

**Smart Card  
Alliance**

## **End-to-End Encryption and Chip Cards in the U.S. Payments Industry**

*A Smart Card Alliance Position Paper*

*Publication Date: September 2009*

*Publication Number: CMPC-09003*

**Smart Card Alliance**  
191 Clarksville Rd.  
Princeton Junction, NJ 08550  
[www.smartcardalliance.org](http://www.smartcardalliance.org)

## ***About the Smart Card Alliance***

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit <http://www.smartcardalliance.org>.

Copyright © 2009 Smart Card Alliance, Inc. All rights reserved. Reproduction or distribution of this publication in any form is forbidden without prior permission from the Smart Card Alliance. The Smart Card Alliance has used best efforts to ensure, but cannot guarantee, that the information described in this report is accurate as of the publication date. The Smart Card Alliance disclaims all warranties as to the accuracy, completeness or adequacy of information in this report.

**TABLE OF CONTENTS**

- 1 INTRODUCTION ..... 4**
- 2 WHAT IS END-TO-END ENCRYPTION? ..... 5**
  - 2.1 WHY IS THERE INTEREST IN END-TO-END ENCRYPTION NOW? ..... 6
  - 2.2 PERSPECTIVE: PANACEA OR GRASS HUT? ..... 6
  - 2.3 PERSPECTIVE: UNDERSTANDING THE MERCHANT DILEMMA..... 7
- 3 TRUE END-TO-END DATA PROTECTION: CONTACTLESS CHIP CARDS AND ONLINE DYNAMIC CRYPTOGRAMS..... 8**
- 4 SMART CARD ALLIANCE POSITION ..... 10**
- 5 PUBLICATION ACKNOWLEDGEMENTS..... 12**

# 1 Introduction

Recent and highly publicized data breaches at merchants and processors involving payment cardholder data have had a significant impact on the payments industry. For example, *Wired* magazine reported that Heartland Payment Systems estimates that the breach it experienced in 2008 has conservatively cost the company in excess of \$12 million.<sup>1</sup> According to *Bank Info Security* magazine, the breach impacted at least 659 banks and credit unions.<sup>2</sup>

Analysis of the attacks has led to a flurry of interest in the implementation of end-to-end encryption solutions to protect cardholder data. Electronic payments industry stakeholders are taking action to address data security problems through the Accredited Standards Committee X9 (ASC X9) by embarking on the development of a new standard to protect cardholder data with end-to-end encryption.<sup>3</sup> This paper presents the Smart Card Alliance perspectives on this initiative.

Encryption of data would make it much harder for attackers to benefit from the kind of network break-in that Heartland suffered. Since sensitive data was not sufficiently protected, cyber-thieves were capable of stealing millions of debit and credit card details for several months after initially infiltrating the Heartland computer systems.<sup>4</sup>

Supporters of end-to-end encryption envision that cardholder data would be encrypted from the moment the magnetic stripe of the payment card is swiped through the end of the payment processing cycle. The devil is in the details, however. End-to-end encryption does not necessarily mean the same thing to all people, and the payments industry has not yet defined standards.

This position paper attempts to clarify and define end-to-end encryption, and detail the problems it solves and those it does not. It also explores the advantages of an alternative strategy for protecting cardholder data—moving data protection to the true endpoint, the payment card itself, using chip card technology.

Instead of implementing “chip and PIN” and following the full EMV standard, this paper proposes a new course optimized for the U.S. market: using contactless chip cards, including a dynamic cryptogram with each transaction and authorizing transactions online.

The existing U.S. payments infrastructure can process such transactions today in the same way that current contactless payment transactions are accepted.

Compared to end-to-end encryption, contactless cards with dynamic cryptograms would have the following advantages:

- Result in less impact on the payments acceptance infrastructure for merchants, acquirers and issuers
- Enable merchants to implement a solution more quickly and without waiting for new standards
- Provide a high level of cardholder data protection by including a dynamic cryptogram with each transaction
- Reduce the threats posed by cloning magnetic stripe-based cards and stealing cardholder data

The Smart Card Alliance is making another important recommendation as well. If the industry does indeed move forward with end-to-end encryption, the standard should be defined in a way that lays the messaging foundation for globally-interoperable secure payment transactions using chip card technology in the future. This would have no impact on end-to-end encryption cost or complexity, and yet would make the U.S. payments messaging standard compatible with global payments infrastructure requirements.

