MAGTEK®
SECURITY FROM THE INSIDE

Magensa Services

Stop counterfeit cards from being accepted. PERIOD.

- ☑ Saves merchants billion on chargebacks and fees
- ☑ Saves banks billions in fraud losses
- ☑ Requires no major changes to existing cards, processes, or systems
- ☑ Costs less than one tenth of first year savings to deploy
- ☑ Tested, proven and ready to deploy world-wide today
- ☑ Disrupts funding of global terrorist groups
- ☑ Halts a major segment of global organized crime

Transaction Security Services

Gateway Services

Application Services

Call a representative to learn more: 562-546-6400.

MagTek® Inc., 1710 Apollo Court, Seal Beach, CA 90740 | p 562-546-6400 | f 562-546-6301 | 800-788-6835 | www.magtek.com

Have the ability to fight fraud and earn rewards

Magensa is a fraud prevention, detection and advisory service

It maintains a globally accessible registry of authentication information so that consumers, financial institutions, retailers, businesses and governments can assess the validity and trustworthiness of the credentials and products they rely upon in the course of online identification, payment, and other important transactions.

Only Magensa does it all:

- Complies with PCI-DSS
- Fights fraud
- Detects counterfeit cards
- Assists law enforcement
- Protects your customers
- Provides Code 10 fraud alerts
- Provides you with easy access to industry rewards

VISA

Skimming is a Scam

(It's a crime and you can stop it!)

It's your job to keep your customers' credit card information secure.
Skimming is just one trick criminals use to illegally obtain credit card information.

Be on the lookout for skimming activity.
If, in your workplace...

- You see anyone using a device that is not part of your day-to-day activities
- Anyone offers you money to record account information
- Anyone asks for customer account information over the telephone

Call your Merchant Processing Center or Company Security and let them know IMMEDIATELY!

What does a skimming device look like?
Skimming devices record and store credit card account information. Most skimming devices are small and portable—and may resemble a pager.

What is skimming?
Skimming is an illegal act that helps criminals obtain credit card account information to produce counterfeit cards.

How does skimming work?
Typically, someone in a workplace uses a small device to steal information from a credit card's magnetic stripe. That information is put onto a counterfeit card and used to make fraudulent purchases.

Say NO to criminal activity and you could earn a reward!

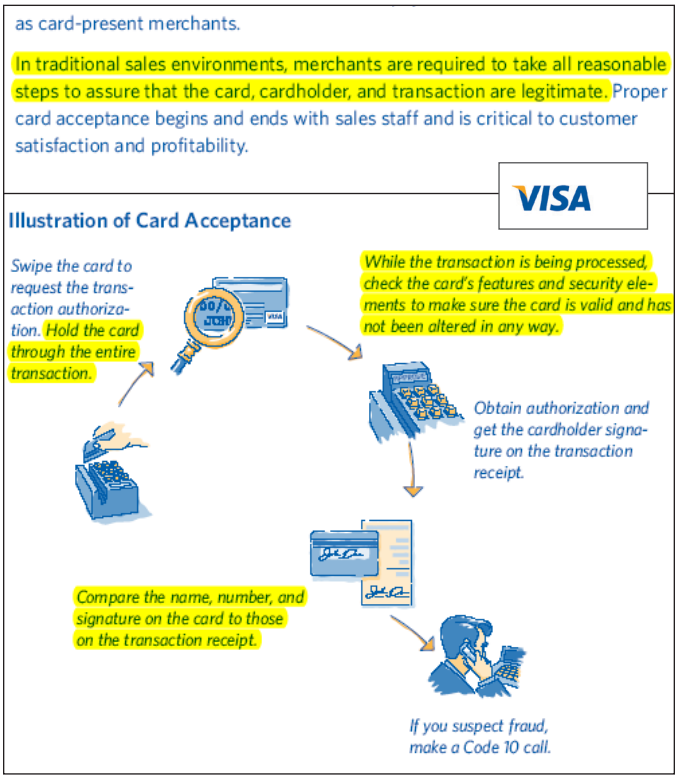
Visa will pay a reward of up to $1,000 for information leading to the arrest and conviction of anyone involved in the manufacture or use of counterfeit cards.

Be assured that the card, cardholder, and transaction are legitimate

Magensa is more than a "reasonable" step to assure legitimacy Magensa services can assure the card, the cardholder and the transaction's authenticity. This exponentially limits fraudulent claims and liability and provides more immediate access to rewards.

Only Magensa can authenticate the:

1. Card
2. Cardholder
3. Reader
4. Card data
5. Host/network



as card-present merchants.

