JTC Resource Bulletin

EMV and Credit Card Liability: What Courts Need to Know

Version 1
Adopted December 5, 2014

Abstract

Nearly every country in the world uses the global standard called EMV (short for Europay, MasterCard, and Visa) for bankcard processing because of the technology's effectiveness in protecting cardholder data and reducing counterfeit, lost and stolen bankcard fraud. The US is finally making that shift. Merchants that accept bankcard payments (including courts) must implement devices that can read EMV chip-enabled cards by October 2015, or be liable for any fraudulent purchases made at their terminals. While addressing the requirements of EMV payment processing, courts should also evaluate the possibility of simultaneously incorporating other payment technologies, including contactless EMV and Near Field Communication (NFC).

Acknowledgments

This document is a product of the Joint Technology Committee (JTC) established by the Conference of State Court Administrators (COSCA), the National Association for Court Management (NACM) and the National Center for State Courts (NCSC).

JTC Mission:
To improve the administration of justice through technology

Joint Technology Committee:

COSCA Appointments

David Slayton (Co-Chair)
Texas Office of Court Administration

David K. Byers
Arizona Supreme Court

Laurie Dudgeon
Kentucky Administrative Office of the Courts

Gerald A. Marroney
Colorado Administrative Office of the Courts

Robin Sweet
Nevada Administrative Office of the Courts

NACM Appointments

Kevin Bowling (Co-Chair)
Michigan 20th Judicial Circuit Court

Paul DeLosh
Supreme Court of Virginia

Yolanda Lewis
Superior Court of Fulton County, Georgia

Kelly C. Steele
Florida Ninth Judicial Circuit Court

Jeffrey Tsunekawa
Seattle Municipal Court

NCSC Appointments

The Honorable O. John Kuenhold
State of Colorado

The Honorable Michael Trickey
Washington Court of Appeals, Division 1

CITOC Appointments

Jorge Basto
Judicial Council of Georgia

Craig Burlingame
Massachusetts Trial Court

Ex-officio Appointments

John Greacen
Forum on the Advancement of Court Technology

NCSC Staff

Paul Embley
Jim Harris
Ilonka Dazevedo

Document History and Version Control

Version	Date Approved	Approved by	Brief Description
1.0	3/24/2015	JTC	Release document

Contents

Introduction

EMV standard chip-enabled bankcards have been widely implemented in other parts of the world for more than ten years now, but US credit card issuers have been slow to adopt the technology. Countries where the technology has been implemented have seen dramatic reductions in the incidence of fraud, but the cost of implementation, coupled with the financial disincentives of US fraud loss laws have made US card issuers reluctant to adopt the technology. Recent well-publicized data breaches of major retailers have highlighted the vulnerabilities inherent in magnetic stripe "swipe and signature" authentication, and have accelerated efforts to move to a more secure standard.

Until 2010, US laws allowed credit card issuers to write off a major portion of fraud losses and pass the rest of the cost on to consumers. The Dodd-Frank Wall Street Reform and Consumer Protection Act included a provision that lowered the "swipe fees" or interchange fees that credit card issuers could charge merchants. Those fees were intended to cover transaction costs, other overhead, and the risk of fraud, but credit card issuers relied on profits from swipe fees to offset the cost of fraud. There was no financial incentive for card issuers to fix the system's vulnerabilities because merchants and consumers bore the cost. With fees limited, card issuers can no longer afford to ignore the cost of fraud.[1]

A Brief Explanation of EMV Technology

EMV (which stands for Europay, MasterCard, and Visa – the three payment brands that launched the initiative) is a global standard for chip-enabled "smart" credit and debit cards and the point-of-sale (POS) infrastructure required to authenticate those transactions. EMV cards carry security credentials that are encoded into the card's chip by the card issuer. The biggest benefit of EMV is the reduction in card fraud resulting from counterfeit, lost and stolen cards.

Payment transactions using EMV are more secure because of enhanced functionality in three areas: card authentication, cardholder verification, and transaction authorization.

