PCI Security Standards Council

PAYMENT CARD INDUSTRY SUMMIT ADVANCES CROSS-INDUSTRY COLLABORATION ON CYBERSECURITY AND DATA PROTECTION
In the Midst of the U.S. EMV Migration Liability Shift, Global Cybersecurity, Technology and Data Forensic Experts Convene on the Next Generation of Payment Security at North America Community Meeting in Vancouver

VANCOUVER, 01 October 2015 — Leading cybersecurity, technology and data forensics experts gathered in Vancouver this week at the Payment Card Industry (PCI) Security Standards Council Community Meeting to share the many advances made over the past year in protecting consumer payment information from criminals. Collaboration between industry, governments, law enforcement and consumers, information sharing between countries and competitors, and proven technologies that devalue stolen data were only a few of the topics discussed among 1,500 in attendance.

The meeting comes at a critical turning point for payment security globally, as the U.S. system transitions to EMV chip technology in accordance with the October 1, 2015 fraud-liability shift set by payment card brands. As the cost of cybercrime climbs to $US465 billion a year, the Council urged the payments industry to come together and tackle an increased threat to card data, especially because improved EMV chip protection at the point-of-sale (POS) is expected to criminals toward more vulnerable online and mobile channels domestically and internationally.

"We are fighting a silent, pervasive war against cybercrime. Collaboration is crucial in this effort," PCI SSC General Manager Stephen W. Orfei told attendees in his keynote address. "We must use our shared experiences to beat cybercrime. We can't legislate our way out of it, we can't wall ourselves off from one another and there is no technical silver bullet that is going to solve cyber theft. It's going to take a 24x7 effort, and we all have to work together."

Added Orfei, "EMV chip technology used with point-to-point encryption and tokenization will tame emerging risks and help achieve our true endgame. Our endgame in the payments industry is to devalue stolen card data so it's useless in the hands of cybercriminals. We hope other industries can look to our solutions and use them to combat crimes such as identity theft and stolen medical records, both of which are on the rise."

 "With Canada already migrated and the U.S. moving over to EMV chip technology, we are making major strides forward in global payment security," said PCI SSC International Director Jeremy King. "It also signals the need for businesses to be forward-looking about adopting technology and best practices that both secure data online and across channels, and take advantage of mobile and other emerging forms of payment."

Keynote presentations at the meeting included Brian Krebs and John Nance, who both spoke about today's cyber threat and breach landscape. Panel presentations covered topics such as resources and best practices to help businesses protect their customer payment data, with a specific focus on how to drive a 24X7 approach to security rather than one-time compliance mindset; simplifying security for small businesses; helping businesses detect and respond to breach incidents; and driving increased information sharing with forensic investigators and law enforcement.

For more information on news and presentations from the North America Community Meeting, please visit the blog.

The Vancouver meeting was the first of three PCI Community Meetings this year. For more information on the Asia-Pacific and Europe Community Meetings in Tokyo, Japan and Nice, France, visit: http://events.pcisecuritystandards.org/2015/.

About the PCI Security Standards Council
The PCI Security Standards Council is a global forum that is responsible for the development, management, education, and awareness of the PCI Data Security Standard (PCI DSS) and other standards that increase payment data security. Connect with the PCI Council on LinkedIn. Join the conversation on Twitter @PCISSC.