Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

# MasterCard Exec, Others Urge Flexible Cybersecurity Regime

By **Allison Grande**

*Law360, New York (October 14, 2016, 8:35 PM EDT)* -- A MasterCard executive and other cybersecurity experts on Friday cautioned regulators against following the lead recently set by a New York banking authority and instituting proscriptive cybersecurity rules that would quickly become irrelevant, saying that a regime akin to a flexible industry-driven framework rolled out two years ago provided a better way forward.

During a panel at a Women Leaders in Cybersecurity symposium hosted by New York University's Center of Cybersecurity, executives from MasterCard Inc. and Goldman Sachs Group Inc., as well as former government officials who are now in the private sector, explored the complex regulatory landscape that faces business when it comes to cybersecurity.

With an array of regulators in the U.S. and abroad becoming increasingly interested in the topic, and policymakers struggling with how to best tackle rapidly evolving cyberthreats, businesses are left to follow a patchwork of mostly sector- and state-specific privacy regulations in the U.S. while carefully monitoring moves domestically and in the European Union to formally tighten rules for protecting information systems from malicious actors.

One such recent move toward more proscriptive regulations came from the New York Department of Financial Services, which last month unveiled a proposal to impose stringent rules on banks, insurers and other financial institutions that would require them to take steps such as setting out detailed plans for dealing with breaches and protecting their information systems.

Asked by moderator Danielle Gray, a partner at O'Melveny & Myers LLP, about the possibility that other policymakers could follow the New York agency's example, panelists responded that the scenario was a definite possibility.

"I worry about that as a trend," said Kendall Burman, a cybersecurity and data privacy counsel at Mayer Brown LLP and former deputy general counsel at the U.S. Department of Homeland Security. "Different companies experience this stuff really differently, especially when it comes down to size, budget and what industry they're in."

Moving to set rules that broadly mandate certain tech fixes such as encryption — which is currently a best practice but could be deemed useless in the future — is also risky, experts noted.

"We're seeing ecosystems change and shift and morph ... so the challenge for regulators is to create mandates that don't bump into the changing landscape," said JoAnn Stonier, executive vice president and chief information governance and privacy officer at MasterCard.

As an example of the difficulty with setting proscriptive rules for a rapidly evolving area, Ann Barron-DiCamillo, partner and chief technology officer at Strategic Cyber Ventures and former director of the U.S. Computer Emergency Readiness Team, pointed to the Federal Information Security Management Act. The act is a piece of legislation enacted by Congress in 2002 that defines a comprehensive framework to protect government information and assets against a broad range of threats and directs agencies to produce certain categories of information to achieve this objective.

"A lot of the data required, over time, was no longer cyber-relevant," Barron-DiCamillo said. "It didn't keep pace. [An amendment] passed in 2015, so that statute was in effect for 13 years before it got updated, way past its longevity and its uselessness and its effectiveness."

Instead of rushing to impose rules on companies that are likely to quickly become obsolete, the panelists advocated for regulators to embrace voluntary cybersecurity frameworks such as the one that was released by theNational Institute of Standards and Technology in February 2014. The framework has been widely praised by industry for its flexibility and its utility in helping businesses across a range of sectors map out and understand their cybersecurity risks, a result that is likely a byproduct of the fact that private companies had a hand in developing the framework.

"Because the framework was built collaboratively, it actually works very well," Goldman Sachs Vice President of Technology Sandie Ritucci said. "It's flexible, it's adaptive, it's risk-based, it does provide guidance and regulators can use it as a tool to evaluate ... but it's not proscriptive so it is levergeable across different industries."

Although experts stressed that the framework was far from a panacea, they said it does provide them with a model that is able to easily adopt to rapid changes in technology, allows them to address their own unique cybersecurity risks and gives them a tool to have sometimes difficult but necessary conversations with C-suite executives about these issues.

"It gives chief information security officers a framework to show executives what tools they are applying and helps create a conversation about what they're doing to better secure their systems," Barron-DiCamillo said.

The panelists mostly shied away from the idea of having more regulations thrust upon the private sector, but there was one notable exception.

"Wouldn't it be great if the regulators joined forces and said, 'Here's one rule, and this is what we need to do?'" Ritucci asked. "Cybersecurity is too important for people to get dizzy because there are so many rules."

--Editing by Christine Chun.

---