Preface

I wrote this book because it was the book I wanted to read. Amid all the discussions in the legal world and broader world of privacy and data security—the hottest of hot topics these days—it seemed there was a need for a resource focused specifically on how these subjects intersect with financial services. The goal was not to create an exhaustive treatise compiling every case and interpretation of every single law and regulation—which would carry the certainty of being immediately outdated upon publication. Instead, my goal was to create a practical, digestible guide to help make sense of it all.

Those of us who have spent our careers in the banking world may remember, with nostalgia, a time when it seemed data protection laws touched us only in narrow ways—mostly via the federal Gramm–Leach–Bliley Act (GLBA), Fair Credit Reporting Act (FCRA), and Right to Financial Privacy Act (RFPA). Otherwise, we seemed somewhat isolated from the data protection frameworks that affected other sectors. This was never completely true—financial institutions were always subject to other laws with relevance to data protection—but it is becoming even less true as the world moves toward more comprehensive data protection laws and also more comprehensive risk considerations. Regulators are addressing data protection through broader laws under their enforcement authority, not only through data protection laws. And whether or not a law exempts banks, credit unions, or others—or mentions privacy or data security explicitly—we are all subject to the same concerns about reputation risk and client-relations issues as anyone else—and even more so as financial entities hold such sensitive information that is important to the entity itself and even the larger economy, not only to individuals.

My audience is, particularly, in-house or outside counsel advising financial services entities and service providers to those entities. The ability to advise these clients on data protection is not simply a matter of memorizing or understanding the requirements of a law but also how multiple laws—and risk considerations—intersect and may be at odds. For instance, it is important to understand the tension between the principle of data minimization—collecting, using, and retaining only the minimum information needed—and the need to collect and use certain information that is sometimes required or encouraged by laws specific to financial services.

And understanding the intricacies of this interplay is still not enough; one must understand programmatic and operational matters to be able to successfully

implement compliance and manage risk. In fact, despite the rise of new laws and regulations, and of new threats to security, it is not those external developments that pose the most risk. Instead, often the most significant risks come from inside the house: failure to structure and operate mechanisms in ways that support compliance and risk management. This could happen, for instance, through failure to coordinate among the right stakeholders within an entity or across legal entities in a bank holding company or other corporate family. It could also happen through inadequate third-party risk management, evidenced by insufficient attention to due diligence or vital contract provisions, lack of awareness of subcontractor relationships, or lack of ongoing oversight of a vendor. Lawyers will find themselves advising on challenges like these as well, because data protection risk management is not simply a matter of reciting the basic requirements of laws; the practical import of how to implement them, and identify and manage risks, is where it all comes together.

This book is arranged to provide a lay of the land as to the major laws and regulations in this space, and, where appropriate, historical context of the issue at hand to understand its evolution. Chapters 1 to 4 give an overview of the landscape and of the major federal laws in this space—GLBA, FCRA, and RFPA—as well as relevant state analogues. The book then discusses other data protection laws and general consumer protection laws that can have relevance to financial privacy and data security. Chapter 7 addresses laws, regulations, and risk considerations relevant to incident response—what happens before, during, and after a data breach. Chapter 8 addresses industry standards and initiatives, which can be helpful sources for best practices, information sharing, and peer benchmarking, and in some cases have been leveraged into legal requirements.

So, all in all, the goal is to orient the reader as to where we are, provide some context of where we have been, and look to where we might be going, to be able to knowledgeably advise clients along the way. I hope that you will find this book a useful and practical resource.