First Data
b›yond the transaction

TransArmor® Solution

Protect valuable payment card data from the moment of swipe throughout the transaction with the First Data® TransArmor® solution.

Go Beyond: TransArmor® Solution

The First Data® TransArmor® solution is powerful payment card security that combines the flexibility of software- or hardware-based encryption with random-number tokenization technology. With the TransArmor solution, payment card data is protected at every transaction stage – in transit, in use and at rest – reducing the risk of data breach as well as the scope and costs of PCI compliance.

First Data Advantages

The TransArmor solution was developed through partnership between First Data, VeriFone Systems and RSA, the Security Division of EMC. It provides an easy way to protect your business and your customers from the growing threat of card information theft.

Combines Two Layers of Powerful Payment Card Data Protection

→ Protects data in transit with state-of-the-art encryption options that secure data from the moment of swipe throughout the transaction

→ Removes data from the card data environment (CDE) after authorization by replacing it with a token or randomly generated number

- Eliminating card data helps prevent a data breach - the best way to protect card data is not to have any at all

→ Reduces the risk of data loss, brand damage, customer confidence, financial liability and litigation due to a security breach

- Safely stores non-sensitive tokenized card data for use in back-end business operations and customer analytics

Offers Multiple Encryption Types to Protect Merchants in any Industry

→ Multiple encryption options let merchants choose an encryption type based on their needs and, in many cases, use existing terminals or hardware

- Software-based encryption provided by RSA's Public Key Infrastructure, can be installed on terminals or PC-based POS systems, letting you add the TransArmor solution with little-to-no investment in new or upgraded hardware
- Hardware-based, format-preserving encryption, offered on standalone and integrated VeriFone devices, through the TransArmor solution, VeriFone edition, usually requires no software changes at the POS application level and no extra steps or training for the retailer

Helps Reduce PCI Compliance Time, Costs and Effort

→ Removing card data from merchant systems also removes it from PCI scope, minimizing time and resources needed to meet PCI requirements

- Can reduce the scope of annual PCI audits by as much as 80%[1]
- Can reduce the time PCI compliance requires by as much as 50%[2]

89%

Most organizations suffering a data breach were not validated compliant with PCI DSS at the time of the breach[3]

$1 Billion

Total amount businesses have collectively spent on PCI-DSS Compliance[4]

$214

Average cost for businesses per compromised record[5]

PCI Compliance requires significant – and on-going – effort and is no guarantee of security against a breach

