Two-Factor Authentication May Be Coming to a

Digital Media and Data Privacy Law Blog

on 02.26.2015
Posted in Data Security, Privacy

Ed. Note: This entry is cross posted from Cady Bar the Door, David Smyth's blog offering Insight & Commentary on SEC Enforcement Actions and White Collar Crime.

When I was at the SEC and online broker-dealers' customers were the victims of hacking incidents, I used to wonder, why don't the broker-dealers require multi-factor authentication to gain access to accounts? It was a silly question. I knew the answer. Multi-factor authentication is a pain and nobody likes it.

Do you know what it is? Here's what Wikipedia says, so it must be true:

Multi-factor authentication (MFA) is a method of computer access control which a user can pass by successfully presenting authentication factors from at least two of the three categories:

· knowledge factors ("things only the user knows"), such as passwords

· possession factors ("things only the user has"), such as ATM cards

· inherence factors ("things only the user is"), such as biometrics.

The idea is, hackers might figure out your password, but they won't be able to figure out a number that changes every 30 seconds on a card you carry or on your cell phone. They won't be able to replicate your fingerprint. That's the idea, anyway. Brokers and banks have been loathe to require multi-factor authentication because it's inconvenient and customers often hate it.

But here comes Ben Lawsky, the Superintendent of New York's Department of Financial Services, who just unveiled a number of proposals to increase cybersecurity at banks under his jurisdiction. One of these is to require that banks use multi-factor authentication. This move could take a lot of the economic pressure off banks that would otherwise like to implement this control for its customers, but have been unwilling to do so for fear of losing those customers to rivals. If everybody has to do it, there's not a lot of fear from imposing it unilaterally.

That's not all Lawsky has in mind. His proposal also includes:

· requiring senior bank executives to personally attest to the adequacy of their systems guarding against money laundering;

· ensuring that banks receive warranties from third-party vendors that those providers have cybersecurity protections in place;

· random audits of regulated firms' transaction monitoring systems, meant to catch money laundering; and

· incorporating targeted assessments of those institutions' cybersecurity preparedness in its regular bank examinations.

Lawsky's proposals could be a big deal. Stay tuned.