Health & Human Services Council
WHITE PAPER
Smart Card Alliance

A SMART CARD ALLIANCE HEALTH AND HUMAN SERVICES COUNCIL WHITE PAPER

EMV 101 for the Healthcare Industry

Publication Date: September 2015
Publication Number: HHSC-15001

Smart Card Alliance

191 Clarksville Rd.
Princeton Junction, NJ 08550

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.

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. This white paper does not endorse any specific product or service. Product or service references are provided to illustrate the points being made.

Smart Card Alliance

Table of Contents

1 Introduction

The payments industry in the United States is migrating to EMV chip technology, replacing the magnetic-stripe bank cards and point-of-sale (POS) terminals that have been in use for decades. EMV-compliant chip cards offer better security for card-present transactions by making every transaction unique. In addition, chip cards are more difficult to counterfeit or copy.

This white paper provides an overview of EMV chip technology to help prepare the healthcare industry for EMV migration. The white paper provides the following information:

- What EMV chip technology is and why it is important for card-present payment transactions
- What the impact of EMV is for healthcare providers and hospital systems
- How healthcare providers and hospital systems can prepare for EMV chip technology

Additional information about EMV chip technology is available from two web sites:

- GoChipCard.com, which provides easy-to-understand educational content for consumers, merchants, and issuers
- EMV-Connection.com, which provides detailed educational resources for the entire payments industry

Healthcare providers and hospital systems are also encouraged to contact their bank card acquirers and POS solution vendors for assistance in planning for EMV migration.

2 What Is EMV?

The process of paying with a credit or debit card in the United States is changing. The U.S. is moving to the use of chip cards based on a global payment standard, EMV, that is already implemented in 3.5 billion payment cards in more than 80 countries worldwide. EMV chip cards (Figure 1) contain secure computer chips that validate the authenticity of the card and include a one-time security code in every transaction, making chip payment data virtually impossible to use for counterfeit card fraud.

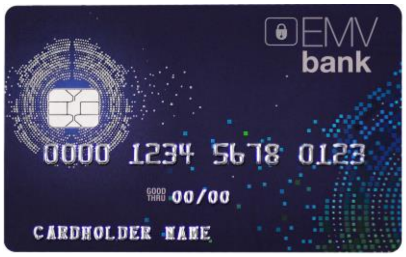
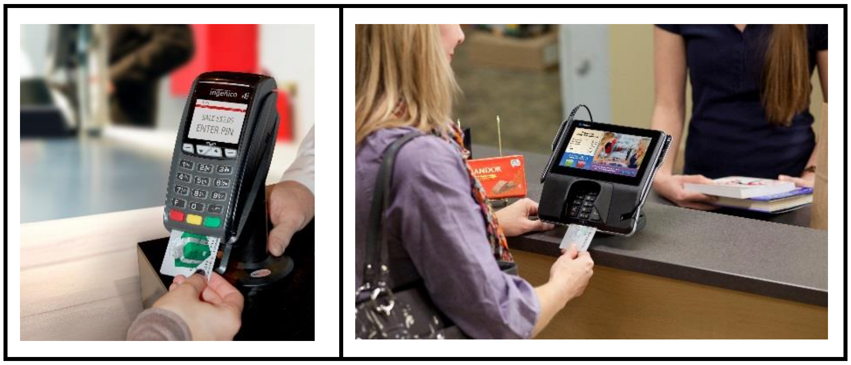


Figure 1. Example of an EMV Chip Card

The move to EMV chip card payment in the U.S. is driven by the desire to reduce the incidence of card fraud in card-present transactions, provide global interoperability, and enable safer transactions across contact and contactless channels. According to the EMV Migration Forum, by the end of 2015 a total of 50 percent of all cards issued in the U.S. (600 million cards) will be chip cards and 60 percent of all point-of-sale (POS) terminals in the U.S. (7 million terminals) will be enabled to accept chip cards.

To accept EMV chip credit and debit cards, businesses need to update their payment terminal to be chip-enabled. To pay using a chip card, the cardholder inserts the card into the terminal rather than swiping it. Chip-enabled terminals (Figure 2) include all of the features of a traditional payment terminal and incorporate the slot in which to insert the card.



Source: Ingenico and Verifone

Figure 2. Using a Chip-Enabled POS Terminal

While businesses are not required to accept chip cards, the U.S. payments industry is focused on moving quickly to the use of chip cards and appropriate acceptance terminals to reduce card-present fraud. The global payment networks and certain U.S. debit networks are encouraging both issuers and merchants to migrate to EMV chip technology by shifting fraud liability starting in October 2015. These liability shifts will affect both counterfeit card transactions and certain lost or stolen card transactions.

