

# Financial and Merchant Industries Group and Obama Administration to Address Privacy Concerns

March 25, 2015

On behalf of its 19 participating trade association members from the merchant and financial services industries, the Merchant Financial Cyber Partnership (MFCP) announced "8 Next Steps" to protect customers and their sensitive data from the ever-growing host of cyberthreats. The 8 Next Steps are as follows:

1. Establishing a formal administrative link and protocols for information sharing between merchants and financial services institutions;
2. Holding threat information sharing forums;
3. Hosting exercises that simulate significant cyber attacks;
4. Implementing and refining the National Institute of Standards and Technology's Cybersecurity Framework for developing a listing of leading cybersecurity practices;
5. Developing formal breach notification response programs;
6. Outlining recommendations for merchants, issuers, acquirers, and processors to collaborate in developing technology standards to combat cyber threats to payment systems;
7. Outlining technological and other principles for protecting payment systems; and
8. Proposing tailored, effective legislation in support of cyberthreat information sharing.

The essence of these principles has been echoed by policymakers in the United States and other countries. President Obama, during his most recent State of the Union address, stated that he intends to propose comprehensive federal legislation regarding data privacy and cybersecurity.

Many are hopeful that federal legislation will mean a single data privacy breach law that will obviate the need to meet the differing obligations under state and federal data privacy laws and regulations. Depending on the precise language of the federal legislation ultimately enacted, it is possible that a single federal data privacy breach notification law could actually result in a heavier compliance burden on businesses than exists today. MFCP members include the American Bankers Association, American Hotel and Lodging Association, Financial Services Forum, International Council of Shopping Centers, and the National Retail Federation. All industry stakeholders will want to stay abreast of the MFCP developments, as well as the ever-changing state, federal, and foreign data privacy and cybersecurity legal landscapes.

## Related Practices

[Technology](#)

[Intellectual Property](#)

[Cybersecurity and Privacy](#)

[Financial Services Regulatory](#)

## Related Industries

[Technology](#)

©2024 Carlton Fields, P.A. Carlton Fields practices law in California through Carlton Fields, LLP. Carlton Fields publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information and educational purposes only, and should not be relied on as if it were advice about a particular fact situation. The distribution of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship with Carlton Fields. This publication may not be quoted or referred to in any other publication or proceeding without the prior written consent of the firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our Contact Us form via the link below. The views set forth herein are the personal views of the author and do not necessarily reflect those of the firm. This site may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.