Guide to Computer Law—Number 291

CCH GUIDE TO COMPUTER LAW

Practitioner's Perspective

by Alan S. Wernick
FSB FisherBroyles, LLP

T: 847.786.1005;
M: 847.770.1355;
E: WERNICK@FSBLEGAL.COM;
Web: WWW.FSBLEGAL.COM;
listing of articles & lectures available at WWW.WERNICK.COM.

Practitioner's Perspective appears periodically in the monthly Report Letter of the CCH Guide to Computer Law. Various practitioners provide in-depth analyses of significant issues and trends.

Illinois Consumer Data Breach Notification Law Takes Effect

By Alan S. Wernick, Esq.

Addressing the growing concerns about identity theft, the Illinois Governor on June 16, 2005, signed into law the Illinois Personal Information Protection Act ("PIPA"). This law applies to privately and publicly held corporations, retail operators, government agencies, public and private universities, financial institutions, and any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information of an Illinois resident. In essence, all organizations that use or maintain Illinois consumer personal information will be subject to this law. The law requires any such organization to promptly notify the Illinois resident in cases where their personal information has been compromised due to a breach in organization's security. A violation of this law can result in monetary, statutory, and punitive damages against the organization. The Illinois PIPA law took effect January 1, 2006.

Illinois PIPA defines "personal information" as an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

1. Social Security number.
2. Driver's license number or State identification card number.
3. Account number or credit or debit card number, or an account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. However, it would include both customer and employee personal information.

Prompt disclosure notification is mandatory as soon as the organization either discovers or is notified of a breach, or reasonably believes that the personal information may have been acquired by an unauthorized person. PIPA provides specific requirements for notification. However, this law also provides a safe-harbor provision for those organizations that, in advance of a data breach, have developed and maintain their own notification procedures as part of their information security practices for treatment of personal information, provided that such procedures are otherwise consistent with the notice timing requirements of PIPA.

Notification procedures consistent with the Illinois PIPA must be followed in the event of a breach of the security of the data subject to Illinois PIPA.

A violation of PIPA constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act. In addition to a civil right of action by an individual, business or organization, an action may be brought by the Attorney General. Remedies and damages for a violation may include, among other things, injunctive relief, actual damages, and attorney fees.

The legal and regulatory compliance landscape is rapidly evolving with numerous and often overlapping (and sometimes inconsistent) privacy and security laws and regulations. PIPA is only one of several recent privacy law regulatory developments in Illinois and other states. Organizations wanting to provide appropriate protection for their consumers' personal information and limit potential liability should become aware of these legal developments and implement a privacy and security compliance program that takes into account these legal developments and relevant best practices.

Recent studies have indicated that customers highly value how a company handles the privacy and security of the customer's personal information. Thus, these issues impact the very foundations of an organization's relationship with its customers and the public.

Perhaps now is a good time to review your organization's privacy law compliance program.