---

<sup>1</sup> “Heartland Breach Cost Company \$12.6 Million So Far,” Kim Zetter, *Wired*, May 7, 2009, <http://www.wired.com/threatlevel/2009/05/heartland-breach-cost-company-126-million-so-far/>

<sup>2</sup> “Heartland Data Breach Update,” Linda McGlasson, *Bank Information Security*, February 12, 2009, [http://www.bankinfosecurity.com/articles.php?art\\_id=1200&opg=1](http://www.bankinfosecurity.com/articles.php?art_id=1200&opg=1)

<sup>3</sup> “Accredited Standards Committee X9 Developing New Merchant Data Security Technology Standards,” press release, April 29, 2009, <http://www.heartlandpaymentsystems.com/article.aspx?id=1782>

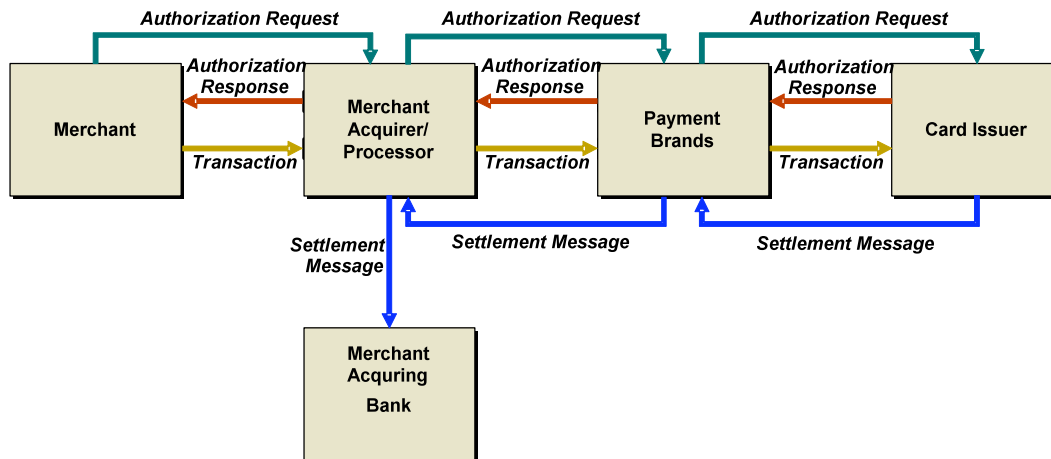
<sup>4</sup> “Three Indicted in Major Hacking Case,” Kim Zetter, *Wired*, August 17, 2009, <http://www.wired.com/threatlevel/2009/08/tjx-hacker-charged-with-heartland/>

## 2 What Is End-To-End Encryption?

The *Computer Desktop Encyclopedia* defines end-to-end encryption as the continuous protection of the confidentiality and integrity of transmitted information by encrypting it at the origin and decrypting it at its destination.<sup>5</sup>

A reasonably good example of true end-to-end encryption is the distribution of a secret key under a Key Exchange Key (KEK) process between two hardware security modules (HSMs). The KEK process is a common practice in many industries including government, telecommunications and banking, in applications where end-to-end security must be ensured. Using this technique, the secret key is never seen in the clear outside of the two endpoints. The first HSM (the origin) encrypts the secret key using the Key Exchange Key then the encrypted key can be securely sent to the second HSM (the destination) where it is decrypted.

With respect to a payment transaction, “origin” and “destination” are not single places, causing the potential for confusion. There are many temporary endpoints in a transaction lifecycle where all or part of the transaction information is required. In addition, there are several processes, starting with authorization and settlement; but data may be used or stored for refunds, chargebacks or reporting purposes in other places as well. The figure below illustrates a generic credit card transaction process today.



According to end-to-end encryption proponents, end-to-end encryption in the brick-and-mortar space would ensure that cardholder data is protected from the card swipe all the way through to the issuing banks. To do this, the magnetic card reader would be required to encrypt cardholder information immediately after the swipe and before any transmission, even inside the merchant location. This in itself may present challenges because the account number contains the information needed to route the transaction, requiring at least a portion of the data to be in the clear. In addition, other stakeholders require access to account and transaction information. For example, loyalty providers use transaction and cardholder data to create and track loyalty points for cardholders. For these reasons, end-to-end encryption is somewhat of a misnomer and may be misleading.

