Payment Card Technology Solutions to Prevent Fraud

Visa is leading the industry in developing a comprehensive approach to making payments safe through smarter technologies, so consumers and businesses can pay or be paid with confidence.

Our approach is to make payment data unusable to criminals. There are three technologies that are being deployed to reduce or eliminate the ability to misuse this sensitive data.

Together, these technologies will significantly reduce payment fraud in the U.S. and around the world and help protect merchants from cyber security threats.

The Three-Pronged Approach

	What is it?	*How does it protect cardholders?*	*When can I use it in the U.S.?*
Chip (EMV)	Chip technology is a computer chip that adds an extra layer of protection for plastic payment cards and other form factors, such as mobile phones. Sometimes referred to as a smart card or chip card, a chip securely stores the payment data that currently resides on the magnetic stripe, and enables more secure processing by generating a unique, one-time use code for each transaction.	Today, criminals try to steal account information in order to counterfeit cards that can be used to make fraudulent purchases or ATM withdrawals. Chip cards protect payments by generating a unique, one-time code needed for the transaction to be approved. This feature cannot be replicated in counterfeit cards, reducing fraud.	Chip cards are already the norm in Europe and many other countries, with 2.4 billion chip cards in circulation worldwide. An industry analyst estimates that by the end of 2015, about 70 percent of credit cards and 41 percent of debit cards[1] will be chipped in the United States. Many national retailers have committed to making the upgrade as well.
Tokenization	Tokenization protects your account information by replacing it with a digital alias or "token" that has no value if stolen.	Tokens can be restricted for use with a specific merchant, mobile device, transaction or category of transactions. The merchant does not need to store your personal account information when processing a payment, protecting data from theft. All of this means that if a token is stolen or intercepted in the payment process, the data is worthless. Further, tokens simplify the purchasing experience for consumers by eliminating the need to enter and re-enter the account number when shopping on a smart phone, tablet or computer.	Visa, MasterCard and American Express worked together to develop an open, industry standard for tokenization services managed by EMVCo. Visa launched its token service in **September 2014**.

[1] AITE

Point-to-Point Encryption (P2PE)

What is it?

Point-to-point encryption (P2PE) is a secure method of transmitting data across the payment chain, masking the cardholder's 16-digit account number in such a way that only legitimate entities can unlock and read it.

How does it protect cardholders?

Encrypted data is useless to criminals because they cannot unmask it to reveal the original account information without the decryption key, which is held securely by the acquirer, gateway or Visa.

When can I use it in the U.S.?

Encryption technologies are already available today. Visa offers its own encryption service, **Visa Merchant Data Secure** with Point-to-Point Encryption. This service has been available to acquirers and their merchants since early 2013.

Visa is Committed to Preventing Fraud

Visa continues to make advances in spotting fraudulent purchases in real-time through predictive analytics. In a split second, Visa analyzes multiple data sets such as past transactions, whether the account has been involved in a data compromise, global fraud trends, and nearly 500 other pieces of data to create a risk score. This intelligence helps identify criminal patterns and prevent fraud before it happens.

Visa services, including ***Visa Advanced Authorization*** and ***Visa Transaction Advisor***, provide an instantaneous rating of a transaction's potential for fraud.