Card Authentication

Card authentication is the process of ensuring the card is valid. This happens when encrypted data from the card is transmitted to the card issuer via the POS

[1] Johnston, Susan. "Coming Next Fall: More Chip and PIN Cards in the U.S." *US News RSS*. US News and World Report, 28 Oct. 2014. Web. 11 Dec. 2014.

terminal. Unlike magnetic stripe cards, which can be relatively easily created using information "skimmed" from legitimate cards, chip-enabled cards are almost impossible to counterfeit.

Practically speaking, the authentication process in an EMV transaction takes slightly longer than traditional "swipe and sign" card processing because the card must remain in the reader for the duration of the transaction.

Cardholder Verification

Cardholder verification is the process of proving the identity of the person holding the card. EMV Cardholder Verification Methods (CVM) include signature, online or offline PIN, or no CVM (meaning that no customer verification occurs at the time of the transaction). Low-dollar and "unattended" transactions at fast food restaurants, grocery and convenience stores may not require any CVM for a transaction to be approved. Card issuers specify the Cardholder Verification Method required.

Transaction Authorization

Transactions are authorized through applications unique to one of the payment processing brands (Visa credit, Visa debit, Maestro, Cirrus, American Express, etc.) that reside on both the card and the terminal.

A card's chip may carry more than one application, so the same card may be used in more than one way (e.g., at an ATM or as a credit card). Card readers (POS terminals) come in multiple varieties, as well, depending on which cards they read and what transactions they can process.

Chip-enabled cards come in three varieties:

- contact
- contactless
- dual-interface

In the United States, the most common variety of chip-enabled cards require contact with the POS device. Contactless smart cards do not require physical contact between a card and reader. Examples of contactless smart cards include mass transit fare cards, ExpressPay (American Express) and PayWave (Visa). Dual-interface cards are equipped to do both contact and contactless EMV transactions.

Transitioning the US to EMV

Because the impetus behind the US shift has not been primarily fraud prevention, implementation in the United States is more nuanced than in Europe or the rest of the world. Instead of requiring chip and pin authentication (the most secure form), US card issuers are implementing chip-enabled cards, but not PIN authentication. Chip-enabled cards, with or without PIN authentication, are still more secure than magnetic strip cards, so card issuers are now making that transition. However, EMV cards are much more costly to produce ($15-$20 for chip-enabled, versus $1 for magnetic strip), so institutions may take several years to fully deploy new cards.

Retailers will have a similar transition, replacing old-style readers with readers that can authenticate the new chip. To ensure that consumers are not impacted at the point of sale, EMV cards issued in the US will carry both chip and magnetic stripe functions for the foreseeable future. Courts will need card readers that can handle both magnetic stripe and chip authentication processes.

During the transition, major financial institutions that don't provide chip-enabled cards to their cardholders remain accountable for fraudulent purchases. According to Tom Risen, a technology and business reporter for U.S. News & World Report, "Transactions still can be performed using the old card technology after the transition, but banks will be liable for any payment fraud if they do not issue a card containing a smart chip, and merchants will be liable if their teller machines do not accept the chip cards."[2]

Government-based purchasing and benefits cards are also shifting to chip-enabled cards. In late 2014, President Obama signed an executive order[3] requiring that this technology be used in all government-issued credit and debit cards. The BuySecure initiative requires the use of chip-and-PIN security on government-issued cards through the General Services Administration.[4] Payment terminals at federal government facilities will be equipped to handle cards with the new technology.

---

[2] Risen, Tom. "Credit Cards Will Get Security Upgrade in 2015." *US News*. U.S.News & World Report, 11 Feb. 2014. Web. 11 Dec. 2014.

[3] Zients, Jeffrey. "The President's BuySecure Initiative: Protecting Americans from Credit Card Fraud and Identity Theft." The White House. The White House Blog, 22 Oct. 2014. Web. 03 Mar. 2015.

[4] Gordon, Marcy, and Josh Lederman, Associated Press. "Obama Announces Plan to Tighten Security for Debit Cards Used for Federal Benefits." *US News*. U.S.News & World Report, 17 Oct. 2014. Web. 03 Mar. 2015.

