

Epsilon Breach: Small Businesses Who Get "Hacked" Must Act – Now

Fernando M. Pinguelo and Bradford W. Muller, Norris, McLaughlin & Marcus, P.A.

If you have a credit card or bank account, then you may have received an ominous e-mail alert discussing the data breach that recently occurred at Epsilon, a third-party vendor which provides marketing services to many companies. Luckily, the stolen information appears to have been limited to the names and e-mail addresses of only some customers. Apparently, no account numbers or other confidential information was compromised. Nevertheless, names and e-mail addresses are powerful tools for certain types of cybercriminals known as "phishers" who use social engineering to target potential victims and lure them into exposing confidential financial information.

Users of the Sony Playstation Network may not be as lucky, as upwards of 10 million credit card accounts may have been accessed by hackers in the recent network attack. Sony has been criticized for its response to the incident, and recently put in place a \$1 million identity theft insurance policy to cover affected gamers.

The danger posed by such data breaches has resulted in the federal government and many states adopting data breach notification laws. If you operate a small business, you may not be aware of your responsibilities under these laws. Further, although many of the state laws are similar, small business owners must be aware that if they have customers in multiple states, they must comply with the data

breach laws of each of those states. This begs the question: what are your responsibilities if cybercriminals hack into your company's computer system and steal sensitive customer data?

Legal Requirements

Here are some state law requirements you should know:

Was customers' personal information accessed by an unauthorized person? (In certain states these data notification laws broadly define the personal information protected to include that of employees. Therefore, even data breaches only involving the personal information of employees may be subject to the notice provisions of these laws.)

If so, disclosure of the breach must be made to the customers in the most expedient time possible and without unreasonable delay. In some instances, disclosure to a customer is not required if the business establishes that misuse of the information is not reasonably possible.

If you are required to disclose, some states mandate that in advance of the disclosure to the customer, the business must report the breach to law enforcement authorities for investigation or handling. Similarly, some states require reporting to the state Attorney General's Office.

© 2011 Norris, McLaughlin & Marcus, P.A. Originally published by Bloomberg Finance L.P. Bloomberg Law Reports® is a registered trademark and service mark of Bloomberg Finance L.P.

This document and any discussions set forth herein are for informational purposes only, and should not be construed as legal advice, which has to be addressed to particular facts and circumstances involved in any given situation. Review or use of the document and any discussions does not create an attorney-client relationship with the author or publisher. To the extent that this document may contain suggested provisions, they will require modification to suit a particular transaction, jurisdiction or situation. Please consult with an attorney with the appropriate level of experience if you have any questions. Any tax information contained in the document or discussions is not intended to be used, and cannot be used, for purposes of avoiding penalties imposed under the United States Internal Revenue Code. Any opinions expressed are those of the author. Bloomberg Finance L.P. and its affiliated entities do not take responsibility for the content in this document or discussions and do not make any representation or warranty as to their completeness or accuracy.

Finally, the business must notify the individual customers affected by the breach. Depending on the state, such notification may be provided by one of the following methods: (a) written notice; (b) electronic notice; or (c) substitute notice if the business can demonstrate that the cost of providing notice would exceed certain monetary levels or that the affected class of customers exceeds certain numbers, or the business does not have sufficient contact information. Substitute notice may consist of: (i) e-mail notice when the customer has an e-mail address on file; (ii) conspicuous posting of the notice on the Internet web site page of the business; and (iii) notification to major statewide media.

Also note that despite these specified methods of notification, for a business that maintains its own notification procedures as part of an information security policy, and the policy is otherwise consistent with the requirements of the state law, some states deem those businesses to be in compliance with the notification requirements as long as the business notifies customers in accordance with its policies. Additionally, in the event of a data breach involving more than 1,000 persons at one time, some states provide that the business must notify, without unreasonable delay, all consumer reporting agencies of the timing, distribution, and content of the notices.

Every federal and state notification law has its own nuances, but the general principles are similar: If you're hacked, notify your customers.

Fernando M. Pinguelo, a Partner at Norris, McLaughlin & Marcus, P.A. and co-Chair of the Response to Electronic Discovery & Information Group at the firm, is a trial lawyer who devotes his practice to complex business lawsuits with an emphasis on how technology impacts them. Mr. Pinguelo founded and contributes to the ABA Journal Award-winning blog, eLessons Learned—Where Law, Technology, & Human Error Collide (www.eLLblog.com). To learn more about Mr. Pinguelo, visit www.NJLocalLaw.com or email him at info@NJLocalLaw.com.

Bradford W. Muller, an Associate with Norris McLaughlin & Marcus, P.A., and a member of the Litigation and Internet Law groups, has been published in scholarly journals on numerous topics, including cloud computing, real estate, and appellate practice.

*For a comprehensive survey of federal and state legislation concerning cybercrime, see Pinguelo, Fernando M. and Muller, Bradford W., Virtual Crimes – Real Damages: A Primer on Cybercrimes in the United States and Efforts to Combat Cybercriminals (February 1, 2011). *Virginia Journal of Law and Technology*, Forthcoming. Available at SSRN: <http://ssrn.com/abstract=1789284>.*