Q: What is EMV?	
A: EMV is an open-standard set of technical specifications for chip card payments and acceptance devices such as point-of-sale (POS) terminals, kiosks and ATMs. EMV chip cards contain embedded microprocessors that provide strong transaction security features and other application capabilities not possible on traditional magnetic stripe cards. When a consumer uses an EMV-enabled device to pay at an EMV terminal, the device is instantly identified as an authentic, approved payment instrument belonging to that consumer through a process called dynamic authentication.	**Basically,** EMV is a global industry standard used to govern card payment technology. Cards with chips embedded provide strong security features and other capabilities.
Q: Where has EMV been adopted?	
A: Over 80 countries already support EMV chip card payments. MasterCard's focus is on security for the next generation of payments.	**Basically,** EMV is used around the world. The United States is the last major country to adopt the standards. EMV is an essential first step to being able to accept payments from mobile devices such as phones.
Q: What does the Fraud Liability Shift mean for my business?	
A: October 1, 2015: the Fraud Liability Shift date for cards and POS devices, which is aligned across all of the major payment brands. This means that after October 1, 2015, the party, which can be either the issuer or the merchant who does not support EMV, assumes liability for counterfeit card transactions. The Fraud Liability Shift is <u>not</u> a mandate – meaning there is no penalty if you do not meet this date. However, as many other merchants move to secure their payments with chip technology, fraudsters may focus on those merchants that have not yet upgraded and there is a risk that you could become a target of fraud. The decision to migrate is your and	**Basically,** MasterCard's fraud rules provide protection to the party with the higher level of security. For merchants, if you install EMV enabled card readers with PIN support by October 1, 2015, then MasterCard will not hold you liable for fraudulent transactions – counterfeit or lost/stolen fraud. It is not a mandate. However, in order to protect yourself from counterfeit and lost/stolen fraud you will need to upgrade your terminals at some stage.

you must consider this with these risks in mind.	
Q: What are the benefits of accepting chip payments?	
A: EMV secures the payment and reduces the opportunities for fraudsters to steal data that can be later used to counterfeit cards as fraudsters are currently able to do with magnetic stripe cards. By accepting chip payments, you are providing a more secure transaction environment for your customers. You are also ensuring that you are able to accept the next generation of payment technology such as mobile phones. Merchant POS terminals are generally capable of processing both contact and contactless chip payments.	**Basically,** Chips cards are harder to clone or steal data from. Accepting chip payments makes you more attractive to customers because there are generally more payment options at the terminal (e.g., mobile, contactless or standard dip) and the consumer will feel more confident when making a purchase.
Q: How are chip transactions authorized?	
A: Just as with magnetic stripe cards, chip transactions are authorized mostly online. This means that the transaction will be authorized by going online to the issuer host system to confirm that the transaction is cleared for processing.	**Basically,** Most transactions are validated directly with the card issuer to confirm that the cardholder is allowed to make that transaction and has enough money or credit in the account.
Q: What changes will I need to make to my terminals?	
A: In order to accept EMV chip payment devices, which includes cards that have both contact and contactless chips, mobile phones and other types of devices, your POS terminal will need to be EMV capable and enabled. You may already have a chip-capable terminal, which may need to be enabled or you may need to purchase a new EMV terminal. Your payment processor will be able to assist you with upgrading to an EMV capable and enabled terminal.	**Basically,** If you want to be protected from fraud chargebacks, you will need to upgrade your terminals and support PIN and other cardholder verification capabilities (this is optional but strongly recommended). There may be some extra works that needs to be done to support these terminals, so you may want to contact your processor sooner rather than later.