# The Time for EMV in the United States Is Now

by Paul Beverly, President, Gemalto North America
December 2010

TECHNOLOGY

## Introduction

In the past year, the topic of secure payments and secure payment cards (i.e., microprocessor-based EMV smart bank cards) has become one of the most discussed technology shifts in the U.S. banking industry. For many years, there has been a belief that magstipe cards issued by nearly all U.S. banks would continue to be the payment modality of choice, and that EMV would simply be a way that payments are conducted "over there." However, as the world continues to become more accessible to a broader number of U.S. travelers, this type of viewpoint has created a significant inconvenience when their magstripe card was rejected or simply not accepted by smaller merchants not willing to risk the liability of purchase chargeback.

The conversation is now one of "when," not "if," EMV will be issued in the United States. Of course, there are many other factors playing into this decision, but one key consideration should be the security of the cardholder's information for both in-person transactions and in the ever-expanding online world. This is one of the significant benefits to EMV and a driving factor in moving the United States toward this type of secure payment technology.

## *How Am I Protected?*

EMV smart bank cards and smart card-ready terminals work with the transaction authorization network to make an entire payment system more secure. By using the microprocessor chip as an active part of the payment transaction, EMV cards and terminals prevent credit card fraud, whether from stolen account numbers or cloned payment cards. They can also be used online to secure access to bank accounts or to authenticate payment transactions. The transaction can even be completed in an offline environment.

## Editor's Note

Over the last 12 months, I have witnessed the debate about EMV migration in the United States heating up again. The debate has been fueled by renewed merchant interest, possible regulatory intervention and the pending payments infrastructure conversion in the rest of the world.

With the U.S. payments industry undergoing a massive transformation driven by regulations, changed economics, evolving consumer behavior, renewed merchant demands and emerging technologies, it is timely to consider the arguments for and against EMV in the United States. I am honored to debate with Paul Beverly, President of Gemalto Americas, whether now is the time to upgrade the U.S. payments infrastructure and whether EMV is still the right option.

- Patrick Gauthier, Technology Editor

AUTHORS

Nikki Baird

Robert Ballen

Paul Beverly

Peter Ciurea

David S. Evans

Patrick Gauthier

Thomas Fox

Margaret Weichert



This option is interesting to issuers, as it saves telecommunications costs or solves infrastructure shortcomings in other regions.

One important EMV security feature is that the chip contains a unique key. As part of the transaction authorization, the smart card uses the key to prove it is authentic. Digital keys on smart cards have been used for more than 10 years to prevent cloning of chip cards.

Magnetic stripe cards, on the other hand, do not have the same kind of data storage and have no internal computer. Therefore, magnetic stripe cards cannot contain the same security features as smart bank cards. With magnetic stripe cards, the cardholder's data is encoded on the magnetic stripe on the back of the card, similar to a tape recorder. When the card is swiped, all of the cardholder data, such as the account number, name and expiration date, is sent in one direction from the payment terminal to the authorization network that checks the information, authorizes the charge and provides a payment guarantee to the merchant.

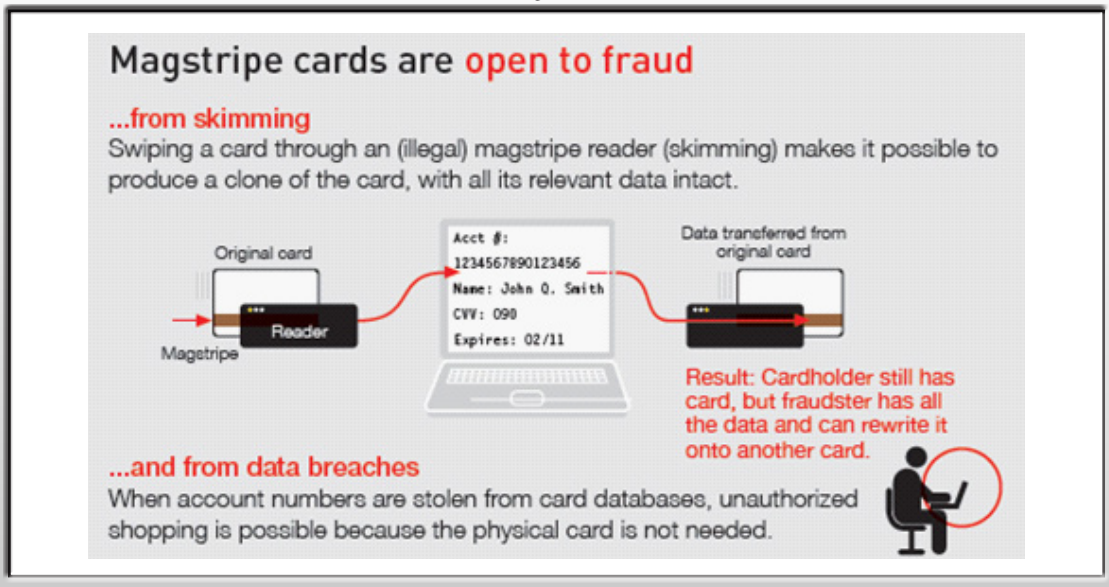
The problem is that data can easily be stolen from a magnetic stripe card with a practice known in the industry as "skimming." By running the card through a small, handheld reader called a skimmer, the magnetic stripe information can be copied and then later transferred to another plastic bank card and used fraudulently. When the fraudulent card is swiped, it is the stolen data on the stripe that is sent for authorization, not what is printed or embossed on the card. What is insidious about skimming fraud is that the cardholder is not even aware that his or her card has been cloned, because the original card is still in the cardholder's possession.

