EMV Questions and Answers

Updated 2/6/13

The following is a listing of the most popular questions and their answers that SHAZAM has received to date on EMV (chip-and-PIN technology). We will update this document as additional questions are received. ***Please Note:*** *This document is not intended to be a definitive analysis of the subjects discussed or interpreted as legal advice.*

Question: What is EMV®?
Answer: EMV stands for Europay, MasterCard®, and Visa® and was developed in 1993; however, EMV commonly refers to a chip card used for payment technology. The ISO 7816 is the official standard for chip technology, much like magnetic stripe transactions are managed through the ISO 7813. The chip within the card stores cardholder and application data more securely, and the technology itself provides protection against card reproduction fraud. EMV cards can be contact or contactless. The EMV specifications are managed by EMVCo, which is a consortium currently made up of MasterCard, Visa, American Express® (AMEX), and JCB. SHAZAM is a business and technical associate of EMVCo.

Question: When will we be required/mandated to issue EMV cards?
Answer: There is currently no mandate to issue EMV cards. Each financial institution should consider developing a business case for determining when EMV support is necessary. One primary consideration is determining how many counterfeit fraud losses you incur. Please contact your SHAZAM Account Executive to weigh all options, including risks versus benefits.

Question: There are a lot of discussions regarding EMV and liability shifts. What do you mean by liability shift? How and when does it shift?
Answer: There are a number of liability shifts that different networks are imposing on issuing financial institutions (issuers) and acquiring financial institutions (acquirers). The dates and information on the liability shifts are listed in the table below. Remember that for a loss to occur, not only the card but also the PIN would need to be compromised.

Effective Date	Type of Liability Shift	Current Liability	Liability after Shift
April 2013	Maestro® ATM interregional transactions (foreign cardholders at U.S. ATMs)	Currently, the liability for fraud on an ATM transaction lies with the issuer.	Beginning in April 2013, if a foreign cardholder's magnetic stripe card is used at a U.S. ATM, the ATM is chip-enabled, and that magnetic stripe card is counterfeit, the foreign card issuer would be liable for that fraud. Conversely, if the card is a chip card, the ATM only accepts magnetic stripe cards, and there is fraud on that transaction, the U.S. ATM acquirer would be liable.
October 2015	Point-of-sale (POS) terminals	Currently, the liability for fraud on a POS	Beginning in October 2015, if a foreign or U.S. cardholder's magnetic

	for MasterCard, Visa, AMEX, Discover®, and PULSE®	transaction lies with the issuer.	stripe card is used at a POS device, the POS device is chip-enabled, and that magnetic stripe card is counterfeit, the issuer would be liable for that fraud. Conversely, if the card is a chip card, the POS device only accepts magnetic stripe cards, and there is fraud on that transaction, the acquirer/merchant would be liable.
October 2016	All MasterCard ATM transactions	Currently, the liability for fraud on an ATM transaction lies with the issuer.	Beginning in October 2016, if a foreign or U.S. cardholder's magnetic stripe card is used at an ATM, the ATM is chip-enabled, and that magnetic stripe card is counterfeit, the foreign or U.S. card issuer would be liable for that fraud. Conversely, if the card is a chip card, the ATM only accepts magnetic stripe cards, and there is fraud on that transaction, the ATM acquirer would be liable.
October 2017	All Visa ATM transactions	Currently, the liability for fraud on an ATM transaction lies with the issuer.	Beginning in October 2017, if a foreign or U.S. cardholder's magnetic stripe card is used at an ATM, the ATM is chip-enabled, and that magnetic stripe card is counterfeit, the foreign or U.S. card issuer would be liable for that fraud. Conversely, if the card is a chip card, the ATM only accepts magnetic stripe cards, and there is fraud on that transaction, the ATM acquirer would be liable.
October 2017	Automated fuel dispenser (AFD) transactions for MasterCard, Visa, AMEX, Discover, and PULSE	Currently, the liability for fraud on an AFD transaction lies with the issuer up to a certain dollar amount that is determined by the payment card network.	Beginning in October 2017, if a foreign or U.S. cardholder's magnetic stripe card is used at an AFD, the AFD is chip-enabled, and that magnetic stripe card is counterfeit, the issuer would be liable for that fraud. Conversely, if the card is a chip card, the AFD only accepts magnetic stripe cards, and there is fraud on that transaction, the acquirer/merchant would be liable.

