



VIEW S & VISIONS

A publication of Bowles Rice LLP

Summer 2015



EMV Chip Cards Expected to Reduce Card Fraud

Darren K. Williams, Corporate Risk Manager
United Bank, Inc.

Darren K. Williams is the Corporate Risk Manager for United Bank and the former President of the Morgantown, West Virginia region for United Bank. Prior to joining United Bank, Inc. in 2011, Mr. Williams was the Chief Financial Officer and Chief Information Officer of Centra Financial Holdings, Inc. and Centra Bank, Inc.

From 2004 to 2006, he served as the Chief Information Officer for the West Virginia University Foundation, where he handled information security and IT operations. He was a senior manager with Ernst & Young LLP from 1995 to 2004, specializing in financial and IT audits. Mr. Williams is a Certified Public Accountant.

In the wake of several high-profile data breaches in 2014, over half of the nation's adults had their personal information compromised, according to the Financial Services Roundtable. In order to combat this cyber-security threat, the United States is in the final stages of adopting EMV chip cards. EMV, which stands for EUROPAY, MasterCard and Visa, is a standard for chip-and-PIN cards that are considered far more secure than the magnetic stripe cards we use in the United States today. EMV chip cards contain embedded microprocessors that provide strong transaction security features and other application capabilities not possible with traditional magnetic stripe cards. The biggest benefit of EMV is the reduction in card fraud resulting from counterfeit, lost and stolen cards.

The United States is one of the last major countries to adopt this technology, as approximately 80 countries globally are in various stages of EMV chip migration, including Canada and countries in Europe, Latin America and Asia. In the U.S., many financial institutions, including United Bank, have begun to roll out EMV cards. But what the financial institutions are doing is only part of the story. Business owners, processors and financial institutions alike are all involved with card payments.



The major networks, including VISA, MasterCard and Discover, have instituted a liability shift in the U.S. for domestic and cross-border counterfeit transactions, effective October 1, 2015. The liability shift policies are designed to encourage EMV chip card issuance and acceptance, effectively creating a more secure environment

for transactions. With this type of liability shift, the party that is the cause of a chip-on-chip transaction not occurring (i.e., either the issuer or the merchant) **will be financially liable for any resulting card-present counterfeit fraud losses.**

The most encouraging aspect of EMV adoption will be the opportunity for the financial sector and retailers to work together to fight fraud. Today, crime does pay for too many criminals.

This shift is important, as most fraud losses are currently incurred by the banks or payment networks. Financial institutions in the U.S. saw a dramatic increase in fraud as a result of recent major retail breaches. After October 1, many of those kinds of **losses will be shifted to either a non-compliant merchant or eliminated altogether.**

The most encouraging aspect of EMV adoption will be the opportunity for the financial sector and retailers to work together to fight fraud. Today, crime does pay for too many criminals. However, the EMV adoption is forecasted to make a major dent in this kind of fraud. In the United Kingdom, where 99.9 percent of their cards have an EMV chip, we can see impressive examples of success. For example, according to the UK Card Association, fraud on lost and stolen cards is now at its lowest level for two decades, and counterfeit card fraud losses also have fallen and are at their lowest level since 1999. Losses at U.K. retailers have



A rendering of United Bank's new card design featuring the EMV chip

fallen by 67 percent since 2004, and lost and stolen card fraud fell by 58 percent between 2004 and 2009.

However, we cannot stop with EMV adoption. The experiences of the U.K. and other countries that have adopted the EMV chip have shown a reduction of card-present fraud. However, their experiences also have shown a migration to other types of fraud, namely card-not-present (CNP) fraud and cross-border counterfeit fraud (particularly ATM fraud). Fraud migration offsets some of the savings from the decrease in domestic card-present fraud that EMV cards are specifically designed to combat. This reality reinforces the need for a layered approach to security, even with EMV deployment, to address fraud migration and other security vulnerabilities. United Bank has found that the single most effective way of fighting fraud is working with our customers and educating them to continue traditional practices of protecting their information

and managing their businesses and personal lives with a degree of skepticism. In addition, adoption of emerging technologies, such as EMV cards and utilizing fraud detection systems, will assist us in fighting back together. ▽