porterwright

Information Privacy & Data Security Practice Group Law Alert

A Corporate Department Publication

May 2009

This Information Privacy & Data Security Law Alert is intended to provide general information for clients or interested individuals and should not be relied upon as legal advice. Please consult an attorney for specific advice regarding your particular situation.

Donna M. Ruscitti
614-227-2192
druscitti@porterwright.com

Mason Evans
614-227-2148
mevans@porterwright.com

Jack J. Gravelle
614-227-2084
jgravelle@porterwright.com

Brian D. Hall
614-227-2287
bhall@porterwright.com

Dennis D. Hirsch
614-227-2064
dhirsch@porterwright.com

Jeremy A. Logsdon
614-227-2093
jlogsdon@porterwright.com

Robert J. Morgan
614-227-2186
rmorgan@porterwright.com

James H. Prior
614-227-2008
jprior@porterwright.com

Kenneth K. Rathburn
614-227-2128
krathburn@porterwright.com

Justin L. Root
614-227-2129
jroot@porterwright.com

H. Grant Stephenson
614-227-2155
gstephenson@porterwright.com

Mark K. Velasco
937-449-6723
mvelasco@porterwright.com

Ohio Legislature Clarifies Requirement To Report Data Breach To Law Enforcement

You may be aware that Ohio (and most other states) requires companies to disclose a breach of security of their computer system to those whose electronic personal information may have been compromised.[1] But did you know that in Ohio you may also be required to report the breach to law enforcement?

Under Ohio law, the unauthorized access or attempted access of a computer system is a crime.[2] Those with knowledge that someone has accessed or attempted to access a computer system without authorization are required to report the crime to police.[3] Although this reporting obligation existed previously under a combination of various Ohio laws that required a person with knowledge of a felony to report it to law enforcement, Ohio recently revised state law to expressly require a person with knowledge of the unauthorized use of a computer or computer system to report it to a law enforcement agency.[4] Those who fail to report such incidents to law enforcement are themselves guilty of a crime.[5]

This reporting requirement raises a number of issues for affected companies. For instance, company leaders must now anticipate the uncertainty of how law enforcement officials will respond to company reports of data breaches. Will law enforcement officials simply take a report or will they launch a full-scale investigation of the breach? If law enforcement officials opt to investigate, companies will need to consider how best to work with law enforcement to protect their electronic data, confidential information, computer systems, and hardware. Logistical issues may also arise, including whether it will be necessary to idle company computer systems in order for law enforcement to conduct an investigation. All of these factors have the potential to adversely affect your operations. As a result, it is imperative to take steps now to mitigate the potential adverse effects of a criminal investigation by balancing your

(Footnotes)

[1] For private entities, see ORC § 1349.19; for state agencies or agencies of a political subdivision, see ORC § 1347.12.

[2] *See* ORC § 2913.04(B) (establishing various levels of felony offenses for the unauthorized use of a computer or computer system).

[3] *See* ORC § 2921.22(A)(2).

[4] *See* ORC § 2921.22(I) (establishing the failure to report a violation of ORC § 2913.04(B) as a second degree misdemeanor).

[5] For limited exceptions to this reporting obligation, see ORC § 2921.22(G).

porterwright

company's needs with the need to cooperate with law enforcement. Such steps might include:

- Establishing a data-breach response plan if your company does not yet have one;
- Considering a system back-up plan that allows an investigation to proceed without disrupting ongoing operations; and
- Appointing a data steward/liaison devoted to working with law enforcement.

As state and federal governments take additional steps to protect electronically stored personal information, companies that maintain such information need to stay up-to-date on their legal obligations. Having a data-breach response plan in place and periodically reviewing that plan can go a long way. Making adjustments to take into account changes in the law — such as Ohio's new law enforcement reporting requirement — can go even further to protect your company from liability.

Porter Wright Morris & Arthur LLP
www.porterwright.com

Cincinnati, Ohio
800-582-5813
Cleveland, Ohio
800-824-1980
Columbus, Ohio
800-533-2794
Dayton, Ohio
800-533-4434
Naples, Florida
800-876-7962
Washington, DC
800-456-7962