The term end-to-end encryption, however, has become a catchall for the encryption of sensitive cardholder data as it is transmitted from the point of sale entry point through each of the various organizations and networks in the payments process. Initially, much of the focus may center on data at rest on merchant servers or processor databases.

The true endpoint in the payments process is the data on the magnetic stripe that is static and always in the clear on the card, and therefore vulnerable to skimming and cloning. Preventing these attacks would require the use of chip cards or similar technology in order to better protect cardholder data.

<sup>5</sup> *Computer Desktop Encyclopedia*, www.answers.com, <http://www.answers.com/topic/end-to-end-encryption>

## 2.1 Why Is There Interest in End-To-End Encryption Now?

Traditionally hackers have focused on compromising databases of sensitive information through SQL injection, privilege abuse or other platform vulnerabilities. More recently, analysis of data breach incidents shows that cyber criminals have focused on stealing cardholder data in transit. Visa has also recently warned against "packet sniffing" in which hackers use malware to intercept and collect data while it is in transit.<sup>6</sup>

As a result, electronic payments industry stakeholders are taking action to address data security problems through the American National Standards Institute (ANSI) Accredited Standards Committee X9 (ASC X9) by embarking on the development of a new standard to protect cardholder data with end-to-end encryption. The mandate of ASC X9 is to develop and maintain standards for financial services in the U.S. Among other things, ASC X9 was responsible for creating the standards for PIN encryption.

The ASC X9 started this work in April, 2009. As of September 1, 2009, the committee had not decided if a standard or a technical report is needed. Another open question is whether to build a standard on top of Payment Card Industry Data Security Standard (PCI DSS)<sup>7</sup> or provide an independent work item.

As a first priority, the group must determine the definition of end-to-end encryption in the payments industry. For example, does end-to-end mean terminal to acquirer, terminal to payment brand or all the way from terminal to the issuer? Defining encryption throughout the transaction life cycle including authorization, clearing, settlement, disputes and reporting is equally important.

Other questions to resolve include the following:

- Which portions of the payment transaction should be covered by end-to-end encryption and the ASC X9 efforts?
- How is the transaction data needed for transaction routing made usable while still protecting cardholder data?
- How is encrypted data shared among all of the stakeholders in the transaction flow, including merchants, acquirers, aggregators, payment brands, issuers and other value-added service providers serving the retail market (e.g., loyalty program providers)?
- Within each stakeholder, how is encrypted data handled in all stages of the transaction, from authorization, clearing and settlement to reporting and chargebacks?

In the face of all of these issues, it is the Smart Card Alliance's position that it is likely that industry standards for comprehensive end-to-end encryption will take considerable time to develop and implement.

## 2.2 Perspective: Panacea or Grass Hut?

There is no doubt that encrypting sensitive data would make merchants and processors more secure and resistant to the types of recent attacks that resulted in large data breaches. As industry specialists look deeper into what end-to-end encryption means, however, three major considerations arise.

One important question is: *Will end-to-end encryption eliminate the chance that stolen cardholder data can be used successfully for fraudulent transactions?* The answer, unfortunately, is no.

There is an old saying in the security industry that you cannot secure a grass hut with a steel door. In other words, if you harden the merchant and processor systems with end-to-end encryption, criminals may simply skim magnetic stripe data elsewhere. Imagine hordes of credit card magnetic stripe skimmers in the hands of restaurant employees. Or criminals using false fronts on ATMs in the U.K. to capture magnetic stripe and PINs, and then sending cloned magnetic stripe data to the U.S. for fraudulent attacks, as was done recently on a large scale.

---

<sup>6</sup> Visa Data Security Alert, *Top Vulnerability—Packet Sniffing*, February 2, 2009; [http://usa.visa.com/download/merchants/20090202\\_packet\\_sniffing.pdf](http://usa.visa.com/download/merchants/20090202_packet_sniffing.pdf)

<sup>7</sup> Additional information is available at <https://www.pcisecuritystandards.org/>

End-to-end encryption does not eliminate the risk of card cloning. Current U.S. payment process security mechanisms rely heavily on host neural networks, velocity checking and other sophisticated methods to identify fraud; however, as long as anyone can record the magnetic stripe, the ability to create a counterfeit card exists.