If there is fraud on a transaction, the owner of the lesser technology between the card and the ATM/POS device is liable for the fraud.

Example 1:

1) A fraudster captures an ATM/POS chip-enabled card.
2) The fraudster creates a counterfeit ATM/debit card with the magnetic stripe information.
3) An ATM/POS transaction is performed at a chip-enabled ATM/POS device with the counterfeit card.
4) The liability falls to the issuer, as the counterfeit card is not chip-enabled but the ATM/POS device is, so the ATM/POS device has the greater technology.

Example 2:

1) A fraudster captures an ATM/debit chip-enabled card.
2) The fraudster creates a counterfeit ATM/debit card with the magnetic stripe information.
3) An ATM/POS transaction is performed at a non-chip-enabled ATM/POS device with the counterfeit card.
4) The liability falls to the ATM acquirer/merchant, as the counterfeit card is not-chip-enabled but neither is the ATM/POS device.

Question: Is there a date when ATMs must accept EMV?
Answer: No, there is no mandate for ATMs; there is only a liability shift, as described above.

Question: Are we being required/mandated to modify our ATMs to accept EMV transactions?
Answer: No, you are not required to modify your ATMs to accept EMV transactions. MasterCard is imposing liability shift dates as a way to give an incentive to financial institutions to move to chip-and-PIN technology. It is up to each individual financial institution to decide whether to upgrade ATMs. Some things to consider are as follows:

- How many international transactions do you see happening at your ATMs, as the initial liability shift is only applicable to international transactions? Are some of your ATMs located in high-traffic, foreign visitor areas (for example: the airport or a hotel)?
- Do you need to upgrade your ATM terminals in the near future? If you do, it is advisable to buy hardware that is EMV compatible to protect yourself from potential liability shifts and also in the event EMV terminal support is ever mandated. Your institution can buy chip-enabled card readers now but not turn them on until you have completed certification, are ready to accept chip transactions, and the industry resolves the Regulation II (the Durbin Amendment) and issuer portability issues that currently exist.
- What is the cost of supporting EMV-compatible terminals? **Please Note:** You will need to discuss pricing options with your ATM service provider.

SHAZAM will communicate more information on this in the near future.

Question: How is SHAZAM preparing for EMV?
Answer: SHAZAM has numerous enterprise-wide projects that will allow our customers to shift to EMV technology when they deem the time to be appropriate. The migration to EMV in other countries has taken more than a decade to accomplish for each country, most recently Canada. With the U.S. being the largest market in the world, the migration of EMV support could take more than a decade to fully complete. Although there will be early adopters and programs designed to incent issuers and acquirers to upgrade early, the business case to support EMV is not yet clear.

SHAZAM will work to meet industry mandates, when and if any should occur. Incentive programs provided by the various networks will be reviewed, but they will not be considered an industry mandate; they will be evaluated on a case-by-case basis. Some of the incentive programs are listed below. Although it is SHAZAM's intent to support all industry milestones, many of our partners may not be able to complete such tasks. There are also a number of issues in relation to transaction routing, Regulation II compliance, and issuer portability. The major industry stakeholders (with a goal to limit any significant duplication of effort) are discussing these issues.

