MERCHANT FINANCIAL CYBER PARTNERSHIP

8 Next Steps

The Merchant Financial Cyber Partnership has succeeded in its goal to work collaboratively across the payments system to enhance security in order to protect customers and their data from cyber threats. Strong and productive relationships have been formed across the merchant and financial industries throughout the course of the Partnership's work. It is to the benefit of both industries those relationships be maintained.

The Partnership brought together executives from the financial services and merchant industries, government and other stakeholders to work together on key public policy issues impacting the entire payment ecosystem. Our industries are stronger together than we are divided and to keep the trust of our customers, we must work collaboratively to improve overall security.

To ensure the Partnership's efforts fulfill its goals, the following outlines eight next steps for the Partnership in key areas:

Threat Information Sharing

1. Secure an agreement between the Financial Services Information Sharing and Analysis Center (FS-ISAC) and the Retail Cyber Intelligence Sharing Center (R-CISC) to have a formal administrative link and establish protocols for sharing information between the financial services sector and the merchant sector.
2. Convene periodic threat information sharing forums.

Cyber Risk Mitigation

3. Host a joint "table top" cyber exercise with financial and merchant institutions to simulate a significant attack against a processor or multiple processors simultaneously that degrades ability to conduct commerce.
4. Leverage the National Institutes of Standards and Technology (NIST) ongoing workshops to implement and refine the voluntary NIST Cybersecurity Framework and drive its usage along with existing work with the FSSCC, FS-ISAC and other relevant bodies. Develop compendium listing of leading practices.
5. Develop a paper on breach notification response programs.

Advanced Card Present & Card Not Present Security Technology

6. Outline recommendations for merchants, issuers, acquirers, and processors to collaborate more in the development of technology standards to ensure the safety and security of the payment system.
7. Outline principles for protecting the payments system, focusing on technologies that minimize the value of payments information if it is stolen, lost or breached and on customer authentication.

Cybersecurity Legislation

8. Present to congressional leaders joint principles supporting cyber threat information sharing legislation.