Currently, issuers bear the risk when a card-present transaction is counterfeit. Beginning in October 2015, if a merchant accepts a magnetic stripe card that was counterfeited using track data copied from the magnetic stripe of an EMV chip card and the merchant does not have a POS terminal that is EMV chip-enabled, the merchant or the acquirer may be liable for the fraudulent transaction. The counterfeit card fraud liability shift applies for all global payment networks (American Express, China Unionpay, Discover, MasterCard and Visa) and certain U.S. debit networks. American Express, Discover, and MasterCard also have a liability shift for lost or stolen PIN-preferring chip cards used at less secure acceptance devices.

Adopting EMV chip technology creates a more secure card-present payments environment and reduces a business's liability for fraudulent transactions.

3 Impact of EMV on Healthcare Providers and Hospital Systems

The fraud liability shift that is scheduled to occur in October 2015 (described in the previous section) represents a major change for U.S. businesses. The liability for counterfeit card-present credit or debit card fraud will be borne by whichever party does not support EMV chip card transactions. Three areas that are impacted by EMV chip acceptance and that are of particular importance to physicians, dentists, orthodontists, other providers, and hospital systems are:

- Consumer/patient receivables
- Consumer/patient experience
- Financial data security

3.1 Consumer/Patient Receivables

Most healthcare providers have seen a dramatic increase in the number of patients paying with a payment card at the time of service. They have also seen a significant increase in the dollar amount of those transactions. These increases are caused by a steady rise in high deductible insurance plans and improvement in the tools used to estimate payment amounts and perform real-time adjudication.

For healthcare providers and healthcare systems, the changes in payment type and amount increase the threat of fraudulent and counterfeit card transactions. After October 2015, healthcare providers and systems could become liable for fraudulent transactions while experiencing a spike in the incidence of such transactions. By understanding and implementing an EMV-capable payment process, healthcare providers can dramatically reduce the risk of fraudulent card-present payments.

3.2 Consumer/Patient Experience

The growth of high deductible healthcare plans has led to increases in the amount consumers pay for services and the need for providers to be consumer-focused beyond delivering superior patient care. Superior care must be extended to patient payments.

Providers also need to be prepared to accept consumer payments in all forms, including EMV chip cards for in-person transactions as well as mobile and digital transactions. Consumers have already begun using EMV chip cards at many national merchants (such as Walmart, Target and Home Depot), regional merchants and local shops and restaurants. Given the speed at which they are adopting the new cards, consumers (patients) will expect to be able to use their EMV chip cards at healthcare providers as well.

3.3 Financial Data Security

Security is "top of mind" for all parties in the healthcare ecosystem. With the rapid growth of consumer payments, financial data security is a paramount concern as is continuing to protect and secure patient information.

The payments industry and payment networks recommend three components to help ensure card data security[1]:

1. EMV chip technology
2. Encryption
3. Tokenization technology

Chip cards used at EMV chip terminals protect against counterfeit transactions by replacing static data with dynamic data. Protection starts with a unique cryptogram. A one-time code validates card authenticity to the entire payment ecosystem. For a successful transaction, unique credentials must be presented and validated. Without validation, there is no transaction.

However, it is important for healthcare providers to protect consumer financial data through the entire system by using point-to-point or end-to-end encryption and tokenization. Encryption helps to protect cardholder data throughout the entire transaction, from the point of entry to the payment card processor and provides a shield against malware that can sniff and capture data. Tokenization replaces cardholder data with surrogate values, or tokens, allowing merchants to limit or eliminate the storage of cardholder data. This technology helps mitigate the risk of financial data breaches and reduces the scope for Payment Card Industry Data Security Standard (PCI DSS) compliance.

A layered approach to security incorporating all three technologies – EMV, encryption and tokenization – is a recommended payments industry best practice to more fully secure the payments infrastructure.

4 Getting Ready for EMV

From the perspective of the consumer and the payment card accepting business, the introduction of EMV chip technology marks a significant shift in the way card-present transactions are processed. Rather than being swiped, payment cards with an EMV chip are inserted into a slot in the chip-enabled POS device and must remain there for the length of the transaction. During the transaction the card is authenticated as valid and the use of a

[1] For additional information, see the Smart Card Alliance white paper, "Technologies for Payment Fraud Prevention: EMV, Encryption and Tokenization," available at http://www.smartcardalliance.org/publications-technologies-for-payment-fraud-prevention-emv-encryption-and-tokenization/.

PIN or signature ensures that the person presenting the card is the rightful cardholder. It is important to remember that EMV chip cards are used only when the card is present. There is no change in the transaction process or liability for transactions when a physical card is not present (e.g., for telephone or Internet payments).