A second important question: *What are the complexities and costs of end-to-end encryption?* No one can answer that question today because there is no standards-based technical approach that has been fully vetted. The merchant impact has also not been defined. For end-to-end encryption to be successful, merchants would need to implement new functionality to encrypt data at the point-of-payment, while retaining the capability to use transaction data for other functions. POS terminal upgrades would likely be required, including software changes and capabilities to manage encryption keys.

Dynamic end-to-end encryption would also require a robust key management scheme. Merchants would likely not want to contend with the added complexity of this critical element, and any issues with synchronization and using the correct keys could lead to issues with authorizing transactions.

A third consideration is that the implementation of a new end-to-end encryption standard would once again send the U.S. payments industry in a different direction from the rest of the world, which is implementing chip card technology as a fundamental security measure. The U.S. magnetic stripe acceptance infrastructure already creates an opportunity for criminals to export fraud into the United States. For example, according to the U.K. Payments Administration (formerly APACS), chip cards decreased counterfeit card fraud domestically by 32% in 2007; however, counterfeit card fraud increased by 46% overall, to £144.3 million, “due to fraudsters copying U.K. cards and using these stolen cards in countries which do not yet have chip and PIN.” This trend continued in 2008, and APACS reported that exported fraud has nearly doubled in two years.<sup>8</sup> End-to-end encryption would not address the problem of counterfeit magnetic stripe cards, and would not complement global efforts to fight fraud with chip cards.

### **2.3 Perspective: Understanding the Merchant Dilemma**

Regardless, it is vitally important to understand that, from the processor and merchant perspective, encryption is a powerful weapon in the war against external cyber attacks. Bringing these weapons to bear quickly should be a top priority for the industry.

In the short term, the industry should focus on not storing magnetic stripe data in the first place, unless there is a significant, compelling business reason to do so. If magnetic stripe data does need to be stored or transmitted for business reasons, the industry should focus on implementing encryption technology where it makes sense and where it can be done quickly using off-the-shelf technology. A good place to start is encrypting data where it is most vulnerable. Store-level, merchant-wide and merchant-to-acquirer networks should use VPNs, if they are not already, and be sure that wireless networks have the latest WPA security. Where transaction information must be stored, it should be encrypted.

What must be examined carefully, however, is the idea of truly extending encryption from end-to-end in the U.S. payment transaction system. End-to-end encryption will require changes to the payments infrastructure -- both at merchants and in the processing system. Considerable investment has already been made in complying with PCI DSS, and while great strides have been made, some vulnerabilities will always remain and new threats are constantly emerging. What guarantee is there that end-to-end encryption will have a different result? The nature of crime is that it always seeks the weakest point. If the stakeholders make the investment and put end-to-end encryption in place, will they have put a steel door on a grass hut?

The answer is yes. End-to-end encryption still leaves the United States with a payments infrastructure that has a glaring weakness—the magnetic stripe. Criminals will find other ways to steal magnetic stripe information and perpetrate card-based fraud.

A more effective way to solve the cardholder data security problem is to implement on-card data protection using chip card technology, which is the subject of the next section.

---

<sup>8</sup> U.K. Payments Administration, “Card Fraud Facts and Figures,”  
[http://www.apacs.org.uk/resources\\_publications/card\\_fraud\\_facts\\_and\\_figures.html](http://www.apacs.org.uk/resources_publications/card_fraud_facts_and_figures.html)

### 3 True End-to-End Data Protection: Contactless Chip Cards and Online Dynamic Cryptograms

In the ongoing battle against cyber crime, a real solution to data breaches and other attacks on payment card data can be achieved by rendering transaction data useless for fraudulent transactions, using contactless chip card technology and online dynamic cryptograms. This approach has two important advantages:

1. It renders stolen cardholder data useless to criminals in retail locations.
2. The existing U.S. payments infrastructure can process such transactions today, as it does for contactless payment.