In traditional sales environments, merchants are required to take all reasonable steps to assure that the card, cardholder, and transaction are legitimate. Proper card acceptance begins and ends with sales staff and is critical to customer satisfaction and profitability.

VISA

Illustration of Card Acceptance

Code 10 fraud alerts for counterfeit cards delivered

Magensa provides the reporting you need

Magensa delivers alerting and reporting services that can help prevent theft. Our real-time fraud alerts protect you from charge backs, tampering, illegal (rogue) devices, unauthorized devices, replays, expired sessions, counterfeit cards, illegal and out of pattern usage preventing fraud, and providing a true return on investment. Magensa also provides the best in custom analytical reporting so you get the information you need, when you need it, saving countless time and resources. Our team of experts will work with you to determine the most critical elements for your specific transactional needs.

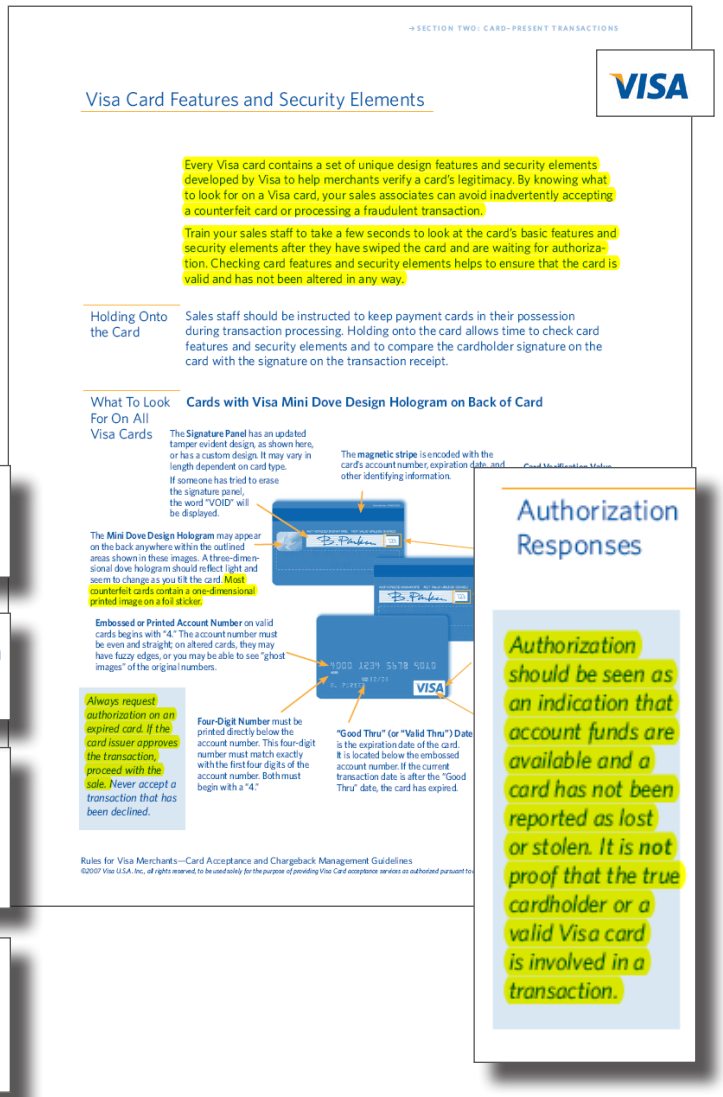
Emphasize to your sales staff that they can make Code 10 calls even after a cardholder leaves the store. A Code 10 alert at this time may help stop fraudulent card use at another location, or perhaps during a future transaction at your store.

If you are suspicious about the transaction or feel you need additional information to insure the identity of the cardholder, make a Code 10 call.

When Something Doesn't Look Right

If any of the Visa card security features is missing or looks altered, keep the card in your possession and make a Code 10 call to your authorization center. You may be instructed to try to recover the card or simply to return it to the cardholder and decline the transaction (see *Code 10 Calls* on page 33).

If you feel really uncomfortable or suspicious about a cardholder or transaction, keep the card in your possession and make a Code 10 call. In any situation where making the call with the customer present feels inappropriate or unsafe, complete the transaction, return the card, and make the call immediately after the customer leaves.



→ SECTION TWO: CARD-PRESENT TRANSACTIONS

VISA

Visa Card Features and Security Elements

Every Visa card contains a set of unique design features and security elements developed by Visa to help merchants verify a card's legitimacy. By knowing what to look for on a Visa card, your sales associates can avoid inadvertently accepting a counterfeit card or processing a fraudulent transaction.

