Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

SEC's Identity Theft Rules Will Drive Up Data Security Costs

By **Allison Grande**

Law360, New York (April 23, 2013, 8:43 PM ET) -- Investment advisers, broker-dealers and other entities regulated by the U.S. Securities and Exchange Commission are scrambling to enact programs to detect red flags for identity theft under new agency rules, a major undertaking that attorneys say will require costly and ever-evolving assessments of data security risks.

In accordance with their expanded purview under the Dodd-Frank Act, the SEC and the U.S. Commodity Futures Trading Commission on April 10 **released** final rules that require certain entities regulated by the two agencies — including investment advisers, mutual funds and commodity pool operators — to adopt an identity theft program.

The program should include policies and procedures designed to identify relevant types of identity theft red flags, detect the occurrence of those red flags, respond appropriately to them and periodically update the program. The rules also require entities to provide staff training and oversight of service providers.

"There's a lot of personal information like financial account numbers and credit card numbers in the hands of these entities that they should be treating with a high level of sensitivity already," Day Pitney LLP Compliance Risk Services Director Jim Bowers told Law360 on Tuesday. "However, what the SEC and the CFTC have done is ... forced companies to think about securing this personal information in a much more systematic way."

But attorneys say that building an identity theft program and training employees on how to assess red flags won't be the most challenging step in companies' march to comply with the rules by Nov. 20. Rather, the most difficult part will be carrying out thorough assessments of their data security risks to determine how to craft programs that most effectively match their needs.

"These companies know how to implement policies and conduct oversight and training. Identifying risk is the hardest part," Quarles & Brady LLP partner Hoyt Stastney said. "They need to get their arms around the identity theft risks that currently exist around their businesses and be aware that even after establishing a policy, they always need to re-evaluate because the way that data thefts are being carried out are constantly changing."

Covered entities need to immediately undertake an examination of their risks, given that it is vital to building robust identity theft programs and the process could involve lengthy document review and interviews with scores of individuals who have firsthand knowledge of where the company's vulnerabilities lie, attorneys say.

"It's not just a matter of finding a model program on the shelf and adapting that to a particular entity," Bowers said. "That approach is doomed to fail because you missed the mark. In order to develop an effective program, it needs to be preceded by an analysis of the risk to the secure maintenance of confidential information."

While the new rules require that each program contain policies and procedures for identifying and responding to red flags, the rules do not force companies into a strict framework, allowing room for each entity to take an approach that addresses its own specific risks.

"There is a certain amount of flexibility baked into the rules so that they are not so prescriptive that they would be insensitive to the unique qualities and characteristics of each business," Covington & Burling LLP attorney Michael Nonaka said. "That's helpful because it allows companies to tailor programs to their particular operations, but it could also be frustrating because it doesn't prescribe elements that they can pick up and run with."

The level of difficulty that companies will experience in implementing their programs will hinge on the size of their risks and if they have given any thought to their identity theft exposures in the past, according to attorneys.

"Ever since Dodd-Frank passed, the community has been aware that the rules were coming, but unlike some banks and others that have had to focus on identity theft for some time, a lot of these entities have not had to think about identity theft before," Nonaka said.

The new rules encompass entities like mutual funds, which had to follow red flag rules when they were being administered by the Federal Trade Commission before the Dodd-Frank Act transferred oversight for mutual funds and other regulated entities under the red flag rules to the SEC and CFTC. But even though the previously regulated entities shouldn't have as hard a time complying with the new rules, the shift of enforcement power to their primary regulator could result in a higher level of scrutiny than they had under the FTC's rules.

"The FTC has broad jurisdiction over a range of companies, while the SEC and CFTC have these specific constituencies," Bowers said. "I would expect the SEC to mount a much more rigorous enforcement effort going forward."

While entities like investment advisers and broker-dealers that have not been regulated before will likely have to play catch-up to the previously-regulated entities, their efforts could be eased by their relatively low identity theft risks, attorneys noted.

"For most private equity firms, it's probably not going to take a whole lot more work than putting together an appropriate policy and educating their employees about the red flags, since the risks in the private equity world are low," Edwards Wildman Palmer LLP partner Heather Stone said.

But despite the varying degree of difficulty in implementing programs, the covered entities will share at least one similarity: significant financial consequences.

"While the measures are certainly helpful given the recent and rampant uptick in identity theft, this will have a significant impact on the cost structure for these companies," DLA Piper securities litigation practice co-chair Perrie Weiner said. "And, in an uncertain and continued unstable economy where profit margins already are extremely lean, adding increased costs like this will hit the companies' bottom-line numbers."

But attorneys noted that the costs could be offset by the benefits gained from having

better protections against the growing threat of data breaches, which costs companies millions of dollars to mitigate, and from having a stronger defense when responding to regulators after an incident.

"Data breaches are increasing exponentially every year, and it's just a matter of time before a company gets hit," Bowers said. "And if companies don't have a program in place at the time of the incident, they'll be faced with a whole host of new issues when the regulator comes knocking."

--Editing by Elizabeth Bowen and Katherine Rautenberg.