Most of the rest of the world is following the EMV standard, which implements a microprocessor chip on payment cards as a security measure. In many cases, a PIN entry is also required, sometimes called "chip and PIN." As of Q1 2008, more than 730 million EMV compliant chip-based payment cards were in use worldwide.<sup>9</sup>

EMV was defined for the global payments market, however, and some aspects of this standard are not needed for the U.S. market. In particular, EMV defines a mechanism for offline card authentication by the terminal. To do this securely adds the costs of a cryptographic coprocessor in the card and the complexity of public key certificate management at the merchant terminal.

U.S. critics of EMV chip card implementation have long argued that the merchant terminal implementation costs and the complexity of key management made chip cards prohibitively expensive. Yet, advocates of end-to-end encryption are in effect calling for similar changes to the payments infrastructure.

The Smart Card Alliance is proposing another option for the U.S. payments market that has clear benefits over both EMV "chip and PIN" and end-to-end encryption: Use contactless chip cards, include a dynamic cryptogram with each transaction and authorize transactions online.

The U.S. payments industry supports contactless payment transactions with three-digit, online dynamic cryptograms today.<sup>10</sup> Combining this with velocity checking in all credit and debit card processing would be a very effective barrier to counterfeit card fraud.

The cryptogram itself is a type of digital signature that works in conjunction with traditional magnetic stripe data. The cryptogram is a value based on specific inputs for an individual card and transaction that makes each transaction unique. Since only the chip card itself can create a valid cryptogram, the authorizing host can confirm that the actual card is present. In addition, the cryptogram is generated using secret keys inside the chip card, so key management is not required for merchants. The card issuer controls key management entirely.

An online dynamic cryptogram completely achieves the conceptual goal of end-to-end encryption. By making the payment card chip an active part of transaction authorization using dynamic cryptograms, stolen cardholder data cannot be used for fraudulent transactions at merchant locations, where a significant portion of fraud still takes place today.

An online dynamic cryptogram could also prevent card-not-present (CNP) online fraud, which is essential to effectively combating fraud. This would require an application in the chip such as MasterCard Chip Authentication Program (CAP) or Visa Dynamic Passcode Authentication (DPA), standards that are already defined. These applications enable a cardholder to use a handheld device to generate the cryptogram signature. Web merchants would pass this unique-per-transaction value to the issuer. The beauty of this approach is that it would provide proof that the card was in possession of the person performing the transaction. Further, since the transaction would have the same online dynamic cryptogram protection, fraudsters would not be able to use stolen cardholder data.

---

<sup>9</sup> See <http://www.emvco.com> for more information.

<sup>10</sup> "What Makes a Smart Card Secure," a white paper from the Smart Card Alliance Contactless and Mobile Payments Council at <http://www.smartcardalliance.org/pages/publications-smart-card-security>.

It should be noted that the proposal to use online dynamic cryptograms is consistent with well-established global standards for chip cards. Issuers that want to provide clients with an internationally compatible card could issue dual-interface contact/contactless cards that are also EMV compatible.

## 4 Smart Card Alliance Position

Many industry experts agree that building end-to-end encryption capabilities is an important step in securing the payments infrastructure. However, it is unlikely that any of these same experts believe it will solve all of the security issues that Heartland and other payment processors face from hackers. According to Tom Wills, senior analyst, Security, Fraud & Compliance, Javelin Strategy and Research, it will be expensive and a big logistical challenge to execute.<sup>11</sup> The Smart Card Alliance agrees with this assessment.

Moreover, several industry experts have expressed the concern that fraud rings will simply skim card data elsewhere. Crime syndicates typically use less than three percent of the card data they steal. So a standalone skimming device at a restaurant or even attached to an "end-to-end encrypted" terminal at a local "mom and pop" store will harvest more than enough data for their needs. A recent incident in New York proves this point rather conclusively; criminals used skimming devices attached to ATMs to steal some \$1.8 million in a few days.<sup>12</sup>

Outside of the United States, many countries are turning to chip cards to solve their payment security issues, which means that end-to-end encryption in the U.S. would be a local rather than a global solution. If the U.S., the world's largest economy, moves in a direction of chip-based payment cards compatible with global standards, the entire global payments infrastructure can be made more secure.

