LAWYER LIT

Business and Commercial Litigation in Federal Courts (4th Ed.); Edited by Robert L. Haig

Book Review by John P. McEntee

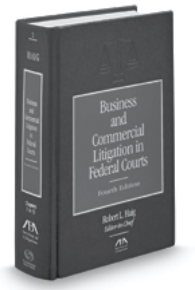
The evolution in legal research methodology can be viewed from a variety of perspectives. For me, it is reflected in office space allocation.

Fifteen years ago, to write a brief, I could escape to my firm's library, avoiding telephone calls, emails, people looking for my time sheets, and other distractions while seated at one of a number of large oak tables nestled among rows and rows of regional, federal, and state reporters. If I needed help locating a resource, I could turn to our librarian for assistance.

Ten years ago, our librarian retired, the regional reporters were introduced to their new home in a landfill, and the accounting department, sensing an opportunity, effected a hostile takeover of a large portion of the library.

This month, as we move into new office space, our library is gone, replaced with the functional equivalent of several walk-in closets with treatises grouped by practice area. This development is a recognition that briefs are not written in libraries but in individual offices where, with the insertion of a laptop into a docking station, vast amounts of primary and secondary research materials are available at one's fingertips through LEXIS and Westlaw.

And so, in this era of research by Boolean search term, what will become of legal treatises? For me, as I prepare for our office move, this question is more practical than rhetorical. Like Andy in *Toy Story*, I am packing the treatises I plan to take to my new office while depositing those that did not make the cut into the capacious dumpsters lining our office hallways.



Business and Commercial Litigation in Federal Courts (4th Ed.);
Editor: Robert L. Haig
Thompson West
2017
List price: $116

Among the treatises I am packing are two multi-volume treatises: *Commercial Litigation in New York State Courts* and *Business and Commercial Litigation in Federal Courts*. Edited by noted commercial litigator Robert L. Haig, the treatises are a staple for anyone practicing commercial litigation in New York.

The Fourth Edition of *Business and Commercial Litigation in Federal Courts* has just been released, expanding from eleven to fifteen volumes. There are chapters on subjects one would expect from any treatise on federal practice, such as Subject Matter Jurisdiction; The Complaint; Responses to Complaints; Removal to Federal Court; Third Party Practice; Joinder, Consolidation, and Severance; and Provisional Remedies. There are also chapters on Discovery Strategy and Privilege; Motion Practice; Depositions; Interrogatories; Magistrate Judges and Special Masters; and Selection of Experts and Expert Disclosure. In many of these chapters there is practical advice not found in other treatises, such as tactical considerations in trying to foil or to effectuate the removal of an action from state to federal court.

The treatise distinguishes itself from similar resources in at least two ways. First, it provides practical advice on all aspects of federal trials, with chapters on topics such as Motions in Limine; Jury Selection; Trial Strategy and Advocacy; Opening Statements; Presentation of the Case in Chief; Cross-Examination; Evidence; and Final Arguments. This grouping includes a chapter on Litigation Technology by David Boies, who discusses the use of trial aids such as ELMO document cameras and LCD projectors as well as the admissibility of computer-generated exhibits, demonstratives, and displays, including computer-generated simulations and animations.

Second, there are seven volumes addressing a broad variety of substantive areas of law. These volumes include chapters on common federal practice areas such as: Antitrust; Securities; Admiralty; Patents; Trademark; Copyright; and ERISA; and chapters on less common federal practice areas such as: Alien Tort Statute; Torture Victim Protection Act; and Foreign Corrupt Practices Act.

The Fourth Edition adds twenty-five new chapters to the treatise, addressing topics both new (Social Media) and not-so-new (Declaratory Judgments). Some of the chapters will be helpful to practitioners generally, such as those on Mediation and Arbitration, while others may be of particular help to those with niche practice areas (Fashion and Retail). For many of us, the new chapter topic on Cross-Border Litigation will have limited utility unless it can be applied to the Nassau-Suffolk border.

The Fourth Edition of *Business and Commercial Litigation in Federal Courts* may not stretch "to infinity and beyond" to answer every conceivable question you may encounter in federal practice. But, its depth and breadth of coverage on both procedural and substantive topics will allow you to become a more knowledgeable and efficient federal practitioner.

John McEntee, a commercial litigation partner at Farrell Fritz, P.C., is the Association's Immediate Past President and the Vice-Chair of the Commercial Litigation Committee.

BREACHES ...

Continued From Page 6

stance, OCR recently announced a $2.2 million settlement with MAPFRE Life Insurance Company of Puerto Rico (MAPFRE) based on the impermissible disclosure of unsecured electronic protected health information (ePHI) as well as Social Security numbers.[10] MAPFRE filed a timely breach report with OCR indicating that a USB storage device containing ePHI was stolen.[11] However, after MAPFRE filed the report an OCR investigation revealed that MAPFRE did not conduct a risk analysis and failed to implement corrective measures.[12] The size of the settlement is due to the fact that OCR uncovered that MAPFRE made misrepresentations to OCR, including that it had conducted a risk analysis and implemented risk management plans and MAPFRE failed to execute a security awareness and training program, failed to implement encryption and failed to execute reasonable and suitable policies and procedures. [13] In sum, whether an organization is untimely with regard to its cybersecurity breach notification obligations or fails to take corrective actions, the costs and liabilities are extensive.