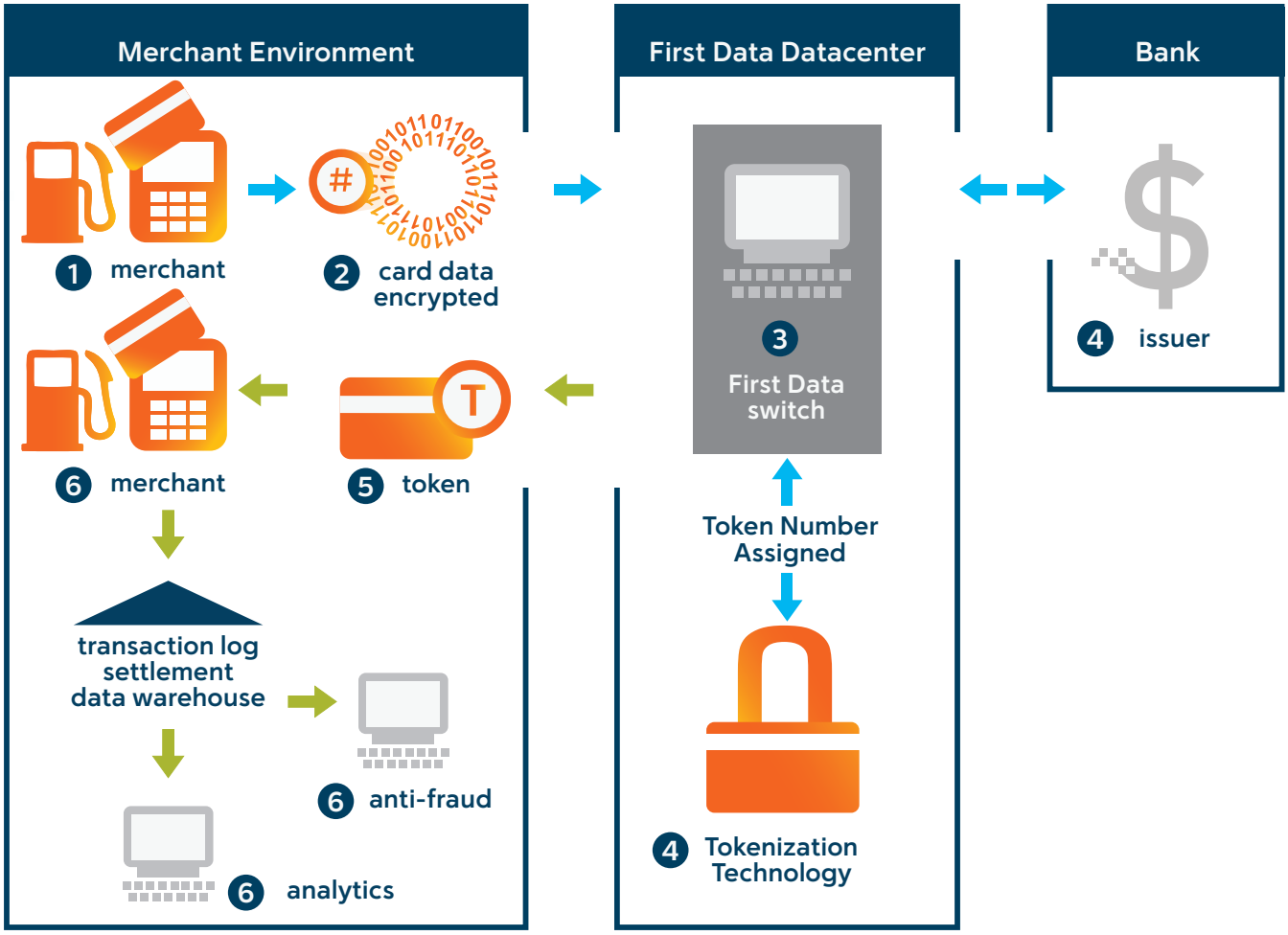
TransArmor® Solution

First Data

Dual-Layered Payment Card Security

While encryption protects payment card data with an algorithm and a secret key, tokenization is the critical second security layer that completely eliminates card data from the environment, replacing it with a random-number token. Tokens are useless to criminals yet remain in the format of payment card data so merchants can carry out existing processes. Tokens also retain the business advantage of card data for analyzing customer buying behavior. This dual-layered security solution protects payment card data from the moment of initial capture through the entire payment process.

How the TransArmor Solution Works



1. Consumer presents card to merchant POS
2. Card data is encrypted and transmitted to First Data front-end
3. First Data front-end decrypts the data payload
4. Card data is sent to issuing bank for authorization and, in parallel, tokenized
5. Token is paired with authorization response and sent back to the merchant
6. Merchant stores token instead of card data in their environment and uses token for subsequent business processes

TransArmor® Solution

First Data

Multi-Pay Tokens

The TransArmor solution includes the Multi-Pay Token option to support businesses that need to submit a financial transaction in a card-not-present situation. These tokens are unique to each merchant that uses them and are stored in place of the primary account number (PAN). With these tokens, merchants can initiate new or recurring payments within their own environment instead of using the original card number.

