DATA SECURITY BREACHES:
INCIDENT PREPAREDNESS AND RESPONSE

Washington Legal Foundation
MONOGRAPH

In response to a recent survey asking corporate board members and general counsel, "What keeps you up at night?," data security was second only to succession planning for board members and to regulatory compliance for general counsel. This is not surprising, given the high financial and reputational costs data breaches impose on businesses, in addition to the attendant regulatory exposures and liability. With the ever-increasing number and sophistication of cyber-criminals, it now is not a question of *if*, but *when* a business will have to confront a serious data security problem.

A Washington Legal Foundation (WLF) MONOGRAPH provides in-house counsel and other key personnel a concise, plain-language guide on the continuous process of securing consumer data and readying a breach response. The MONOGRAPH's *pro bono* authors are **Jena Valdetero** and **David Zetoony**, partners with the law firm Bryan Cave LLP. It features a foreword by **Commissioner Maureen K. Ohlhausen** of the Federal Trade Commission, and an introduction by Ceridian HCM Corporate Counsel and Chief Privacy Officer **Lisa Clapes**.

Commissioner Ohlhausen notes in her foreword:

> ***Although written by lawyers, the WLF MONOGRAPH is not—to the authors' great credit—a legal treatise. Instead it is a practical guide to help in-house counsel understand security incidents and the role of in-house counsel in dealing with such incidents.***

Ms. Valdetero and Mr. Zetoony organized the guide into three main sections. **Section I** focuses on understanding the nature and scope of data events, incidents, and breaches. As the authors explain, these three concepts are often lumped together into the general term "data breach," but each has a distinct meaning and the differences can be critical for planning, response, and legal compliance.

Section II discusses preparations for a data security breach. The authors explain why simply taking steps to physically protect data is no longer sufficient. This section addresses cyber-insurance, written information security programs, and incident response plans. Each sub-topic includes a valuable checklist of items that in-house counsel must consider.

Section III prepares readers for an incident response. This section delves into the four key factors organizations must consider when investigating a security incident. It also reviews how organizations should coordinate with data owners as well as

communicate with the customers, the media, and law enforcement. Such coordination and communication, the authors explain, must be done with a full understanding of the applicable laws and regulations. Even an ostensibly basic consideration, such as when and how to inform data owners and consumers of a breach, is influenced by state laws, unwritten federal standards, and reputational concerns. Section III ends with a brief discussion of unique incident response considerations for specific types of breaches: payment card breaches; breaches involving healthcare information; and those involving financial institutions.

***If you are interested in receiving a copy of the WLF MONOGRAPH* "Data Security Breaches: Incident Preparedness and Response," please email glammi@wlf.org.**