Most current POS solutions will require additional hardware to become EMV capable. The simplest upgrade is to add a PIN pad that contains a chip card insertion slot, typically located on the top or front of the pad. The addition of the PIN pad (and the proper software upgrade) should enable organizations to accept EMV chip cards and protect the organization from the liability shift scheduled for October 2015. Healthcare providers and hospital systems are advised to contact their POS solution provider for more information on the steps required to become EMV enabled.

When upgrading current POS systems to EMV, organizations should take the opportunity to look at their payment and point-of-service strategy to consider other payment types (e.g., mobile payments) and functionality that could be included in the upgrade.

The EMV payment process is new to both consumers and employees. Paying with an EMV chip card requires different actions by the consumer than paying with a magnetic stripe card. Early indications are that consumers adapt quickly to the new payment process, but education is a key component of successful conversion to EMV chip acceptance. Employees who interact with customers or card acceptance equipment will also need to become familiar with the chip card acceptance procedure. To assist in the education process, a cross-section of industry experts has created a website on the use and benefits of the EMV chip card. The website, www.GoChipCard.com, contains information and educational materials that can be used to train employees and consumers. The site contains an overview of EMV, an overview of the payment process, and a list of frequently asked questions. Most of the material on the site can be downloaded and placed near card acceptance equipment as a reference for customers and staff.

The United States is the last of the top 20 global economies to convert from magnetic stripe to EMV chip card payment. One benefit of this delayed conversion is that key lessons are available from other implementations that can ease the transition for U.S. consumers and businesses to the chip card payment process. Two of these lessons are:

- The number of cards left behind at the POS will increase.

  Consumers can no longer swipe and put a card away. The number of cards left behind typically increases during the early stages of EMV implementation.

- Customers learn quickly.

  As EMV chip cards become more common and national retailers implement EMV solutions, customers will become accustomed to the new payment process and start to expect it when they pay.

EMV is here to stay. The chip card process will become the new standard in the U.S., allowing American consumers to conform to a payment standard found throughout the rest of the world that is an integral part of the global payment process.

5 Conclusion

U.S. issuers and merchants are in the process of migrating to EMV chip card technology to improve the security of the card-present payments infrastructure. As a result, EMV is being rolled out to healthcare providers of all sizes, including small practices, large providers, and hospital systems.

The implementation of EMV requires EMV chip-enabled terminals for the acceptance of EMV credit and debit chip cards. For providers who have integrated bank card payment with other registration or administrative software, software updates may also be required.

The payments industry is experiencing many changes, of which EMV is just one. Mobile payment using smart phones and watches is becoming increasing popular. (Apple Pay^{TM} has already entered the mobile payments market, with Samsung and Google announcing plans to enter the market.) With the increasing popularity of these alternative payment solutions, many businesses have taken the opportunity to implement new POS systems that accommodate the changing payments landscape. These systems make merchants EMV capable and capable of accepting other payment types.

In addition, chip-enabled terminals can support multiple applications; for example, they could accept EMV chip credit and debit cards and also provide support for upcoming healthcare mobile and ID chip card acceptance.

Migrating to EMV chip card payment can reduce card-present fraud and improve overall payments security. Healthcare providers should consult their bank card acquirers and POS solution vendors to acquire EMV chip-enabled solutions and to start planning for EMV chip migration.

6 Publication Acknowledgements

This white paper was developed by the Smart Card Alliance Health and Human Services Council to provide an educational resource on EMV chip migration for the healthcare industry.

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 wishes to thank Health and Human Services Council members for their contributions. Participants involved in the development of this white paper included: ABnote; First Data Corporation; LifeMed ID Inc.; NXP Semiconductors; XTec, Inc.

The Smart Card Alliance thanks the Council members who participated in the project team to write the document, including:

- **Joan Christensen**, First Data Corporation
- **Kathleen Finnegan**, First Data Corporation
- **Thomas McNeila**, First Data Corporation
- **Cathy Medich**, Smart Card Alliance

The Smart Card Alliance also thanks Council members who participated in the review of the white paper including:

- **David Batchelor**, LifeMed ID Inc.
- **John Ekers**, ABnote
- **Peter Esser**, NXP Semiconductors
- **Morgan Richard**, XTec, Inc.
- **Bryan Russell**, XTec, Inc.
- **Kevin Sheehan**, First Data
- **Mike Strock**, Smart Card Alliance

Trademark Notice

About the Health and Human Services Council

The Smart Card Alliance Health and Human Services Council brings together human services organizations, payers, healthcare providers, and technologists to promote the adoption of smart cards in U.S. health and human services organizations and within the national health IT infrastructure. The Health and Human Services Council provides a forum where all stakeholders can collaborate to educate the market on the how smart cards can be used and to work on issues inhibiting the industry.