WHAT YOU NEED TO KNOW ABOUT EMV…

AND WHY YOUR BUSINESS COULD BE AT RISK

Perhaps you're hearing about EMV for the first time or you've heard about how you need to upgrade your equipment with EMV-capable hardware and software but don't understand what that actually means. We're here to help you navigate through all the ins and outs of EMV, what it is, how it works, why it should be important to you, and why you could be liable for fraudulent EMV transactions if you don't upgrade your equipment by the upcoming deadlines.

What is EMV?

EMV is a term coined by the original card associations that created the payment security standards for "chip card" technology, namely, Europay®, MasterCard® & Visa® (EMV). EMV transactions add dynamic data to the data stream that, unlike magnetic stripe cards, make it nearly impossible to replicate the data.

An EMV card looks very similar to a standard magnetic stripe card except it has a small metal chip embedded into the card itself. The technology was developed for card present credit, debit and ATM transactions.

Why was EMV created?

In an effort to stop fraud, EMV technology was created as a global replacement for the outdated, fraud-prone magnetic stripe technology used by the payments industry for the past 40+ years.

The purpose of EMV is to help prevent the use of counterfeit cards and limit card skimming abilities using cryptography technology, as well as to help prevent acceptance of lost or stolen cards through the use of cryptography & PIN (dual authentication).

How does an EMV transaction work?

When an EMV card is inserted into an EMV reader, a metal contact on the card connects it to the terminal and the two devices are able to communicate, passing dynamic data to/from the chip. As such, the card is "held" by the EMV reader during the entire transaction, making it essential that the terminal have the proper hardware and software installed in order to process chip (EMV) transactions.

WHAT YOU NEED TO KNOW ABOUT EMV... *AND WHY YOUR BUSINESS COULD BE AT RISK*

Why is EMV important to me?

The card associations have released deadlines that must be met for upgrading your equipment or you will be held responsible for fraudulent EMV transactions (also known as "liability shift"). What this means is that a Reg E claim could be issued against you as the ATM owner/operator if your terminal has not been upgraded with EMV hardware and software by the deadlines listed below.

The average fraudulent occurrence is $618 (three consecutive transactions combined), possibly adding up to thousands of dollars essentially stolen from your ATM within minutes if you're not EMV compliant. So, if your terminal has been upgraded for EMV card acceptance, the liability shifts back to the card issuer, freeing you (the ATM owner/operator) of liability for the fraudulent transaction.

What are the timelines I need to meet before I'm liable for fraudulent EMV transactions?

If you haven't already developed a plan for upgrading your equipment for EMV compliance, the time is now! ATM manufacturers offer limited EMV hardware today, and we expect pricing to increase as the deadline nears due to declining availability of equipment as terminals are upgraded.

The liability shift has already gone into effect for cross-border Maestro® transactions and all U.S. issued MasterCard® cards are next, with Visa® to follow! Card issuers have exponentially ramped up the issuance of EMV cards in the past year, so it is possible that non-compliant ATMs could be targeted by counterfeiters using a magnetic stripe card with fraudulent data.

Don't be caught before the deadline – let us help you develop a plan today!

For More Information:

Green Genie ATM
877-651-2867
http://GreenGenieATM.com