



# Big Data in the Retail Industry

Today's retail industry has evolved into a multi-channel shopping experience. The collection of data through new inputs—from online tracking to video analytics to mobile location tracking—makes it possible for retailers to glean deep insights about customers and prospects, and to reach them with targeted offers based on their likely affinity for specific products. And Big Data has many other applications, such as prediction of demand and optimization of inventory. At the same time, collection, analysis and monetization of Big Data present a multitude of legal and other challenges for retailers.

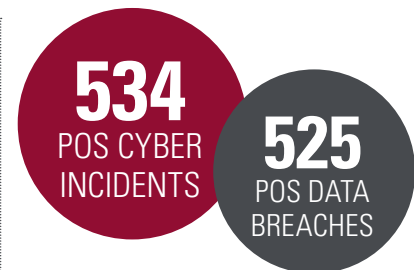
## PRACTICE AT A GLANCE

- WilmerHale's Big Data Practice helps retail clients navigate regulatory and policy issues, privacy concerns, cybersecurity risks, data ownership issues, complex technology transactions and licensing, thorny IP applications and registrations, and disputes about who owns the algorithms, devices and data inputs that power insights about consumers and prospective customers.
- We have helped some of the world's most prominent retail brands overcome highly public missteps with respect to Big Data, including perhaps the largest and most widely reported data breach. And we have assisted many other retailers in avoiding such pitfalls.

## INDUSTRY-SPECIFIC ISSUES

**Privacy:** Retailers have access to customer data both directly and through a wide variety of third-party sources, from online browsing data to in-store video and precise mobile locational data. The collection, use and sharing of such data implicate many facets of privacy law, as does the re-use of data to optimize sales and marketing.

**Data security:** Due to the large amounts of data that retailers collect about their customers (including sensitive data such as credit card information and home addresses), retailers have become a frequent target of malicious cyberattacks. Effective and legally compliant cybersecurity policies and procedures are therefore essential.



**In 2015, there were 534 cyber incidents involving POS alone in the retail industry.**

**525 of those POS breaches resulted in the unintended disclosure of sensitive information.**

**64% of all data disclosures stemmed from POS-centric attacks.**

— Verizon 2016 Data Breach  
Investigations Report

## INDUSTRY-SPECIFIC ISSUES *continued*

**Government investigations and public relations:** When data breaches or privacy violations do occur in the retail sector, they often garner attention from enforcement agencies, such as the Federal Trade Commission and state attorneys general in the United States and the various data protection authorities in Europe. Moreover, Congress frequently holds hearings on high-profile breaches. Such incidents also give rise to very thorny public relations problems.

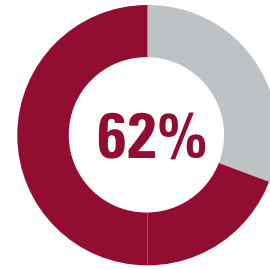
**Intellectual property:** The retail industry faces important intellectual property questions concerning the patentability of algorithms, and other methods of analyzing Big Data, as well as devices, and equipment and systems used for the collection and storage of big data in the retail environment.

**Contracts:** Retailers provide a great deal of data to, and receive a great deal of data from, third parties. Their contracts must account for their Big Data practices, including issues of ownership and licensing provisions, sharing insights and data with third parties, and apportionment of liability.

## EXPERIENCE

- Assist retail clients in collecting data directly from consumers and third parties to obtain a 360-degree view of their customers and to develop “look-alike” audiences of consumers who are not yet customers, but to whom our clients can target offers.
- Negotiate data collection, use and sharing agreements for retailers and their vendors.
- Help retail sector clients develop and deploy in-depth analytics and targeted marketing solutions while respecting consumers’ privacy, providing for appropriate data security, and complying with regulatory limitations around the globe.
- Counsel a wide variety of parties that provide services to retailers, such as online advertising companies that “on-board” in-store and transaction data and enable retailers to reach their customers and similar consumers online; vendors that analyze video footage and in-store traffic patterns to provide insights about store visitors, the efficiency of traffic flows, and the optimization of store layouts; data security firms; and many more.
- Assist retailers and others in developing mobile applications and complying with domestic and foreign laws governing the processing of data collected through mobile devices, as well as the combination of such information with in-store and online transaction data, loyalty card data, information from retailers’ and customers’ social media accounts, and data from retailers’ own CRM databases.
- Represented several prominent retail clients on data breaches, including both point-of-sale and website breaches. Such work includes breach investigation and analysis, crisis management, communication with the client’s board of directors, drafting and sending letters to consumers, and interfacing with regulators.

FOR MORE INFORMATION: visit us at [wilmerhale.com/big-data](http://wilmerhale.com/big-data) | contact us at [big.data@wilmerhale.com](mailto:big.data@wilmerhale.com)



**Retailers report that the use of information (including Big Data) and analytics is creating a competitive advantage for their organizations, compared with 63% of cross-industry respondents.**

— IBM



**Compromising the computers and servers that run POS applications is still proving fruitful for attackers seeking payment card data. These attacks are a significant threat in retail and accounted for 32% of all incidents and 64% of breaches, where data was stolen, in 2015.**

— Verizon 2016 Data Breach Investigations Report