State Attorneys General Data Privacy Settlement with TD Bank Requires Encryption of Sensitive Data on Backup Tapes and Faster Notice

In taking action against TD Bank, N.A., for allegedly losing two unencrypted backup tapes, a group of attorneys general highlighted their increasing focus on encryption in data breach matters, as well as the need to promptly notify customers of the loss of their personal information. In March 2012, TD Bank is alleged to have lost two unencrypted computer backup tapes containing personal information. TD Bank did not notify potentially affected consumers until October 2012, almost seven months after the incident was alleged to have occurred.

This past October, nine state attorneys general from Connecticut, Florida, Maine, Maryland, New Jersey, New York, North Carolina, Pennsylvania, and Vermont (the "multistate") reached a settlement with TD Bank related to the incident, the terms of which included a payment of $850,000 as well as assurances regarding additional security measures. On December 8, 2014, the Massachusetts Attorney General also reached a settlement, which included a monetary settlement of $825,000, of which $200,000 was credited to TD Bank to reflect security measures and upgrades it had taken following the incident. The Massachusetts agreement likewise contained further security assurances.

Encryption is becoming an increasing area of focus in data privacy law. Most state security breach notification statutes contain exemptions where the compromised data was encrypted. Massachusetts regulations actually affirmatively require encryption in many instances, including where "transmitted records and files containing personal information" will "travel across public networks" and where "data containing personal information" is "transmitted wirelessly." 201 Mass. Code. Regs. 17.04(3). Personal information stored on laptops or other portable devices must also be encrypted under the Massachusetts rules. *Id.* at 17.04(5). Similar provisions are in place elsewhere, for example, in Nevada and for some healthcare data; and legislation requiring encryption of data in transit has been proposed in several other states, including California. *See, e.g.*, California Data Breach Report, at 26-27 (October 2014).

As the settlement demonstrates, even in states without express encryption obligations, attorneys general are increasingly focusing on a company's encryption practices. Both the Massachusetts and multistate settlements require that TD Bank encrypt backup data in transit going forward. TD Bank agreed with the multistate, among other things, to encrypt all backup tapes transported off of the Bank's premises or transport them via armored car in the event that the tapes were created prior to the effective date of the multistate agreement and were unencrypted. The Massachusetts settlement also requires encryption of personal information stored on backup tapes.

The Massachusetts settlement may further reflect its Attorney General's Office's potentially broad interpretation of its encryption regulations as extending beyond standard "transmissions" of data through means such as email or on portable devices such as laptops to include the movement of data in any form – even putting backup tapes on a truck. Companies must be wary that data that would seem to be at rest could later be moved in a manner that Massachusetts or other state attorneys general could contend to be covered by their data-in-transit laws. Whether a court would sustain that position if challenged remains an open question and will depend on the particular state law and facts in question.

The settlement additionally reinforces the need to promptly notify affected consumers in the event that their personal information is at risk. TD Bank did not notify consumers for over half a year after the alleged incident occurred. Both the multistate and Massachusetts criticized TD Bank for the delay, and the settlements require prompt notice in the event of future data breaches.

For more information regarding the TD Bank settlement and its potential impact on your operations, please contact a member of our leading privacy & data security team, including Jim DeGraw, Seth Harrington, David McIntosh, Doug Meal, Mark Szpak, and Michelle Visser.

James S. DeGraw
Seth C. Harrington
David McIntosh
Douglas H. Meal
Mark P. Szpak
Michelle Visser