Security
Standards Council

Payment Card Industry
Security Standards Council, LLC

401 Edgewater Place, Suite 600
Wakefield, MA 01880
Phone: 781 876 8855

With the goal of transparency and keeping our Participating Organizations and the industry at large informed on the Council's response to key issues raised in a letter from some of our association PO's, we are providing last month's response here for reference.

June 15, 2009

VIA OVERNIGHT COURIER

David J. Hogan, III
Senior Vice President, Retail Operations & CIO
National Retail Federation

Joe Mcinerney
President & CEO
American Hotel & Lodging Association

Dawn Sweeney
President & CEO
National Restaurant Association

Henry Ogden Armour
President & CEO
National Association of Convenience Stores

Dodd Roberts
President/CEO
Merchants Advisory Group

Matthew Shay
President & CEO
International Franchise Association

Jack Whipple
President
National Council of Chain Restaurants

Dear Messrs. Hogan, McInerney, Armour, Roberts, Shay, Whipple and Ms Sweeney,

Thank you for your letter dated June 9th.

I will address the points in your letter individually below. But before I do that, I would like to reassure you that much of what you are advocating -- for example, opportunity to provide feedback on standards or to explore encryption further -- in fact already exists within the PCI Security Standards Council.

Securing cardholder data continues to be top of mind for all stakeholders in the global payment chain, not just merchants in the United States. For the PCI Security Standards to continue to be effective in protecting cardholder data, the Council must continue to solicit and represent the voices of payment chain stakeholders worldwide. We do this through a structured, but flexible, lifecycle and feedback process that is transparent (available on the Council's Web site at https://www.pcisecuritystandards.org/pdfs/OS_PCI_Lifecycle.pdf) and offers all stakeholders a voice.

The threat landscape continues to evolve, and so we must continue our focus on data security, working together to seek ways to improve cardholder data protection, in spite of the challenging economic circumstances you mention. Now, as ever, all parties in the payment chain must collaborate to meet their collective responsibilities in securing sensitive payment card data.

In that context, I am happy to address the points outlined in your letter:

1. The Council maintains a comprehensive and transparent lifecycle management process for all its standards. This process incorporates two comment and review periods during which Participating Organizations (POs) have the opportunity to provide input to the PCI DSS before it is published. Separately we rely heavily on questions and comments submitted from the public in face-to-face meetings and online, and we lever the skills and expertise of our Participating Organizations in working groups, task forces and Special Interest Groups for specific concerns or issues.

   The next general feedback period for the PCI Data Security Standard and Payment Application Data Security Standard will open on July 1. All current Participating Organizations will receive feedback forms and materials through which they may formally comment on the standards. Following this there is another face-to-face opportunity to provide feedback at the annual community meetings in Las Vegas in September and Prague, Czech Republic, in October.

   Your organizations represent critical constituents in the North American payment environment and your contributions are highly valuable. The Council enjoys input from more than 600 organizations worldwide, including numerous associations such as European Payments Council, Independent Community Bankers Association of America, Merchant Risk Council and South African Retailers Payment Issues Forum. Associations are an important Council constituency. Everyone is interested in a safe and secure payments environment; we invite the organizations among you who have not yet joined us to add their voices to those of your global colleagues in a constructive partnership, and on an equal footing, to achieve that goal. The Council's annual Community Meetings are an important part of this partnership and of the feedback process. The Council re-extends the invitation to you and your members to come and actively participate in these meetings.

   On the topic of partnering with ASC X9, while we recognize the domestic concerns of some of your organizations, the payment chain is global, security threats are borderless, and we must seek input and representation from around the world in this process. As you can appreciate, if the Council were to begin incorporating the domestic norms or standards of each individual country, even from markets as large as the United States, into the PCI Standards, the entire system of data security would become unworkable for all types of players in the payment chain that have international operations or sales, which includes many of your members. Further, the Council would be accused of US-centrism, a concern we have already read about in the press this week following the publishing of your letter (see link at end of letter to *Retail Week* article of June 10th, "NRF lobbying on PCI DSS could be bad news for UK retailers") -- inviting other nations to develop their own standards, resulting in increased complexity and greater challenges to meeting our end goal, securing cardholder data in a globally consistent manner. Therefore, while we will continue to monitor and adopt, when appropriate, security best practices with global applicability (e.g., OWASP, NIST) the Council cannot tie itself to geographically specific organizations.

2. The Council believes that its process of introducing new changes as "best practices" with effective dates six to 18 months or more into the future is a fair and balanced approach to improving security while mitigating the impact of changes. Moreover, as new threats emerge, it is critical that the Council be responsive to emerging threats. We make every effort to balance this responsiveness with merchants' need to transition systems. For example, PCI DSS Requirement 6.6 (application firewall and code review requirement for Web-facing applications) was introduced in v 1.1 in September 2006 as a best practice with a deadline of June 2008 for adoption.