Train your sales staff to take a few seconds to look at the card's basic features and security elements after they have swiped the card and are waiting for authorization. Checking card features and security elements helps to ensure that the card is valid and has not been altered in any way.

Holding Onto the Card

Sales staff should be instructed to keep payment cards in their possession during transaction processing. Holding onto the card allows time to check card features and security elements and to compare the cardholder signature on the card with the signature on the transaction receipt.

What To Look For On All Visa Cards

Cards with Visa Mini Dove Design Hologram on Back of Card

The **Signature Panel** has an updated tamper evident design, as shown here, or has a custom design. It may vary in length dependent on card type.

If someone has tried to erase the signature panel, the word "VOID" will be displayed.

The **magnetic stripe** is encoded with the card's account number, expiration date, and other identifying information.

The **Mini Dove Design Hologram** may appear on the back anywhere within the outlined areas shown in these images. A three-dimensional dove hologram should reflect light and seem to change as you tilt the card. Most counterfeit cards contain a one-dimensional printed image on a foil sticker.

Embossed or Printed Account Number on valid cards begins with "4." The account number must be even and straight; on altered cards, they may have fuzzy edges, or you may be able to see "ghost" images" of the original numbers.

Always request authorization on an expired card. If the card issuer approves the transaction, proceed with the sale. Never accept a transaction that has been declined.

Four-Digit Number must be printed directly below the account number. This four-digit number must match exactly with the first four digits of the account number. Both must begin with a "4."

"Good Thru" (or "Valid Thru") Date is the expiration date of the card. It is located below the embossed account number. If the current transaction date is after the "Good Thru" date, the card has expired.

Rules for Visa Merchants—Card Acceptance and Chargeback Management Guidelines

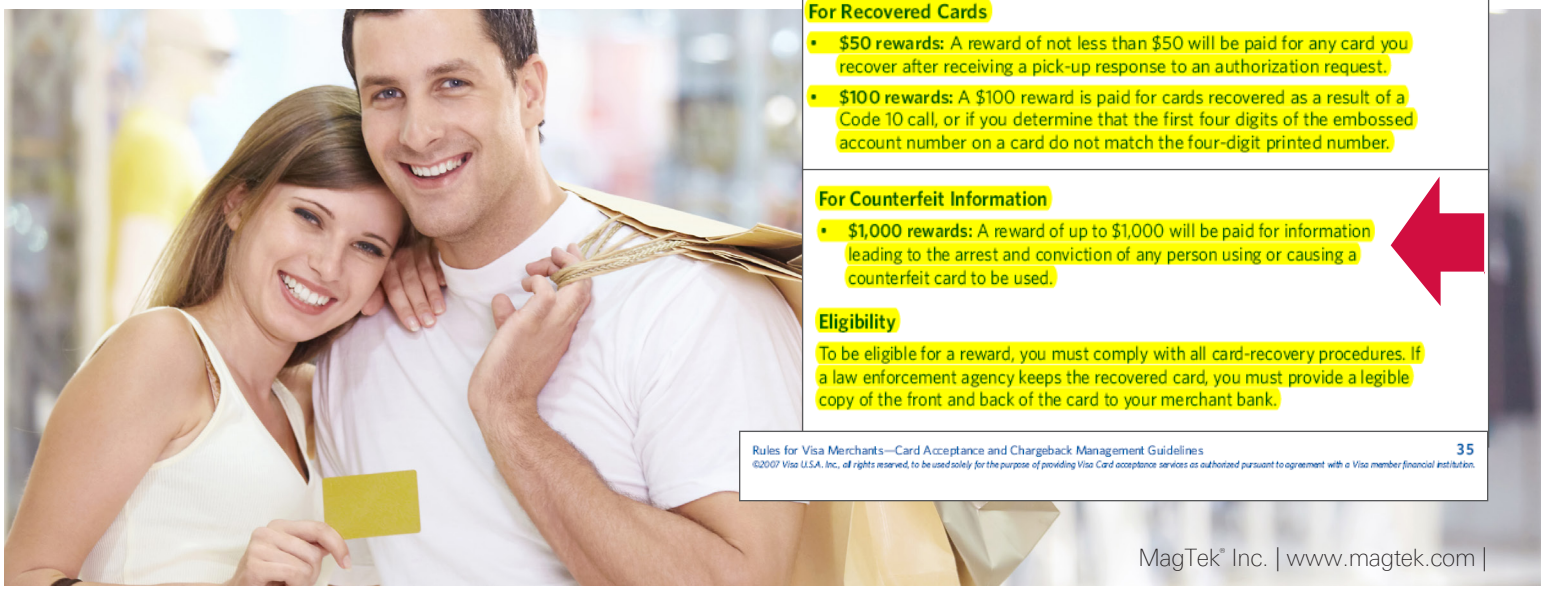
Authorization Responses

Authorization should be seen as an indication that account funds are available and a card has not been reported as lost or stolen. It is not proof that the true cardholder or a valid Visa card is involved in a transaction.

