SEYFARTH SHAW LLP
ATTORNEYS

One Minute Memo®

FTC AGGRESSIVELY ENFORCES SECURITY BREACH OF FINANCIAL AND HEALTH INFORMATION RESULTING FROM CAR BREAK IN

One of the most likely scenarios of any security breach an employer may encounter is the theft of a laptop from an employee's car or rental car. Such a theft could result in the employer being forced to send notices to employees or customers, state regulators, and (in large breaches) credit bureaus and the media. Now, the Federal Trade Commission (FTC) has made it clear that breaches of unencrypted personal data could result in enforcement action and a consent decree mandating **annual external certification of the company's security plan for 20 years.**

On January 28, the FTC announced a settlement with CBR, a leading cord blood bank, of claims that it failed to protect the security of customers' personal information, and that its inadequate security practices contributed to a breach that exposed Social Security numbers and credit and debit card numbers of nearly 300,000 consumers. The claims arose from a December 2010 security breach during which unencrypted backup tapes containing consumers' personal information, a company laptop, a company external hard drive, and a company USB drive were stolen from the employee's personal vehicle in San Francisco, California.

Continued enforcement by the FTC, in addition to the cost of responding to security incidents shows that there is a ROI on conducting your own reviews to ensure that your company has policies and procedures in place such as encrypting or limiting the personal data that can be placed on mobile devices and training employees on the importance of those policies.

By: *Bart Lazar*

Bart Lazar is a partner in Seyfarth's Chicago office. We regularly assist clients in performing such reviews and training. If you would like further information regarding our privacy and security practice, please contact your Seyfarth attorney or Bart Lazar at *blazar@seyfarth.com*.