

# A Moment of Privacy

A newsletter brought to you by the Privacy and Data Security Practice Group at Proskauer Rose

October 2009

Edited by  
Kristen J. Mathews

Welcome to “A Moment of Privacy,” a newsletter brought to you by the Privacy and Data Security Practice Group at Proskauer Rose LLP.

“A Moment of Privacy” addresses one legal development each month in the area of privacy and data security law. We answer the questions our clients are asking, in a way that we hope gives practical information to our readers. If you send us your question, you may find your answer in an upcoming newsletter.

## And now for this month’s question:

---

**Q:** My company’s data security policy classifies consumer contact information as confidential, but not “highly confidential” or “sensitive.” Should we rethink that classification?

**A:** I understand why you would consider reclassifying consumer contact information, such as consumer e-mail addresses, postal addresses and telephone numbers, as “highly confidential” or “sensitive” instead of merely “confidential.”

One case on point has dragged on since late 2007, when Ameritrade reported that a database of its customers’ contact information (including names, physical addresses, e-mail addresses and phone numbers) had been compromised. A class action law suit quickly followed, and the [third settlement attempt was rejected just recently](#) by the court on the grounds that, in the judge’s view, it provided an inadequate remedy for the affected consumers.

The rejected settlement would have required Ameritrade to:

- Post notices on its Web site warning customers about “stock touting spam”
- Retain independent experts to conduct biannual penetration tests on its systems
- Seed its e-mail address databases with monitored e-mail addresses for the purpose of detecting data compromises
- Offer to pay for one year’s worth of a spam or virus filtering service for each of the 6 million customers whose e-mail addresses were compromised
- Retain an analytics specialist to perform analyses of whether the compromised data has been used to commit identity theft
- If identity theft is detected, offer class members identity theft remediation services
- Donate \$55,000 to two anti-spam projects
- Pay plaintiffs’ counsel \$1.9M in attorney’s fees

Since these settlement terms did not satisfy the judge, the parties will reconvene at a hearing on December 10, 2009.

The Ameritrade case has served as a reminder that companies should not ignore the importance of keeping contact information secure while focusing primarily on more sensitive information such as Social Security Numbers and financial account numbers.

However, applicable laws that require companies to protect the security of individuals' information generally do not apply to mere contact information. For that reason, it is still appropriate to classify contact information as "confidential" as long as your policies provide for reasonable protections for such information. As an example, since customer databases compile all customer contact information into one place, and are an attractive target for hackers, such databases should be afforded greater protection than individual documents that contain just one customer's name and contact information. Similarly, when disposing of paper files containing customer contact information in mass, it would be a best practice, although not required by U.S. law, to shred such documents upon disposal.

**Have a question? E-mail Kristen J. Mathews at [kmathews@proskauer.com](mailto:kmathews@proskauer.com).**

## Privacy and Data Security Practice

Our Privacy and Data Security Practice is an outgrowth of our Internet, intellectual property, technology media & communications, labor and employment, health law, First Amendment, international law and litigation practices. Indicative of our experience and reputation in this relatively new field of law is the fact that the venerable Practising Law Institute (PLI) asked our Firm to create its first-ever treatise on the subject of privacy and data security law, called "Proskauer on Privacy," which was published in late 2006.

Privacy and Data Security Practice Group Partners:

Grégoire Goussu  
33.1.53.05.60.11 – [ggoussu@proskauer.com](mailto:ggoussu@proskauer.com)

Kristen J. Mathews  
212.969.3265 – [kmathews@proskauer.com](mailto:kmathews@proskauer.com)

Jeffrey D. Neuburger  
212.969.3075 – [jneuburger@proskauer.com](mailto:jneuburger@proskauer.com)

Anthony J. Oncidi  
310.284.5690 – [aoncidi@proskauer.com](mailto:aoncidi@proskauer.com)

This publication is a service to our clients and friends. It is designed only to give general information on the developments actually covered. It is not intended to be a comprehensive summary of recent developments in the law, treat exhaustively the subjects covered, provide legal advice, or render a legal opinion.

BOCA RATON | BOSTON | CHICAGO | HONG KONG | LONDON | LOS ANGELES | NEWARK | NEW ORLEANS | NEW YORK | PARIS | SÃO PAULO | WASHINGTON, D.C.

[www.proskauer.com](http://www.proskauer.com)

© 2009 PROSKAUER ROSE LLP. All Rights Reserved. Attorney Advertising.