## *How Am I Protected When Paying Online?*

EMV smart bank cards and smart card-ready terminals work with the transaction authorization network to make an entire payment system more secure.

EMV smart cards can be used to secure card-not-present (CNP) transactions – online and telephone purchases where the card cannot be swiped in a payment terminal. In fact, by making chip cards an active part of the online or phone authorization process, stolen payment card

Figure 1



## AUTHORS

Nikki Baird

Robert Ballen

Paul Beverly

Peter Ciurea

David S. Evans

Patrick Gauthier

Thomas Fox

Margaret Weichert




numbers can be made useless to thieves.

There are two ways to accomplish online and telephone transactions with smart bank cards – with a USB reader connected to a PC, which would work much like the POS device in an in-person transaction, or with a One-Time Password (OTP) device.


With the OTP device, end users insert the EMV smart bank card into a small, handheld device (with keypad and display) issued by their bank and enter a PIN. Once the chip confirms the PIN as valid, a one-time password is generated for use on the merchant website. The cardholder then enters that number using the keyboard or the phone. With this method, an end user can have the same confidence shopping online and by telephone as when paying with an EMV smart bank card in person.

EMV cards can generate a unique key for each payment transaction. With OPT readers, end users must type the key on the PC keyboard. By using an EMV card and a USB reader, the authorization can be performed online just as it is at a merchant location. Either way, EMV cards can prevent stolen payment card information from being used online.

For issuers and merchants, making the EMV card an active part of online and phone payment authorization would mean stolen account numbers and CVV2s – the printed security number used for online and phone transactions – could no longer be successfully used for fraudulent online CNP transactions.

Barclays, a leading bank in the United Kingdom, deployed a product like this called PINsentry in

Figure 2

## ARTICLES



## AUTHORS

Nikki Baird

Robert Ballen

Paul Beverly

Peter Ciurea

David S. Evans

Patrick Gauthier

Thomas Fox

Margaret Weichert



July 2007, which now has more than a million devices in use for online bank account login. The organization has stated publicly that not one PINsentry online customer has suffered fraud since that time. They also reported extremely positive user feedback and customer acceptance.

MasterCard and Visa both offer programs to better secure CNP purchases. MasterCard created the Chip Authentication Program (CAP), a specification for using EMV smart bank cards for authenticating users and their transactions over the Internet and telephone. Visa has also created a specification for the same applications under the name Dynamic Passcode Authentication (DPA).

Certainly EMV cards cost issuers more than magnetic stripe, and eventually the acceptance infrastructure has to evolve into chip acceptance to derive the benefits of increased payment security. These costs have long been the primary barriers to EMV migration in the United States.

The situation has changed, and the business case for EMV needs to be reassessed. The hard costs from data breaches, which shared among issuers as well as merchants and processors, are changing the balance. Issuers are increasingly being forced to reissue magnetic stripe cards both as a result of risk from data breaches and higher online fraud. The cost of reissuing payment cards goes beyond the personalized plastic. Customer service may become involved to deal with cardholders. The bank's brand is tarnished. The consumer also is inconvenienced, if not directly impacted financially. Online merchants and other accounts need to be updated with the new number, further aggravating bank customers.

Migrating the United States to EMV is made more complex by the competitive, multi-tiered structure of the payments and acceptance industry. Yet today, all the stakeholders are sharing higher costs driven by the growth of data breaches, online fraud and financial crime malware. For those reasons, the economics of EMV migration need a fresh look in the United States by all of the stakeholders, and the prevailing consensus needs to be that the time for EMV is now.