- **April 2013 Maestro® ATM interregional liability shift date** — SHAZAM will work to support Diebold® and NCR® select terminal models for those acquirers that wish to upgrade their terminals.
- **April 2013 EMV acquirer-processor mandate from the international payment brands** — SHAZAM is in the process of updating our processing systems to support EMV transactions for both MasterCard and Visa. We will then certify our ability to process these transactions with the payment card networks.
- **October 2015 MasterCard, Visa, American Express (AMEX), and Discover® POS terminal liability shift date** — SHAZAM will work with all the major payment card networks to be ready for merchants to deploy a chip-capable POS terminal. Individual network availability may vary.
- **Rules and specifications** — SHAZAM is actively defining network rules and specifications to support EMV transactions for the SHAZAM brand. This will allow SHAZAM issuers to continue being Regulation II compliant. We will release these rules and specifications in early 2013.
- **Card issuance** — SHAZAM is working with chip-card providers and other industry partners to ensure we have the chip, plastic, and personalization services available. SHAZAM does have plans to pilot EMV travel card issuance beginning in the fall of 2013.

Question: When will the SHAZAM debit card application be ready for EMV?
Answer: Currently, there are a number of things going on within the industry to resolve Regulation II issues with EMV. Because of this, it is hard to pinpoint an exact date for the release of the SHAZAM debit card application; however, we anticipate it will happen in 2013-2014.

Question: Is SHAZAM working with card personalization vendors, such as Personix®, to ensure they are ready for the rollout of EMV?
Answer: Yes, SHAZAM is creating specifications to share with card personalization vendors, including Personix.

Question: How will EMV impact a cardholder's ability to select his or her own PIN after the card has been issued? Additionally, how will EMV impact the issuance of a new PIN for an existing card?
Answer: Cardholder PIN selection should work the same as it does today; however, it will become more complex if the issuer decides to support offline PIN. More details on this will be communicated at a later date.
Question: What does offline versus online mean?
Answer: We have described both below:

Online — 100 percent of transactions today are online. Online is a transaction processing method where the terminal sends the authorization request (via telecommunications connectivity) to the issuer-processor for approval in real time. The terminal and the issuer-processor communicate with each other. **Please Note:** Online transactions should not be confused with e-commerce or Internet-initiated transactions.

Offline — Offline is a transaction processing method where the authorization can take place at the terminal and does not need to be sent to the issuer-processor for authorization. The chip on the card (which includes parameters set by the issuer) and the terminal communicate with each other.

There are three communication variations for EMV:

- **Online or offline PIN** — When a cardholder inserts a chip card into a terminal, he or she is prompted for a PIN. The PIN can either be offline (meaning the chip card is going to verify the PIN), or it can be online (meaning the issuer verifies the PIN). However, for ATM EMV transactions, the PIN will always be verified online.

- **Online or offline card authentication method (CAM), meaning the validation of the card** — The card creates a cryptogram as part of the card authentication process to ensure that the card is not counterfeit. If this happens offline, the terminal and the card verify the cryptogram. If it happens online, the cryptogram is sent to the issuer for authentication. However, for ATM EMV transactions, the CAM will always be verified online.

- **Online or offline transaction authorization** — If the POS device does not have connectivity to the issuer for transaction authorization, the transaction could take place offline. In this case, the card would have dollar limits. It would also let the terminal know how high of a dollar amount and how many consecutive offline transactions can be done. If the card is unable to do an offline transaction, then the card would request that the POS device go online for authorization. However, for

ATM EMV transactions, the transaction authorization will always be verified online.

Question: What happens during a transaction if the merchant is not online but the issuer is online?
Answer: If the merchant is only able to process offline transactions and the card is an online only card, the transaction will not work. If a terminal is offline, the card would have to be called into the network or a paper ticket would need to be taken. If there is no connectivity between the merchant and the processor (for example: the connection is down), the transaction will process as it does today.

Question: Can you describe the process for an Internet EMV purchase?
Answer: The process is the same as it is today for a magnetic stripe card. During an Internet purchase, the cardholder would enter the primary account number (PAN), expiration date, and the security code on the back of the card. EMV does not protect against fraud on the Internet unless the financial institution and the merchant have enabled the ability to use special one-time password (OTP) hardware options. This technology is emerging and is not expected to be available for several years.

