PREFACE

Nearly every organization maintains files and systems filled with personally identifiable information: employee information, existing and prospective customer information, and data gathered as a product to sell to others. The list is almost limitless. In this electronic age, personal information is a vital commodity for organizations as they strive to help ensure customer satisfaction, provide employee benefits, drive purchases, counter fraud, and, in general, run their businesses. Unfortunately, personally identifiable information also has become a tool for criminals who prey on organizations with lax safeguards to commit fraud, identity theft, and other acts injurious to consumers.

In response, regulators and industries have crafted requirements and recommended protocols designed to protect personal information within the organization’s control, and to establish an organization’s obligations when it discovers that such personal information has been compromised. These obligations affect the entire business; yet the responsibilities associated with protecting an organization’s personal information often are categorized as a purely technical matter with little interplay between executive management, legal counsel, information technology support, and other key employees. That lack of communication and business-wide appreciation for data security has left many organizations vulnerable to data compromise, legal liability, negative publicity, and associated brand tarnishment. Data security practices also have become relevant for those businesses considering a merger or acquisition: parties need to ensure that their proposed partner complies with all relevant laws and regulations and has a secure data security system in place.

The purpose of this Handbook is to provide legal practitioners and information technology specialists with a concise, practical guide that summarizes (1) common information security vulnerabilities and how to manage them; (2) legal and industry information security safeguard requirements and recommended practices; (3) the legal obligations that apply when an organization has incurred a data breach; (4) factors that contribute to a compliant information security program; and (5) potential legal theories in actions involving the alleged misuse or compromise of personal information.

A great deal of time, effort, and research went into the preparation of this Handbook. First and foremost, I am gratefully indebted to Alysa Zeltzer Hutnik for her tireless work as Project Chair for this Handbook. The countless hours, careful attention to detail, patience, and insight devoted by Alysa led this project to its fruition and, quite simply, the
Handbook would not exist today without her leadership. I also gratefully acknowledge the comments and suggestions provided by Kathryn M. Fenton, Leslie C. Overton, John E. Villafranco, and Keith D. Shugarman, as well as the contributions of the following people:

- Martin Abrams
- Jennifer Armstrong
- Lisa Branco
- Thomas Daemen
- D. Reed Freeman, Jr.
- Christian S. Genetski
- Kristen J. Mathews
- Natalie Newman
- Jennifer Ngai
- Edward J. Palmieri
- W. Joseph Price
- David Rosen
- Aaron Simpson
- Peter Scher
- Lisa Sotto
- J. Andrew Valentine

The Handbook also was extensively reviewed by Books and Treatises Committee members Svetlana S. Gans and Robin L. Moore. Finally, we could not have met the deadline for publication of this Handbook without the support of the staff at Kelley Drye & Warren.

February 2008

Thomas F. Zych
Chair
Privacy and Information Security Committee
Section of Antitrust Law
American Bar Association
2007-08