MINTZ

Don't Shoot the Messenger: Another Court Cautions Against Retaliating Against Employees Who Report Data Security Concerns

November 29, 2010 | Blog | By **Cynthia J. Larose**

VIEWPOINT TOPICS

- Privacy & Cybersecurity

RELATED PRACTICES

RELATED INDUSTRIES

Written by Michael Arnold, Cynthia Larose and Jennifer Rubin

Recently, a California state appellate court in *Cutler v. Dike*, No. B210624, 2010 WL 3341663 (Cal. Ct. App. Aug. 26, 2010), upheld a jury finding that an employer illegally fired an employee because he objected to the manner in which his employer maintained its confidential patient information. This decision, along with a similar New Jersey federal court decision (***Zungoli v. U.P.S.*** *No. 07-2194, 2009 WL 1085440 [D.N.J. Apr. 22, 2009*]), should reinforce for employers the need to take all employee complaints of data security seriously and to avoid taking any retaliatory action against employees who voice these complaints.

Many states statutorily prohibit private sector employers from retaliating against employees who report, or refuse to participate in, employer violations of federal or state laws or regulations. Among these federal and state laws and regulations are laws requiring employers to safeguard employee, consumer, and patient information. For example, New York employers are required to develop and utilize safeguards to protect against the unauthorized access of social security numbers, while California employers are required to implement and maintain security procedures and practices that protect against unauthorized access, disclosure, and use of personal information. Federal Health Insurance Portability and Accountability Act (HIPAA) laws and regulations require covered employers to ensure the confidentiality, integrity, and availability of all electronically protected health information the employer creates, receives, maintains, or transmits, including protecting against any reasonably anticipated threats or hazards to the security or integrity of such information. As the number of identity thefts and data security breaches continues to rise, employers should expect additional state and federal laws to be passed that are designed to protect electronically stored information. As employers attempt to comply with these laws by devising adequate data protection policies and practices, they must also be careful in disciplining employees who identify flaws in their security systems that may result in violations of state or federal laws and regulations. The employer in *Cutler* was not so careful, and a jury held it liable, finding that it fired the employee because he refused to participate in, and voiced his objections to, configuring its computer system in a way that he knew could expose confidential patient information in violation of HIPAA. In *Zungoli*, the court permitted the employee to advance his whistleblowing retaliation claim to trial, where he alleged that his employer disciplined him because he voiced concerns that its computer system could compromise his and other employees' personal and confidential information in violation of New Jersey public policy and its Identify Theft Protection Act.

In response, employers should consider taking steps to avoid whistleblowing retaliation claims, including the following:

- Do not ignore employee complaints of potential or actual security breaches. Take them seriously, including conducting prompt investigations and taking corrective action if necessary.
- Create policies and procedures that will address the security of all private electronic data, including that of employees as well as customers and patients.
- Create a mechanism for employees to report potential or actual breaches without fear of any retaliation.
- Consider creating a response team that will implement and monitor data security policies and procedures, and that will promptly investigate any employee complaints.
- Train employees on how to comply with data security laws, data security policies and procedures, and complaint mechanisms.

- Train supervisory and managerial employees regarding complaint mechanism procedures, how to recognize potential whistleblowing activity, and how to recognize and avoid engaging in retaliatory behavior.
- Tread carefully before taking any adverse personnel action against an employee who raises security concerns. Seek assistance from legal counsel and/or human resources before disciplining an employee for making such complaints.

Authors

Cynthia J. Larose, Member / Co-chair, Privacy & Cybersecurity Practice

Cynthia J. Larose is Chair of the firm's Privacy & Cybersecurity Practice, a Certified Information Privacy Professional-US (CIPP-US), and a Certified Information Privacy Professional-Europe (CIPP-E). She works with clients in various industries to develop comprehensive information security programs on the front end, and provides timely counsel when it becomes necessary to respond to a data breach.