Question: Is it true that in some cases a terminal could prompt a cardholder to determine a payment card network to route the transaction?
Answer: Yes, this is true. The current implementation of EMV requires the terminal to either prompt the cardholder to select an application (network) or to pick the network based on the issuer priority that is associated with the card.

Question: Are merchants allowed to tell cardholders which network to choose?
Answer: Yes, merchants can try to steer cardholders per Regulation II. However, this conflicts with EMV. The following outlines this conflict.

The data on a chip card cannot just be read by a terminal as a magnetic stripe card is read. In order for the data on the chip card to be read, the terminal and the card must agree to use a mutually supported payment application. This process is called "application selection."

According to the EMV specifications, the terminal selects the application on a chip card by prompting the cardholder for the application preference or by defaulting to the application with the highest priority. Application priority is set by the issuer during personalization of the card in what is called the Application Priority Indicator. If the applications are presented to the cardholder, they are presented in priority order. This goes directly against the prohibitions stated in Section 235.7(b) of the regulation where it prohibits an issuer from directly or indirectly inhibiting the routing of debit transactions. If the terminal selects the application, the terminal is directed to select the common application that both the terminal and card mutually support based on the highest priority set by the issuer, through the Application Priority Indicator on the card.

The merchant does not get to choose which application on the card should be used in the transaction. The selection of an application at the terminal limits routing options. The routing options are limited to only those payment networks that are affiliated with the application that has been selected. The application selection also determines the cardholder verification method (CVM) available to the terminal. The selection of a CVM before determination of routing further constrains payment brand routing choice to only those routes supporting the CVM associated with the selected application.

Question: Does near field communication (NFC) have the same problems with Regulation II as EMV does as it relates to processer choice?
Answer: The short answer is yes. No matter which payment device is used, whether magnetic stripe, EMV, or a mobile phone, it must meet the requirements of Regulation II, which do the following:

- Prohibit issuers and payment card networks from restricting the number of payment card networks over which debit transactions may be processed to one network (or two affiliated networks)
- Prohibit issuers and networks from inhibiting the ability of a merchant to direct the routing of a debit transaction to any network that may process the transaction

Question: Will Hypercom® T7 Plus terminals be updated to support EMV processing?
Answer: No. Unfortunately, the terminal is no longer being manufactured and there are a limited amount of units available for sale/replacement.

Question: Is the greater liability for PIN-based transactions negative for issuers?
Answer: In reality, there is not any "greater liability" for PIN-based transactions versus signature-based transactions, as issuers are ultimately liable for the transaction amount. However, the overall fraud level is significantly lower than for signature-based fraud. It is a widely accepted fact within the electronic funds transfer (EFT) industry that PIN-debit transactions are the superior debit authorization method, as PIN debit results in less fraud for the industry. PIN-based fraud losses average approximately one basis point of the transaction amount compared to approximately seven basis points for signature-based transactions. For example: For every $1 million in transaction volume, $700.00 of that will be signature-based fraud losses. For PIN transactions, these losses would only equate to $100.00. Having PIN-based authentication saves financial institutions fraud losses in the long run.

Question: Is it true that contactless cards are easily counterfeited, as is shown in a YouTube video that has surfaced?
Answer: This risk is specific to contactless payment devices, which may or may not be EMV capable. Contactless payment devices contain secure microprocessors and memory and have the ability to perform cryptographic processing. Additionally, a contactless card must be held an inch or two away from a POS device to initiate a transaction. The YouTube video, referred to in the

question, shows a contactless device that uses the radio frequency identification (RFID) tags that are cheap and can work over longer distances. However, according to the white paper, "Contactless Payments Security Questions & Answers," the Smart Card Alliance states that it has only had this type of fraud occur in the demonstration and not in real life.

To read more about the security of contactless payments, please read the Smart Card Alliance white paper. It can be found by visiting: http://www.smartcardalliance.org/resources/pdf/Contactless_Payment_Security_QA.pdf.