



1101 16th Street NW
Suite 402
Washington, DC 20036

www.electran.org
T 800.695.5509
T 202.828.2635
F 202.828.2639

December 12, 2012

Chairman Leahy
Senate Judiciary Committee
224 Dirksen Building
Washington, DC 20510

Ranking Member Grassley
Senate Judiciary Committee
224 Dirksen Building
Washington, DC 20510

Re: S.1223 Location Privacy Protection Act of 2011

Dear Chairman Leahy and Senator Grassley:

On behalf of the Electronic Transactions Association (ETA), I write to express concern about the current version of S.1223 – the Location Privacy Protection Act of 2011. At the outset, ETA applauds this well-meaning effort to address domestic violence and child protection through modifications to the United States Code. Our comments expressed herein on this Bill are in no way intended to address those important policy considerations; rather, our concern is with the unintended consequences of stifling innovation in the nascent market of mobile payments.

ETA is the largest trade association representing the electronic payments industry. Founded as a non-profit association in 1990, ETA's more than 500 member companies make possible the acceptance and processing of credit and debit card transactions by the nation's merchants. In 2012, ETA member companies will process more than \$3.6 trillion in card transactions in the United States.

Since the deployment of credit cards more than 50 years ago, the payments industry has provided consumers with the safest, most reliable and convenient means of making purchases at the widest possible variety of merchants. Consumers in the U.S. have more than one billion credit and debit cards in their wallets, a testament to this preferred method of payment.

Consumers in the U.S. are also enjoying robust adoption and use of mobile phones. According to industry statistics, there are currently more mobile phone subscriptions in the U.S. – more than 320 million -- than the total population of the United States. Importantly, an unprecedented level of innovation in the payments industry today is promising to combine consumers' love of their mobile phones with the trusted, secure and convenient payment card networks through the deployment of mobile payments.

In brief, mobile payments permit consumers to use their mobile phones to initiate a payment in place of the time-honored plastic credit or debit card. The payments industry is providing enormous benefits to consumers through innovation in mobile payments, allowing for a safe and secure alternative to cash,

access to funds in geographically remote areas, secure storage of payment credentials, electronically transmitted discounts, offers, and loyalty rewards, and much more.

As with a traditional payments transaction, numerous companies are involved in the processing of a credit or debit card transaction that is initiated using a mobile device – from the consumer’s card issuer to the mobile wallet provider to the mobile network operator to the card processor to the card network and more. The payments industry works diligently with merchants, consumers and numerous government agencies to fight against fraudulent use of payment cards. The industry uses multiple tools and devotes significant resources to anti-fraud measures. One important component of these efforts is based on location information – so-called “card present” transactions – that facilitate verification of transaction information based on the consumer’s presence on the merchant’s premises. Such “card present” transactions not only prevent fraudulent card use because the customer can be verified more readily, they can also lower costs to merchants for processing the transaction.

As currently constituted, S.1223 could prevent merchants and card networks from ensuring the validity of a payment transaction initiated from a mobile device if the consumer has not given “express authorization” that payment transaction information – the same information that would be transmitted if the consumer were using a plastic credit or debit card – be used by the payments network and merchant to verify the transaction. For example, one significant consumer benefit driving the adoption of mobile payments is the ability of merchants to make coupon, loyalty and other discounts available to consumers based on customer location. A consumer might receive a \$3 discount on the purchase of lunch at a nearby food truck, a discount offer automatically incorporated into the consumer’s mobile wallet so the discount can be processed when payment is made. But the offer of such discounts is based on the consumer’s proximity to a small business (like a food truck) at which the consumer might not yet have eaten – and therefore could not have given “express authorization” for geolocation information, as required by S.1223, to be utilized to save the consumer money. This would be the case even though the consumer seeks to do nothing more than use a mobile phone to initiate a credit or debit card transaction – in essence, to use their phone in place of “swiping” a card. But S.1223, if enacted, could prevent the transmission of the location information necessary in a transaction to verify the validity of the payment credentials, incorporate the discount offer, and process the transaction. In other words, a primary advantage of consumer use of mobile wallets could be unavailable to consumers.

Moreover, the consumer engaging in a mobile payments transaction does not necessarily have a direct business relationship – and therefore would be unable to provide or would be unaware of the need to provide – consent with each company involved in the processing of such a payments transaction. For example, the merchant has a business relationship with its “acquirer” – the financial institution that sponsors the merchant’s acceptance of payment cards – and may have a separate relationship with a processor, which in turn interfaces with the card networks for transaction verification. The consumer has no direct relationship with either of these parties to the card transaction, yet all must engage with the consumer’s payment credentials – including, in “card-present” transactions, the location of the customer – to process the transaction. Lacking such a relationship with the consumer, payments networks and processors could not seek the “express authorization” of the consumer required by S.1223 as drafted, and therefore many mobile payments could not be processed.

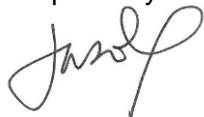
Given the lack of applicability to payments transactions of any of the delineated exceptions in the Bill, and further given the severe financial penalties that can apply under Section 3 of the Bill, this well-intended legislation could have the deleterious effect of stifling nascent innovation in this vital industry segment. Consumers will benefit from innovation in mobile payments and digital wallets, but as with most intelligent applications on mobile phones, the true utility and functionality of such payments innovation is inherently dependent on the location of the mobile device.

In addition to the concerns noted herein, it is also important to note that there are numerous industry efforts already underway to explore voluntary standards that meet the needs of consumers to be informed about any personal information used by mobile apps. For example, the U.S. Department of Commerce, National Telecommunications and Information Administration (NTIA) is engaged in a series of privacy multi-stakeholder meetings to address mobile application transparency, including issues related to collection of location data by mobile apps. Such public/private partnerships to address consumer privacy issues could be derailed if S.1223 were enacted.

Finally, ETA itself, through its newly formed Mobile Payments Committee, is working diligently with dozens of industry participants to address the important issue of consumer protections in mobile payments services. In combination with NTIA and similar agency initiatives, such efforts as ETA's hold great promise for promoting innovation and consumer benefits while protecting consumer privacy.

On behalf of ETA, we appreciate the legislative effort to protect women and children against stalking and violence, and we would appreciate the opportunity to work with Committee staff to ensure that these important policy goals are addressed without impact to consumers seeking to use innovative new mobile payments technologies.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Jason Oxman". The signature is fluid and cursive, with the first name "Jason" being more prominent than the last name "Oxman".

Jason Oxman
CEO