According to our constituents, changes between v 1.1 and 1.2 were not so significant that companies should have faced substantial implementation challenges, if they were already on the road to adopting PCI DSS v1.1. Also, as a clarification, from the Council's perspective, our standards are effective as of their publication. But, that "effective date" is different from any compliance deadlines or mandates that are enforced by the payment brands.

As you can appreciate, for every request we receive such as yours for more time, we receive one that is critical of the Council for not revising its standards more frequently. Our goal and challenge is to try to fairly balance these two competing and understandable viewpoints, while always being mindful of the need to be responsive to emerging threats.

3. The Council continues to follow with interest the recent announcement by ASC X9 regarding end-to-end encryption. The Council is currently conducting its own commissioned research on encryption. I'm sure you will agree it is too early to make a formal commitment to incorporating work by X9, since that work has only just started and it will be some time before a finalized position is created. That said, we will contribute as appropriate to that work effort, both directly (if appropriate) and indirectly through our members and POs. We will also review and include for evaluation material as part of the PCI DSS feedback process. But again I would like to reiterate that the Council is a global standards body, not a U.S.-centric entity. We must ensure that we incorporate feedback and security best practices from around the world, not just here in the United States.

   The Council will continue to take a leadership role in payment card security and this is why we have commissioned research on technologies that may impact organizations' payment security risk. We have followed debates and technological developments in the encryption space for some time. We note that while your organizations have expressed support for end-to-end encryption, this support has not been echoed by many of our Participating Organizations. Many retailers have shared opinions that encryption is too costly and complex, slowing down transaction speed and requiring significant financial investment. In fact, during the 2007 feedback process, not a single Participating Organization recommended end-to-end encryption as a potential solution. In spite of divergent opinion on this topic, the Council will continue to examine this issue and we look forward to discussing the findings of the research study with our Participating Organizations at the Community Meetings in the fall.

4. The Council is confident in the strength of the PCI DSS in its current 12 requirement form. Feedback shows that we have the right blend of specificity and high-level concepts. The standard in its current form affords stakeholders the opportunity and flexibility to work with Qualified Security Assessors (QSAs) to determine appropriate security controls within their environment that meet the intent of the PCI standards. In this threat landscape and in spite of economic challenges all business faces, we need tighter, not looser, more subjective, attention to data security. We heed the concern that some businesses want to approach security in a way that balances risk according to their organizations priorities and risk tolerance. This year, in partnership with the Council's elected Board of Advisors, we introduced the Prioritized Approach to PCI DSS in response to this stakeholder feedback. The Prioritized Approach helps an organization understand how to tackle DSS in a way that removes the highest risk first. At its heart, though, it still supports our position that full and ongoing adherence to all DSS requirements is the best line of defense against a breach.

   To address your point about reporting, although organizations do not report their compliance status to the Council, based on feedback from our Participating Organizations we have tried to streamline the administrative side of PCI adoption within our purview through the provision of Self Assessment Questionnaires and universally accepted Attestation of Compliance forms. Our aim is to provide the tools necessary to assist in any reporting requirements organizations might face, in spite of the specifics of those requirements being outside of the Council's purview.

5. While a move to a system that uses just authorization codes and truncated receipts at the retailer's location is an interesting proposal, it is one of many suggestions focused on an overhaul to the global payments infrastructure, with ramifications that may go well beyond just data security. As such, it involves details of individual business relationships and company policies, which remain entirely outside of the Council's purview.

I would like to reassure you and your members that your voices can be heard both directly in our established feedback process and indirectly through representatives on the Board of Advisors (BoA) that share similar interests. For example, the petroleum industry is represented by Exxon Mobil, and smaller merchants can find a voice through acquiring bank representatives, franchise organizations such as McDonald's, and alternative payment methods such as PayPal. I encourage you to forge relationships with the Board of Advisors, along with actively participating in our upcoming feedback period. As Participating Organizations you are welcome to participate in or request the creation of a special interest group. These groups are led by one or more representatives from the BoA, and they look in detail at particular challenges or areas for development and make recommendations back to the Council. As an example, a NACS representative already chairs the pre-authorization group. I encourage more of you to participate in these groups to channel energies into effecting change or ensuring your members' concerns are fully explored.

In closing, thank you again for your feedback. I would like to reiterate that we all share the same objective to protect payment card data. Many of the suggestions you are make in your letter are already long established. So I invite those among you that are not currently Participating Organizations to take the time to join us and play an active and ongoing role in evolving global payment security standards. I hope to see all of you at our Community Meetings this fall.

Sincerely,

Bob Russo
General Manager

Link to Retail Week story: http://www.retail-week.com/technology/payment-card-security/nrf-lobbying-on-pcidss-could-be-bad-news-for-uk-retailers/5003406.article

cc: Kenneth Chenault, American Express Company
David Nelms, Discover Financial Services
Joseph W. Saunders, Visa, Inc.
Robert Selander, MasterCard Worldwide
Tamio Takakura, JCB International Credit Card Company, Ltd.