PALEY ROTHMAN
ATTORNEYS AT LAW

Password Protected: No Passwords for Employers

The Maryland General Assembly, nearly unanimously, passed the first legislation in the nation banning employers from requesting or requiring that an employee or applicant disclose any user name, password, or other means for accessing a personal account or service. After the Governor signs the Bill, the law will go into effect on October 1, 2012. A copy of the legislation can be found here.

Under the new law, employers will be flatly prohibited from asking applicants for user names or passwords to any personal websites, such as Facebook, LinkedIn, or Twitter. Employers will also be prohibited from failing or refusing to hire an applicant who does not provide that information. There are no exceptions or exclusions for certain employers. There is no size or revenue limitation and no carve out for public employers.

Just as with applicants, employees cannot be asked for user names or passwords to personal websites or accounts. Employers cannot discipline or discharge employees, or threaten to discipline or discharge employees, who fail or refuse to provide user names and/or passwords. Here, however, there appear to be some exceptions. For example, an employer can require an employee to disclose user names, passwords, or other means of accessing non-personal accounts or services that provide access to the employer's internal computer or information systems. Additionally, employers who receive information about an employee's use of a personal website or social networking account for business purposes may conduct an investigation, including requiring an employee to provide user names and passwords, to ensure compliance with applicable securities or financial laws and regulations.

Further, employees are prohibited from downloading employer proprietary information or financial data to an employee's personal website or social networking account. An employer who learns of this type of unauthorized downloading may investigate an employee's actions, including requiring the employee to provide user names and passwords to the websites or accounts believed to have been used in the unauthorized downloading.

How this new law will interact with existing and developing law is unknown. Presently, courts and legislatures around the country are grappling with issues regarding the ownership of social networking sites and profiles. For instance, a Twitter account set up for the employer, but run by an employee, may belong to the employer when an employee's employment ends. However, a LinkedIn page may belong to the employee, depending on how it was setup and operated. Questions likely to arise are: What is a 'personal account"? Can an employer request an employee's LinkedIn password, if the account was setup at the request of the employer? When does a personal account become a non-personal account, and vice versa? Additionally, there may be some interaction between federal laws which give employees the right to discuss their wages and working conditions, with this law which bars employees from downloading employer financial data (which might include wages).

We will keep you updated as the Court's begin to weigh-in on these issues.

 | 4800 Hampden Lane, 6th Floor, Bethesda, MD 20814-2930 | 301-656-7603 | 301-654-7354 fax www.paleyrothman.com