Forensic evidence to stand up in court

Magensa provides you with specific evidence

A Key feature of Magensa services is its ability to provide real-time forensic evidence using authentication scoring, dynamic digital identifiers, session IDs and digital signatures coupled with complete data protection.



Cash Rewards

Cash rewards are available to merchants and their employees for recovering counterfeit or other fraudulent cards, or for information leading to the arrest and conviction of any person or persons involved in a counterfeit scheme. Eligibility for specific rewards is as follows:

For Recovered Cards

- **$50 rewards:** A reward of not less than $50 will be paid for any card you recover after receiving a pick-up response to an authorization request.
- **$100 rewards:** A $100 reward is paid for cards recovered as a result of a Code 10 call, or if you determine that the first four digits of the embossed account number on a card do not match the four-digit printed number.

For Counterfeit Information

- **$1,000 rewards:** A reward of up to $1,000 will be paid for information leading to the arrest and conviction of any person using or causing a counterfeit card to be used.

Eligibility

To be eligible for a reward, you must comply with all card-recovery procedures. If a law enforcement agency keeps the recovered card, you must provide a legible copy of the front and back of the card to your merchant bank.

Rules for Visa Merchants—Card Acceptance and Chargeback Management Guidelines 35

Magensa delivers

MagneSafe™ security MagneSafe™ is a digital identification and authentication architecture that safeguards consumers and their personal data. Designed to exceed PCI regulations, MagneSafe leverages strong encryption, secure tokenization, counterfeit detection, tamper recognition, data relevance and integrity, and dynamic digital transaction signatures, which together validate and protect the entire transaction and each of its components.

A key feature of MagneSafe is MagnePrint® card authentication, a patented, proven technology which reliably identifies counterfeit credit cards, debit cards, gift cards, ATM cards and ID cards at the point of swipe, before fraud occurs. MagneSafe's multi-layer security provides unmatched protection and flexibility for safer online transactions.

MagneSafe secure card reader authenticators are characterized by their ability to:

- Read and encrypt cardholder data at the earliest point possible
- Generate a unique encryption key per swipe
- Mutually authenticate the reader and a legitimate host
- Manage time bound sessions
- Capture and transmit the dynamic digital identifiers of the card and cardholder data
- Generate a unique token of the transaction

Look for the MagneSafe logo at the point of swipe.

See a return on investment where it matters most to you

Magensa lets you be in control

You don't need to wait for anyone else in the transaction process to take advantage of the benefits that Magensa delivers. You can benefit from Magensa services immediately:

- Use Magensa where you need it
- Provide real-time forensic evidence now
- Save time and money on resources
- Prevent fraud and earn industry rewards

Magensa is a security investment with guaranteed returns

Magensa is a fraud prevention, detection and alerting service. It maintains a globally accessible registry of authentication information so that financial institutions, retailers, consumers, business, and government can assess the validity and trustworthiness of the credentials and products they rely upon in the course of online identification, payment, and other high value transactions.

Additionally, Magensa provides cryptographic services, vital to the protection of consumers, payment system intermediaries, and their personal or sensitive information. The company also performs device, key, session, data integrity and token management, for its customers. Its encryption packets are size and format compatible with magnetic stripe track data, minimizing the need for infrastructure changes.

Magensa maintains PCI compliance at all times, does not store cardholder track data, and undergoes annual PCI audits of its geographically separated, redundant data processing facilities. Magensa is a subsidiary of MagTek, Inc.

MAGTEK®
SECURITY FROM THE INSIDE

Founded in 1972, MagTek is a leading manufacturer of electronic systems for the reliable issuance, reading, transmission and security of cards, checks, PINs and identification documents. Leading with innovation and engineering excellence, MagTek is known for quality and dependability. Its products include secure card reader/authenticators, token generators, EMV contact, contactless and NFC reading devices, encrypting check scanners, PIN pads and distributed credential personalization systems for secure magstripe and EMV enabled cards. These products are used worldwide by financial institutions, retailers, and processors to provide secure and efficient payment and identification transactions. Today, MagTek continues to innovate. Its MagneSafe™ Security Architecture leverages strong encryption, secure tokenization, dynamic card authentication, and device/host validation enabling users to assess the trustworthiness of credentials and terminals used for online identification, payment processing, and high-value electronic transactions. MagTek is headquartered in Seal Beach, CA.