What this means for courts

If your organization owns credit card readers, you must upgrade them to devices that can authenticate credit and debit cards with the EMV chip. Because of rapid changes in paypoint technology, Court Administrators should consider implementing readers that support both contact and contactless EMV, as well as Near Field Communication (NFC) mobile payments.

If you have contracted with a vendor for card readers, review your contract carefully. Court administrators should ensure they understand essential vendor-specific details:

1. Who currently bears liability in a card present transaction and how will that change in October of 2015?
2. What payment processing applications do you support?
3. Do these applications support contact, contactless and/or both?
4. What are my routing choices?

Because new card readers may have additional data requirements that could impact court facilities, Court Administrators should act quickly to assess their court's readiness for EMV.

In addition, court personnel who handle in-person debit and credit card transactions must be trained to require payors with a chip-enabled card to process the card through the chip reader, not the magnetic strip. If fraud occurs using a chip-enabled card that was authorized by swiping, the court could be financially liable.

The liability shift does not impact "card not-present" transactions (online or over the phone) at this time.

Dick Mitchell of PaymentSource warns that "Many merchants and banks simply aren't aware of this potential storm cloud on the horizon. For those unprepared, this shift will have organizations scrambling to acquire and deploy smartcard technology before the deadline."[5]

[5] Mitchell, Dick. "Missing the EMV Liability Shift Bears a Huge Cost." Editorial.Payment Source. SourceMedia, 4 Aug. 2014. Web. 11 Dec. 2014.

Credit Card Processing Terminology

Authentication	Checks the authenticity of the card.
Authorization	The issuing bank's transaction approval. (Evaluates the status of the cardholder's account.)
Cardholder Verification	Online PIN, offline PIN, signature, or no CVM; based on issuer preference for the card type (i.e., ATM, debit, credit) and terminal capability.
Card Present	Transactions where the cardholder is present, typically for signature or PIN entry.
Card Not Present	Transactions by phone or internet where the cardholder is not physically present.
Chip-enabled	Credit and debit cards with a secure computer chip that validates the authenticity of the card at the point of sale, generating a one-time use security code for each transaction. Payment data pieces cannot be used again for another purchase.
Chip and Pin	Highly secure credit card processing mechanism requiring both the card's chip and the owner's PIN to complete a transaction.
Contactless	Credit cards, debit cards, key fobs, smartcards or other devices that use radio-frequency identification for making secure payments. The embedded chip and antenna enable consumers to wave their card or fob over a reader at the point of sale.
CVM	Cardholder Verification Method.
EMV	Acronym for Europay, MasterCard and Visa, the original transaction processing companies that banded together to form EMVCo, LLC. EMV is a global standard for cards equipped with computer chips and the technology used to authenticate chip-card transactions.

Dual Interface	Cards that carry both contactless and contact EMV interfaces.
Magnetic Swipe	Also called “Swipe and Signature”. Uses a magnetic strip with “static” data for purchase authentication. Least secure payment mechanism. Fake cards can be easily created using details lifted from legitimate cards or transactions.
MSD	Magnetic Stripe Data. Form of contactless payment implemented by US payment brands. Uses Magnetic Stripe Data plus a chip for dynamic card verification.
NFC	Near Field Communication. A payment method using wireless communication technology that enables devices (including cell phones) with secure elements to exchange data by touching them together or bringing them into close proximity, usually less 2-4”.

Additional Reading

Bell, Claes. "Are Chip and PIN Credit Cards Coming to the U.S.?" *Bankrate*. Bankrate.com, 2010. Web. 11 Dec. 2014.

Tormos, Sebastian. "EMV vs. NFC Technology: Setting the Record Straight." Web log post. Datacard Edge. Datacard Corporation, 18 Oct. 2012. Web. 3 Mar. 2015.

EMVCo.com

A Smart Card Alliance Payments Council. *Card Payments Roadmap in the United States: How Will EMV Impact the Future Payments Infrastructure?* Whitepaper, no. PC-12001. Princeton, NJ: Smart Card Alliance, January 2013. Web.