Nelson Mullins and Atlanta Braves Go Deep on Data

Baseball is a game built on numbers, and the ACC Georgia Chapter's annual Atlanta Braves outing at the new SunTrust Park demonstrated to in-house counsel the volume and value of business data for the Braves, like that of any company. More than 60 people attended the August 9 CLE panel discussion, sponsored by Nelson Mullins, that highlighted the importance of implementing good practices for managing customer information.

Following an introduction by Michael Hollingsworth, managing partner of Nelson Mullins' Atlanta office, Greg Heller, executive vice president and chief legal officer of the Atlanta Braves, provided a snapshot of the ballpark and its surrounding mixed-used development, The Battery Atlanta. Heller said Braves' game attendance is up over 35 percent from last year. SunTrust Park features more premium clubs, and the Braves have 122 corporate partners, the most in team history.

"Be prepared for the worst. You don't want to have to call around in the middle of a crisis."

Joanne Patterson, general counsel for Another Broken Egg Café

The Battery Atlanta's office buildings are at full capacity, with tenants such as Comcast, Dickey Broadcasting and CA South, while 80 percent of residential units and 70 percent of retail space have been leased. The Coca-Cola Roxy Theatre opened in April, and the Omni Hotel opens later this year.

With all this activity, data may be generated and collected everywhere – from ticket buyers, corporate partners, merchandise, concessions, marketing partners, retail tenants, residents, office tenants, community affairs and special events. Dealing with data comes with risks and responsibilities, however. From a legal perspective, Heller said he is concerned about the terms under which data are collected and how customers are informed.

All businesses collect customer data. Leveraging customer data for business purposes requires thought, foresight and planning. During this session, the Nelson Mullins team of partners David Katz and Brad Rustin and associate Bess Hinson outlined the legal and regulatory requirements for the collection, processing, sale, transfer and use of customer data.

Katz emphasized the significance of data as a business asset and how its value is growing continuously. For this reason, he said data due diligence in M&A deals should be a priority. Hinson discussed risks related to a patchwork of privacy laws, which vary significantly from state to state. She provided a roadmap for peace of mind based on robust privacy policies and guidelines for third-party vendors. Rustin focused on new technologies, such as mobile payments, that are changing how businesses collect and store data. He said this may subject an otherwise unsuspecting business to new legal risks, new security obligations and disclosure/consent obligations.

The Nelson Mullins attorneys were joined by Joanne Patterson, general counsel for Another Broken Egg Café, who offered the in-house perspective and shared her incident response plan. "Be prepared for the worst," she said, speaking from previous experience with data breaches. "You don't want to have to call around in the middle of a crisis."

After the 1-1/2-hour CLE panel, which was organized by Nelson Mullins marketing specialist Courtney Maass, attendees continued the conversation over drinks and a dinner buffet at Below the Chop, one of SunTrust Park's hospitality areas. The venue provided a ground-level view along the warning track in right field as the Atlanta Braves took on the Philadelphia Phillies. While the home team did not triumph, attendees found plenty to enjoy at the new home of the Braves.

Make Data Due Diligence a Priority in Merger & Acquisitions

By David Katz, Partner
Nelson Mullins Riley & Scarborough

Due diligence in the context of mergers and acquisitions can be compared to a Sherlock Holmes style exercise. Through careful analysis and the gathering of fractured pieces and bits of information one can form a colorful mosaic that ultimately reveals the landscape that will define the core risk issues in the transaction.

The birth of big data, internet of things, ubiquitous data collection and monetization of data places privacy and data security toward the top of the due diligence list. Consumer data, employee data and intellectual property are valuable corporate assets, and failure to maintain strong controls around the protection of data can create potential exposures that could have bearing on the value of the company.

Unfortunately, a company may not be familiar with the data it has collected and where it is stored, especially if the company has relied on third-party vendors for data collection and storage.

Key Privacy and Security Diligence Requests

The ways data are collected, processed, transferred, stored, retained and ultimately destroyed must be fully understood as part of the due diligence process. Consider these key requests in an M&A deal:

1. Descriptions of the security controls in place for each of the company's data collection platforms.
2. All third-party vendor agreements and copies of any of the vendors' data security protocols or requirements.
3. Copies of all documented information governance guidelines and standards, including information governance categories, retention and destruction requirements for each classification.
4. Summaries of the company's risk assessment and risk management programs, including copies of any reports issued in the last five years.
5. Copies of all security guidelines for hiring personnel, including whether credit checks, background checks, drug tests and/or other screening procedures were performed.
6. Copies of the company's privacy policies. Indicate whether such policies have been endorsed by management, have consequences for violations or undergo an annual risk assessment process.
7. Description of the company's IT business continuity plan, including a description of any testing.
8. Copies of any documented physical security guidelines to ensure security of any buildings, data centers, computer rooms and critical computer infrastructure.
9. Details (including insurer, insured party, agent, policy holder, certificates, expiration dates, exclusions and limits) of each insurance policy relating to an entity.
10. Descriptions of any known event that could give rise to insurance claims as a result of a privacy or information security incident or data breach.
11. Information on claims history involving privacy, information security or data breaches for the past five years.

The responses to these requests will provide M&A counsel with a diagnostic picture of the overall data health of the entities subject to acquisition or merger. By collecting this information, the M&A team will have a baseline understanding of the potential vulnerabilities present in the data environment, will be able to communicate the risks to the client and will be able to develop a potential plan for remediation of the data environment post acquisition.

David Katz is a partner in Nelson Mullins Riley & Scarborough's Atlanta office where he leads the Privacy and Information Security Practice Group.