesses and controls then tries to identify applicable regulations/requirements

Analytical Framework



Data Assets

- What are the categories of key data assets? Sensitive data assets?
- How are they used by the company?
- What is the source? How are they collected?

Location and Storage

- Geographic locations?
- Hosted or onsite?
- Specific IT architecture?

Access and Access Limitations

- Groups/individuals w/in company
- Vendors
- Clients
- Affiliates/partners
- Limitations on access via IT systems, policies, and procedures

Obligations Re: Data Assets

- Applicable legal obligations
- Contractual commitments
- Privacy Policies (external)
- Vendor commitments
- Compliance with obligations

Privacy/Security Policies & Practices

- Written info security program
- Specific policies
- Incident response
- Training
- Testing
- Certifications
- Prior incidents

Technical Security

- IT system security architecture
- Product security (if relevant)
- Frequently conducted by third party
- Dependent on what buyer intends to do with IT systems

What are we looking for?

Limitations on the ability to transfer/use data assets – obligations and promises to data subjects

- *In re Toysmart.com, LLC*
- FTC request for injunctive and declaratory relief in federal district to prevent the sale of PII collected on the toysmart.com website in violation of Section 5 of the FTC Act and of its own privacy policy*:*
  - "Personal information, voluntarily submitted by visitors to our site, such as name, address, billing information and shopping preferences, is never shared with a third party."
  - "When you register with toysmart.com, you can rest assured that your information will never be shared with a third party."
  - End result: Settlement agreement – Toysmart prohibited from selling customer lists as a stand-alone asset. A "qualified" buyer must be in a related market and willing to abide by terms of the privacy policy. No changes allowed regarding previously collected data unless consumers consent ("opt-in") to the new uses

What are we looking for (cont'd)?

- Hidden/Uncertain Liabilities
  - Gov't investigations/regulatory actions; fines and consent decrees
  - Private causes of action; other remediation
  - Contract breaches
  - Loss of certifications

What are we looking for (cont'd)?

- Hidden Costs—integration-related, costs of monitoring/fixing vulnerabilities
  - Significant costs to update programs
  - Gaps discovered in technical diligence (under privilege if possible)
    - Example: Presence of malware- *Are they in an industry where state-sponsored actors are likely to be active*?
    - Example: Product security design flaws or implementation gaps
  - The target relies heavily on 3rd parties for IT-related support
    - but has done no diligence, has no contractual protections

Mitigating Risk in the Deal

Mitigation Strategies

- Representations and warranties
- Indemnification
- Representation and warranty insurance

Reps and Warranties Strategies (buyer)

Privacy and Security R&W should be:

- Tailored to the deal
- Stand-alone or as part of regulatory compliance reps (versus buried in IP reps)
- “Fundamental” or otherwise have a longer survival period (in which buyer can sue for a pre-closing breach)
- Have higher limitation of liability for breaches

Reps and Warranties

- Target's information technology systems operate properly, have safeguards to protect confidentiality and security of information held and managed
- Target's products and services (and websites) comply with its privacy policies and applicable laws
- Transaction will not violate applicable laws
- Buyer will be able to use data assets in same manner as seller.
- All necessary consents obtained for sale/use of personal information.
- Existence of and compliance with security measures and programs
- Existence of and compliance with privacy policies and disclosures
- Absence of complaints, litigation, or investigations
- Absence of security breaches

Indemnification

- Indemnification flows from reps and warranties (for pre-closing breaches) - basis for post-closing issues
- Require additional stand-alone indemnity for any risks identified in diligence
- Negotiate separate/higher caps on indemnification
- Negotiate lower deductible/tipping basket
- Consider holdbacks from purchase price

Addressing Breaches Between Execution and Closing

Example – Yahoo/Verizon

Top stories

Yahoo salvages Verizon deal by giving Verizon a $350-million discount

Los Angeles Times · 3 hours ago

Verizon and Yahoo agree $350m price cut

BBC · 6 hours ago

Verizon Will Pay $350 Million Less for Yahoo

The New York Times · 34 mins ...

Discovery of Breach – Seller's Reaction

Seller will be:

- Balancing need for certainty and full information re: magnitude of problem against duty to report to buyer and regulators and notice obligations
- Assessing impact on timeline for financing and closing
- Assessing impact of damages
- Engaging counsel – covering communications by privilege
- Notifying cyber insurance carriers

Discovery of Breach – Buyer's Reaction

Buyer will be:

- Validating that communication is under privilege
- Asserting that data breach may = MAE. Difficult argument but leverage to negotiate down price and other mitigation remedies
- Assessing scope and impact of potential losses and damages
- Assessing impact on intended integration and staffing

Post-Closing Remediation

Remediation/Integration Post Acquisition

- Make strategic decisions re: data integration
- Update policies/practices
- Address customer issues
- Conduct training
- Review/renegotiate vendor contracts

Questions?

Contact Info

Brett Roberts
515-242-8918
broberts@fredlaw.com

Sten Hoidal
612-492-7334
shoidal@fredlaw.com