HYATT & WEBER, P.A.
ATTORNEYS AT LAW

Legal Alert

May 3, 2012

Maryland Bars Employers From Requiring Disclosure of Social Media Passwords and Other Personal Account Information

On May 2, 2012, Governor O'Malley signed into law a bill that protects employees and applicants against mandatory disclosure of social media passwords and other personal account information. This appears to be the first law in the nation that provides such protection to employees and applicants for employment.

Section 3-712 of the Maryland Labor and Employment Code, which takes effect on October 1, 2012, states that an employer "may not request or require that an employee or applicant disclose any user name, password, or other means for accessing a personal account or service through an electronic communications device." The new law also bars other employer activity. In this regard, the law states that an employer may not "discharge, discipline, or otherwise penalize or threaten to discharge, discipline, or otherwise penalize an employee for an employee's refusal to disclose" any of the aforementioned information related to social media and other personal accounts. The law also protects applicants in this regard and prohibits employers from refusing to hire applicants who refuse to provide such information.

The statute defines "employer" as "a person engaged in a business, an industry, a profession, a trade, or other enterprise in the State" or "any unit of State or local government." The statute further defines "employer" to include "an agent, a representative, and a designee of the employer." "Applicant" is defined as "an applicant for employment."

An employer "may not request or require that an employee or applicant disclose any user name, password, or other means for accessing a personal account or service through an electronic communications device."

The statute defines "electronic communications device" as "any device that uses electronic signals to create, transmit, and receive information." "Electronic communications device" specifically includes "computers, telephones, personal digital assistants, and other similar devices."

The law is not all bad news for employers, however. The law prohibits employees from "download[ing] unauthorized employer proprietary information or financial data to an employee's personal web site, an Internet web site, a web-based account, or a similar account." The law also recognizes the need for employers to undertake certain activities to protect their information systems, proprietary information, and financial information. To this end, the law specifically permits an employer to "require an employee to disclose any user name, password, or other means for accessing nonpersonal accounts or services that provide access to the employer's internal computer or information systems."

The law also permits an employer to require disclosure of personal account information under certain circumstances. An employer may "conduct[ ] an investigation for the purpose of ensuring compliance with applicable securities or financial law, or regulatory requirements" "based on the receipt of information about the use of a personal web site, Internet web site, web-based account, or similar account by an employee for business use." In addition, the law permits an employer to conduct an investigation of an "employee's actions" concerning the statute's prohibited downloads "based on the receipt of information about the use of a personal web site, Internet web site, web-based account, or similar account by an employee for business purposes."

While the law at first glance appears relatively straight forward, some provisions may be subject to further clarification as a result of litigation. For example, what type of "information" must the employer "recei[ve]" to conduct an investigation and require disclosure of passwords and other personal account information? In addition, what information will courts deem to be "unauthorized proprietary information or financial data" that employees cannot download? Will courts require employers to specifically identify such information or will some course of conduct or other standard apply? Additionally, will individuals be held personally liable under the statute? Also, the statute does not specify what remedies are available to a claimant. These and other provisions are likely to be clarified in time after cases make their way through the court system.

This law appears to be aimed at counteracting the growing trend of employers requiring applicants and employees to disclose passwords and user names to social media accounts (such as Facebook) and other personal accounts. While it appears that Maryland employers will be somewhat more restricted than other employers when conducting due diligence on applicants and employees to determine whether they engage or have engaged in behavior that may be incompatible with the company's policies, culture, or image, it appears that Maryland employers will still be given a fair amount of latitude to protect their computer systems, proprietary information, and financial data. Although this law applies only to employers in Maryland, employers in other jurisdictions should take note, as other states are likely to start enacting similar laws in the years to come.

For questions or additional information, please contact Stephen Stern at (410) 260-6585, (301) 261-8550, or sstern@hwlaw.com.

HYATT & WEBER, P.A.
ATTORNEYS AT LAW

BANKING AND BUSINESS LAW
CIVIL AND COMMERCIAL LITIGATION
CORPORATE LAW
EMPLOYMENT LAW
ENVIRONMENTAL LAW
INSURANCE COVERAGE
LAND USE
PROBATE AND ESTATE PLANNING
PROFESSIONAL LICENSE DEFENSE
REAL ESTATE TRANSACTIONS

200 WESTGATE CIRCLE, SUITE 500
ANNAPOLIS, MARYLAND 21401
410-266-0626
WWW.HWLAW.COM