

Daily Union Article

Saturday, September 10, 2016

Title: To Swipe or Not to Swipe

To swipe or not to swipe – that is the question! I was visiting with a friend recently about the confusion she experienced at her local gas station. This last weekend, the gasoline pump at the station she uses wouldn't accept her chip card even though she used it there in the past. In frustration, she asked the clerk to come to the pump to show her what she was doing wrong. Instead of inserting my friend's chip card like she had, the attendant swiped it using the magnetic stripe – the "old way" of initiating the transaction. So how are we to know when to swipe or when to insert? I did some research to find out more about chip cards and their use.

Although knowing whether you should swipe or not swipe can be frustrating, the shift to chip cards (aka EMV cards) is important in combating fraud. The "old fashioned" magnetic stripe cards have become very easy to counterfeit.

The push for chip cards is the result of a significant increase of frauds committed with the mag strips. Of all credit/debit card frauds reported internationally, 47% occur in the United States. Although chip cards have been used worldwide for several years, the United States has been slow to change. In a press release from the U.S. Payments Forum, a justification statement for this transition is provided: *"The U.S. move to EMV chip payments is being driven by the payments industry's desire to reduce card fraud in a face-to-face card-present environment, provide global interoperability, and enable safer and smarter transactions across contact and contactless channels."*

Last October, U.S. major credit card companies and banks began recommending that merchants transition their payment terminals over to ones that had the capability to read the new chip cards. About 75% of credit cards are now chip-enabled while only about 25% of U.S. merchants have made the transition. Consumers will continue to see both of these numbers rise as the transition continues and merchants seek to comply with this change. According to the Electronic Transactions Association, the major card brands are promoting this change as an incentive rather than a mandate. However, failure to make the transition leaves the merchant with a much greater liability for fraudulent transactions that occur through their business. The chip card initiative created by three major card companies (EuroPay, Mastercard, and Visa – hence EMV cards) shifts the liability of the fraud – i.e. a fraud liability shift. The work of continuing the transition for chip card use in the U.S. had now shifted to EMVCo.

With the chip card transaction, the exchange of information between the merchant and your financial institution follows a significantly different path than it does with the mag

stripe. With mag stripe use, the credit card provides the merchant with your payment credentials from which they authorize the transaction. When a chip card reader is used, the chip creates a one-time code that is sent from the reader to your financial institution. The bank matches this code to an identical one-time code then sends back the verification that the transaction is approved. These additional steps, although they may take a few more seconds to move through at the counter, are part of the reason the security is so much stronger with chip cards.

From the consumer standpoint, using either a chip card reader or the mag stripe has the same protections. It doesn't affect your legal rights as they relate to credit card and debit card fraud. However, to be fully protected you still need to review your card statements carefully and regularly. If you find fraudulent charges, report them immediately. If you wait for another statement cycle to go by, you will likely lose the protection you have for that specific transaction and potential transactions from that "merchant" in the future.

By keeping a close eye on your account activity, you will be able to recognize and report a fraudulent transaction more quickly – reducing the risk of additional transactions from occurring. The sooner your report your findings to the card provider, the better!



Image Source: <http://www.emv-connection.com/emv-faq/>

Chip Card Quick Facts

October, 2015 - The target date set by EMVCo for accelerating chip card circulation in the United States.

EMVCo – (Visa, Mastercard, JCB, American Express, China UnionPay, & Discover) controls the standards for chip cards

Fraud Liability Shift – "Fraud liability shifts" for card issuers and merchants are meant to help synchronize the timelines to move all industry stakeholders to implement chip technology. As of October 2015, the payment brands shifted the responsibility for certain types of fraud resulting from a payment transaction to the party using the least secure technology. There are different liability shifts for ATMs (October 2016 and

October 2017) and automated fuel dispensers (October 2017). Source: <http://www.emv-connection.com/press-room/#facts>

Who made this law? – No one. There is no law in the United States requiring businesses to be compliant with the chip card movement. It is the right of the individual business to determine if they want to purchase the technology required to have chip readers. Some businesses, like those selling electronics for example, have a higher risk of fraudulent transactions.

PIN verification – in most credit card transactions occurring outside the U.S., a pin and/or signature is required. Some transactions in the U.S. require one OR neither. Note: EMV standards support both PIN and signature.

For more information about consumer protection and safer credit card use, contact me at the Geary County Extension office at 785-238-4161. Until next time, keep living resourcefully!