DEALING WITH SECURITY BREACH INVOLVING CONFIDENTIAL CLIENT DATA

Lawyers’ computers are sometimes lost or stolen, or their data bases are hacked into, so that confidential personal client information is vulnerable to being used for improper purposes. Lawyers have an obligation to keep client information confidential and should take reasonable steps to protect the confidentiality of client information. When a computer is lost, stolen or hacked into, the lawyer is confronted with the problem of dealing with the situation in which it is possible that some client information might be in the hands of a third party who might use it for an improper purpose, such as selling the client’s personal information. At least 46 states have statutes requiring that those who maintain the personal information of others take certain action when security breaches occur. For example, it is required that the owners of the compromised information be notified of the security breach. Some of the statutes require that those who maintain such information develop and implement security programs to protect the personal information and to use access control techniques to prevent unauthorized access to the data. It would be prudent for lawyers to read and understand the requirements of any statute in the lawyer’s jurisdiction that addresses such issues and to develop a plan to address the risk of a security breach.