KEAN | MILLER LLP
ATTORNEYS AT LAW

BUSINESS BRIEF

Is Your Company's Information "Made for Walking"?

People want to access information with the "touch of a finger." While it may not be the Midas touch which turns things to gold, this touch does quickly unlock a person's "world" that is stored on an iPad, iPhone, BlackBerry, computer, or other similar device. With a key stroke or two, phone numbers, account information, customer contacts can be "pulled up." Businesses are no different. They are storing information such as operational documents, accounting information, customer list on integrated computer systems. The metal filing cabinet is quickly becoming a thing of the past.

An important benefit is information on the computer system can be quickly accessed and utilized in operating the business. As long as the relationship between a business and its employees is good, there is no problem. However, when an employee resigns or is terminated, the business is at risk that its information just "walks out of the door" and onto the street. Prudent business practices call for this information to be safeguarded. Unlike Nancy Sinatra's boots, this data and information should not be "made for walking."

Businesses should adopt a comprehensive policy to protect key business information, documents and data. Information such as new designs, formulas, and customer lists, accounting data, and any documents which contain this information must be identified. Consideration must be given to whether the information or documents may be protected by a copyright, trade secret, or patent. Any documents containing confidential information need to be appropriately labeled so anyone accessing these documents will be on notice of their content. Moreover, information should be password protected so as to appropriately restrict access to only employees whose job responsibility requires access to them.

Employees should sign non-disclosure agreements. Periodic training should be conducted to remind employees of their obligations regarding confidential documents and information. Employees should be reminded by pop-up email or otherwise that they do not have a right of privacy in their work e-mails and that accessing a computer without authorization may be a violation of the Computer Fraud and Abuse Act. A policy should be in place that requires the return of all business documents and electronic data when requested.

Upon the termination or resignation of an employee, an audit should be conducted to determine if the employee has in fact returned all business property, including documents, electronic data, PDAs, etc. The business should request that the employee sign a written statement certifying that he or she has in fact returned all business information without retaining a copy. Prior to department, employers should give a copy of any non-disclosure agreement to the employee to remind him or her of these obligations.

JAMES R. "SONNY" CHASTAIN
Partner
225.389.3706
sonny.chastain@keanmiller.com

It should be no surprise that former employees typically misappropriate confidential information immediately before resigning or after termination. After termination or resignation, the former employee should be watched carefully and escorted out of the facility. Thereafter, an investigation should be conducted to consider any unusual behavior of the former employee, i.e., late night or weekend access to sensitive databases, electronic information or key card building access as a potential sign that some form of misappropriation has occurred. If the business concludes any misappropriation has occurred, immediate action should be taken to limit the damages resulting from these actions.