Did you know your customer can dispute any magnetic stripe transaction? Thieves do! Protect your business from charge-backs by activating your chip-card reader on your Verifone VX520 today! It's free!

FAQ

Q. How do I start?

A. Contact us during business hours 8-4 PST to schedule or facilitate a download 888-269-4523 or after hours contact our 24 hour help desk by pressing 2 when prompted.

Q. If I contact the help desk after hours what should I ask for?

A. First you will be asked to provide the last 6 numbers of your merchant account number (MID) to identify your business account. Next you should ask to facilitate an "EMV" down load to activate your chip reader.

Q. How long will this take?

A. Approximately 10 minutes for the support tech to talk you through each step to activate the chip reader If your terminal has an ethernet connection it will take several minutes. If you have a dial-up connection expect a minimum of 20 min for your terminal to dial out and complete the load.

Q. Do I have to do anything while the terminal is downloading?

A. No.

Q. I have a dial up connection at work and ethernet connection at home – can I take my terminal home for a faster load?

A. Yes. The terminal will hold the load. Plug into electricity and your router before contacting the help desk and you're all set to contact our help desk!

Q. Will the procedure for accepting credit-debit cards change?

A. Yes you will enter the card chip first into the front of the terminal vs. magnetic strip.

Q. What if the chip reader won't read the card?

A. After a few tries the terminal will allow you to key in or swipe the transaction.

Q. If I swipe or key the transaction will I still be subject to charge-backs?

A. Yes. You can take the risk or ask for another form of payment.

Q. I use my terminal for WEX and fleet cards only-should I still down-load the chip reader?

A. Its up to you. Fleet cards don't have in-bedded chips as this time so not a requirement. However, many of our customers use their Verifone for back-up if their POS system goes down so in that scenario adding the chip reader pro-actively is encouraged.

Q. Do chip cards require a pin?

A. Issuing banks are requiring pin numbers be entered for an extra layer of security on all debit and some credit cards. If your terminal was purchased after October 30, 2016 it should have the correct injection key and your customer won't be prompted to enter a PIN.

Verifones purchased before 11/2016 will need the encryption key to avoid keying in the entire transaction.

Q. Will I still be subject to charge-backs if I key-in the transaction after trying to run a chip card?

A. Yes.

Q. How do I encrypt my Verifone VX50?

A. You can ship the terminal to us for encryption. The injection fee is 20.00 and you would be responsible for the shipping cost.

Q. We are open 7 days a week and can't be with-out a way to process credit cards. Are there any other options?

A. Yes. You can add a pin pad to your desk-top for your customers to enter their own chip-card. Pin-pad comes with full encryption and sells for 195.00 plus shipping.

Q. What if I don't do anything.

A. You can continue to process credit and debit cards the way you are now and accept the risk.

Q. Is there any other wat to protect my business from credit card fraud?

A. Yes. Employees should be taught the signs of a customer who uses a stolen credit card. Credit card fraud detection signs may include:

- A customer making purchases of multiple and/or expensive items (laptops, stereos, electronic games).
- Purchases being made at closing time, and the customer is attempting to rush the sale.
- A customer who cannot produce identification matching the name of the card holder.
- A card that swipes but the name on the card doesn't match the name that was printed on the receipt.
- Random purchases with little regard to price of the items.
- It's important to note that the liability shift only pertains to counterfeit fraud tied to EMV chip cards. The liability shift will not apply to large scale data breaches or consumer payment card data stolen prior to October 1.

Here are some examples of who may handle fraud costs based on the situation, post-Oct. 1, 2015:

It's important to note that the liability shift only pertains to counterfeit fraud tied to EMV chip cards. The liability shift will not apply to large scale data breaches or consumer payment card data stolen prior to October 1.

EMV card fraud liability: Who's responsible?

Fraud scenario:	Merchant/Acquirer	Card issuer
Chip card is stolen and swiped by fraudster in store not EMV-ready.	**X** (If the card is PIN-based and from American Express, Discover or Mastercard)	**X** (If the card is a Visa, Accel, China UnionPay, NYCE or STAR Network card)
Stolen card number is used online.		**X**
Chip card swiped at non-EMV compliant merchant, mag stripe data stolen and fraud occurs.	**X**	
Chip card-less consumer gets hit by fraud because they couldn't dip a chip card at an EMV-ready retailer.		**X**
Stolen/lost chip card dipped by fraudster at EMV-ready merchant.		**X**
Mag stripe data copied from chip card onto counterfeit card and swiped by fraudster at non-EMV compliant merchant.	**X**	
Chip card dipped at EMV-compliant merchant.		**X**

- **2. The shift is intended to help parties deal with counterfeit fraud more equally.** The EMV fraud liability shift was implemented by major U.S. payment card networks (nine to be exact: Accel, American Express, China UnionPay, Discover, Mastercard, NYCE Payments Network, SHAZAM Network, STAR Network and Visa) to combat counterfeit fraud.
- Since the U.S. is the only country in which counterfeit card fraud is consistently growing, the shift was put in place to encourage faster adoption of EMV payment technology, according to Stephanie Ericksen, vice president of Risk Products for Visa.
- "The way that the liability shift works is to set a structure in place to incentivize the protection of chip," she said. "Merchants get protection against liability as soon as they get a terminal and enable chip acceptance, and vice versa for issuers."
- Counterfeit card fraud costs the U.S. $7.86 billion in 2015, according to The Nilson Report. In particular, card issuers lost $4.91 billion and merchants lost $2.95 billion to counterfeit card fraud last year.