How to Mitigate Costs and Liabilities

The best and most succinct guidance concerning how to organize and respond to a data breach is provided by the Federal Trade Commission (FTC).[14] The first step for any organization to deal with a data breach is to secure operations and assemble a team of experts. There is no doubt that cybersecurity overall is both a legal and a technical issue and, thus, the team must include outside cybersecurity counsel (counsel with specific experience in this particular field), which will retain technical resources to do a forensics investigation and remediate systems. Notwithstanding the need for experienced cybersecurity counsel to determine the legal requirement to notify and avoid the severe penalties associated with a delay as outlined above, cybersecurity counsel can also mitigate an organization's litigation liabilities to the extent possible by shielding findings and communications between the technical experts, team members and the organization under attorney-client privilege.[15]

After retaining a team of experts, the experts must begin securing the system and fixing vulnerabilities. Securing the system includes preventing additional data loss and further attacks.[16] Once secure, an organization should begin to examine relationships with service providers, conduct risk assessments and develop a communication plan.[17] As demonstrated above in the MAPFRE matter, it is essential that an organization can accurately represent that it has remediated its systems, implemented corrective actions and is in compliance with applicable regulations.

As indicated, cybersecurity counsel will analyze the applicable state and federal laws and regulations based upon the circumstances and determine the notification trigger date as well as the appropriate individuals, businesses, authorities and entities to notify. This requires a detailed analysis given that obligations are dependent upon the residency of the affected individual, the specific elements of data, the number of affected individuals and the respective organization's industry. For instance, obligations vary widely depending on whether the data at issue involves Social Security numbers or credit card numbers and security code or PHI, or combinations thereof. Given the aforementioned severe penalties and increased scrutiny with timely reporting and notifications, it is critical that state and federal obligations are analyzed thoroughly and a plan to communicate and comply is initiated.

Organization and Promptness is Key

The rapid increase in frequency of cyberattacks and the associated surge in regulatory enforcements, private party class actions, as well as state and federal government investigations, means that cybersecurity and data protection should be a top priority for organizations across all industries. Implementing an organized approach and avoiding unnecessary delays will ensure that an organization can concentrate on the data breach and the respective business ramifications and not worry about the aforementioned severe penalties and liabilities associated with delays and disorganization.

John J. Cooney, Esq. is a partner at Ruskin Moscou Faltischek and chair of the Firm's Cybersecurity and Data Privacy practice group. His e-mail is jcooney@rmfpc.com.

Nicole Della Ragione, Esq. is an associate at the firm and a member of its Cybersecurity and Data Privacy practice group. Her e-mail is ndellaragione@rmfpc.com.

1. Information Security Breach and Notification Act, N.Y. Gen. Bus. L. §899-aa(1)(c) (2005).
2. *First HIPAA enforcement action for lack of timely breach notification settles for $475,000,* U.S. Dep't Health and Hum. Serv. (Jan. 09, 2017), http://wayback.archive-it.org/3926/20170127111957/https://www.hhs.gov/about/news/2017/01/09/first-hipaa-enforcement-action-lack-timely-breach-notification-settles-475000.html.
3. *First HIPAA enforcement action for lack of timely breach notification settles for $475,000, supra* note 2.
4. *Id.*
5. *Id.*
6. James Swann, *Delayed Breach Notice Costs Illinois Health Systems,* 16 Privacy & Security L. Rep. (BNA) No. 126 (Jan. 16, 2017).
7. Cybersecurity Requirements for Financial Services Companies, 23 N.Y.C.R.R. Pt. 500.21 (2016).
8. 23 N.Y.C.R.R. § 500.17.
9. Fla. Stat. § 501.171(9)(a) (2016).
10. *HIPAA settlement demonstrates importance of implementing safeguards for ePHI,* U.S. Dep't Health and Hum. Serv. (Jan. 18, 2017), http://wayback.archive-it.org/3926/20170127111936/https://www.hhs.gov/about/news/2017/01/18/hipaa-settlement-demonstrates-importance-implementing-safeguards-ephi.html.
11. *HIPAA settlement demonstrates importance of implementing safeguards for ePHI, supra* note 10.
12. *Id.*
13. James Swann, *Stolen Storage Device Leads to $2.2M Settlement for Insurer,* 16 Privacy & Security L. Rep. (BNA) No. 195 (Jan. 30, 2017).
14. *Data Breach Response: A Guide for Business,* Fed. Trade Comm'n (Sept. 2016), https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business.
15. *In re: Target Corporation Customer Data Security Breach Litigation,* MDL No. 14-2522 (Oct. 23, 2015).
16. *Data Breach Response: A Guide for Business,* supra note 14 at 1-2.
17. *Id.* at 3.