Essential Information Concerning Contracts and Information Security, Part 1 of 3: IT Outsourcing and

Information technology (“IT”) and IT management is built into every modern business transaction. Beyond managing regulations and potential liability, numerous companies outsource their IT functions to third parties, creating significant information security (“InfoSec”), privacy and legal difficulties, including loss of control and challenges with enforcement. Risk and compliance obligations do not merely disappear when using a third-party service provider – the company that outsources needs to consider what any IT management and InfoSec contract will contain. This white paper will cover breaches and remedies that companies and service providers have to consider in any IT service agreement. Failure to meet InfoSec obligations contained in a contract typically triggers material breach clauses. These material breach provisions typically give the non-breaching party the right to terminate the agreement (often immediately), compel specific performance, and/or collect damages. Breaches do not automatically excuse future performance unless they are material. The material breach section of a contract may address fundamental data safeguards such as password protecting files, encrypting databases or securing transmissions. InfoSec obligations can be complex endeavors, increasing a company’s risk of inadvertent breach. Many U.S. financial institutions contractually require their technology vendors to comply with the financial Interagency Guidelines Establishing Information Security Standards and many business concerns also choose to leverage InfoSec standards developed by certain standards-setting entities, for example ISO/IEC 27001/27002 (formerly 17799), which are international standards issued by the American National Standards Institute (ANSI) as the U.S. representative to the International Organization for Standards (ISO), and also via the U.S. National Committee to the International Electrotechnical Commission (IEC). Simple or complex, however, the cost of remediating a breach or paying damages or fines as a result of a breach can dwarf the value of the agreement. Thus, the significant financial risk associated with poor data security and privacy and related regulatory problems makes it imperative that the security, confidentiality, and integrity of information maintained by the customer be secured and not disclosed without authorization or otherwise in contravention of the terms of the agreement protecting the information. ** This is the first part in a three-part series which comprise an abridged version of the article “Thoughts on Contracts and Information Security,” written by Daniel Garrie and published in the Los Angeles Daily Journal. To request a PDF of the complete article, please contact Law & Forensics -- www.lawandforensics.com