

May 31, 2013

Federal Trade Commission
600 Pennsylvania Avenue NW
Room H-113 (Annex B)
Washington, D.C. 20580

Re: Privacy and Security Implications of The Internet of Things

Dear FTC Staff:

In response to the Federal Trade Commission's (FTC) request for input on privacy and security implications of "The Internet of Things," the Electronic Transactions Association (ETA) submits the following comments. These comments – which will focus on consumer privacy and security issues in the mobile payments arena – are intended to assist the FTC as the Commission prepares for the November 2013 public workshop.

Mobile payments are just beginning to realize their full potential as a robust enabler of global electronic commerce. As the trade association of the electronic payments industry, ETA is the hub of activity in mobile payments. Our industry works collaboratively to ensure that the regulatory and business environment promotes innovation and cooperation, and that consumers and merchants have access to an efficient, reliable, and secure mobile payments system.

I. PRIVACY

Any privacy guidelines addressing smart technology should include protections for consumers who use their mobile phones to initiate mobile payment transactions. Consumers engaging in mobile commerce should be notified of any information being collected and should have confidence that their Personally Identifiable Information (PII) will not be used by third parties without their knowledge or consent. Mobile Payment Solutions (MPS) should provide easily digestible and concise notice of privacy policies (including descriptions of the data types that will be used, specific data practices in the mobile payments arena, and any options consumers have for controlling such use). As a practical matter, privacy notices should be clearly readable on small (i.e., handheld) screens.

Thorough privacy guidelines will govern the collection, use, storage, and sharing of PII and should be applicable to all entities in the MPS ecosystem. This includes device manufacturers, application

developers, platform providers, merchants, acquiring processors, online payment services, payment products providers, and payment networks that operate on a mobile device. In short, MPS providers should clearly and plainly articulate to consumers the purposes for which they collect and use any payment-based PII.

Please note that privacy guidelines should not apply to mobile-based payment information used or shared to comply with court orders, subpoenas, lawful discovery requests, and other legal or regulatory requirements; to enforce the MPS provider's legal rights or defend against legal claims; for testing, product fulfillment, or maintenance in the standard operation of any payment-based service; or when data is made in aggregate or anonymously.

II. SECURITY

Security guidelines for mobile payment acceptance by merchants should include general security goals (limiting the exposure of the consumer's payment card data by ensuring that only authorized persons have access to the payment functionality of the solution) and Point-to-Point Encryption (to secure encryption of payment card data at the point of interaction).

Additional security suggestions include:

- Any cardholder data entered into the mobile application, outside of a P2PE validated point of input device (e.g., key-entered account data), should be immediately encrypted for transmission.
- If the mobile application is enabled for EMV (or "chip card") transactions, EMV should be configured for online only authorizations and should not be accepted in an off-line status.
- If merchants wish to accept PIN debit transactions on mobile devices, they should only be capturing the cardholder PIN on mobile devices that comply and are registered with the PCI Pin Transaction Security (PCI PTS) system.
- Merchants should have policies in place that deal with the loss and/or theft of a mobile device that has a mobile payment application installed on it, and have the ability to remediate or disable any payment applications that reside on said device.

Regarding the last bullet point, consumers generally take comfort in knowing that payment account credentials are not stored on their mobile device. To this end, the FTC should consider implementing an open, cloud-based, Trusted Service Manager (TSM) model for mobile payments; one where sensitive credentials never have to be exposed outside of the payment service providers' (e.g., issuers') datacenters. Such an approach benefits both issuers and merchants by extending beyond current card emulation

payments models yet preserving the core strengths of the current card emulation approach (e.g., ubiquity and payments uniformity).

III. IMPORTANCE OF COMPREHENSIVE APPROACH

Lastly, the ETA urges the FTC to take a comprehensive approach to privacy and security. “The Internet of Things” implies a convergence of technologies, applications, and devices; it would not make much sense for the FTC to construct privacy and security rules around one particular software package, one application, or a specific device. In order to encompass the broad spectrum of Internet-enabled devices, a holistic examination of privacy and security implications is necessary.

As consumer payment preferences shift away from more traditional methods and toward mobile payment options, it is critical that we identify early on the ways in which greater connectivity poses privacy and security risks. The ETA looks forward to collaborating with the FTC and other stakeholders as the discussion of privacy and security in the digital age advances.

Submitted by:

Electronic Transactions Association

1101 16th St. N.W., Suite 402

Washington, D.C. 20036

202-828-2635

Point of contact: Mary Bennett, mary.bennett@electran.org