The Smart Card Alliance firmly believes in promoting the use of chip card technology to reduce fraud using strong authentication. History has shown that if crime rings cannot steal data simply and cheaply by hacking into unprotected databases, they will find other places to do so. Thus over the longer term, solutions need to incorporate a dynamic cryptogram in every transaction and chip cards are a proven way to accomplish this. Many countries have already implemented chip cards on a large scale, providing many case studies for research. The Smart Card Alliance supports efforts to make payment cardholder data more secure, especially for data at rest, but its strongest message is that any investments made for end-to-end encryption must also lay the foundation for a globally-interoperable chip card-based solution to fight fraud effectively in the long term.

For these reasons, the Smart Card Alliance recommends that U.S. stakeholders who are examining end-to-end encryption also consider using contactless chip cards, including a dynamic cryptogram with each transaction and authorizing transactions online.

Compared to EMV "chip and PIN," a U.S. contactless online-only implementation:

- Lowers the cost of the cards since a crypto-coprocessor is not required
- Eliminates the need for key management at the merchant terminal by using online cryptogram verification
- Uses the existing contactless infrastructure that is already in place in many retailers
- Readies the payments acceptance infrastructure for mobile NFC payments
- Works with existing transaction processing networks
- Can be coupled with contactless payment, an attractive payment product for consumers
- Achieves the goal of eliminating fraud from cloned cards
- Can be used with a handheld reader or with a mobile application to eliminate CNP fraud
- Supports issuers who want to offer globally-interoperable chip cards

---

<sup>11</sup> "Heartland Data Breach: Is End-to-End Encryption the Answer?," Linda McGalsson, *Bank Info Security*, May 11, 2009, [http://www.bankinfosecurity.com/articles.php?art\\_id=1455&opg=1](http://www.bankinfosecurity.com/articles.php?art_id=1455&opg=1)

<sup>12</sup> "Romanian Men Charged in ATM Scam in Cicero," Sue Weibezahl Porter, *The Post-Standard*, May 11, 2009, [http://www.syracuse.com/news/index.ssf/2009/05/romenian\\_men\\_charged\\_in\\_atm\\_sc.html](http://www.syracuse.com/news/index.ssf/2009/05/romenian_men_charged_in_atm_sc.html)

When examined side-by-side with end-to-end encryption, a strategy based on chip cards and online dynamic cryptograms would have these advantages:

- Have less impact on the payments acceptance infrastructure for merchants, acquirers and issuers
- Enable merchants to implement a solution more quickly and without waiting for new standards
- Provide a high level of cardholder data protection by including a dynamic cryptogram with each transaction
- Reduce the threats posed by cloning magnetic stripe-based cards and stealing cardholder data
- Provide a mechanism to use to fight CNP online fraud

The Smart Card Alliance is making another important recommendation as well. If the industry does indeed move forward with end-to-end encryption, the messaging standard should be defined in a way that lays the foundation for more secure payment transactions using chip card technology in the future. This would have no impact on end-to-end encryption cost or complexity, and yet would make the U.S. payments messaging standard compatible with global payments infrastructure requirements.

As attackers become more sophisticated, the U.S. may need to move to a stronger (and longer) cryptogram. The transmission of the longer cryptogram requires changes to the merchant network infrastructure. The ASC X9 end-to-end encryption project would involve changes to the messaging format and infrastructure as well. If the industry does move forward with end-to-end encryption, it is imperative to include the changes in message formats that support strong authentication using an EMV-compliant cryptogram. It would be very short sighted not to include the foundation for globally-interoperable chip cards as part of any ASC X9 standard for end-to-end encryption.

## **5 Publication Acknowledgements**

This position paper was developed by the Smart Card Alliance to present Smart Card Alliance perspectives on end-to-end encryption and to discuss how chip cards and dynamic cryptograms address card-based fraud. Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance thanks the Contactless and Mobile Payments Council members for their contributions to the development of this position paper.

### **About the Smart Card Alliance Contactless and Mobile Payments Council**

The Contactless and Mobile Payments Council is one of several Smart Card Alliance technology and industry councils. The Council was formed to focus on facilitating the adoption of contactless and mobile payments in the U.S. through education programs for consumers, merchants and issuers. The group is bringing together financial payments industry leaders, merchants and suppliers. The Council's primary goal is to inform and educate the market about the value of contactless and mobile payment and work to address misconceptions about the capabilities and security of contactless technology. Council participation is open to any Smart Card Alliance member who wishes to contribute to the Council projects.

### **Trademark Notice**

All registered trademarks, trademarks, or service marks are the property of their respective owners.