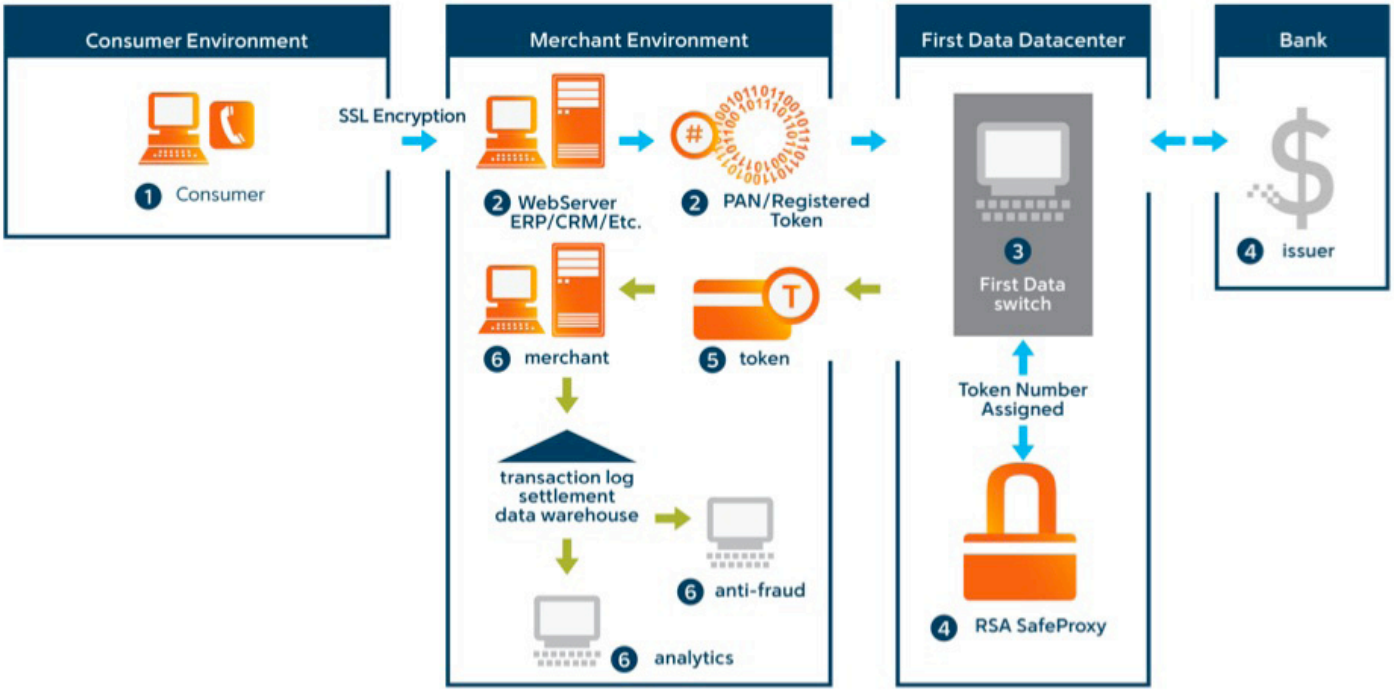
→ Valuable for eCommerce and card-not-present environments

→ Supports all businesses that rely on the ability to submit a sale transaction without card being present

→ Can be used for refunds and credits

→ Tokens let merchants track buying patterns for sales trending and marketing/loyalty programs while remaining PCI compliant

How TransArmor Works in a Card Not Present Environment



1. Card data is keyed into payment page/IVR. If e-Wallet technology is used, a consumer token can be used to initiate a new transaction
2. PAN is encrypted using session encryption and sent to First Data
3. Encrypted session is received at First Data datacenter
4. Card number is passed to bank for authorization and SafeProxy server for tokenization
5. Authorization and Multi-Pay Token are returned to the merchant
6. Multi-Pay Token is stored in place of the card number in all places
7. New financial transactions including sales, adjustments, refunds and settlement use the Multi-Pay Token instead of the PAN

TransArmor® Solution

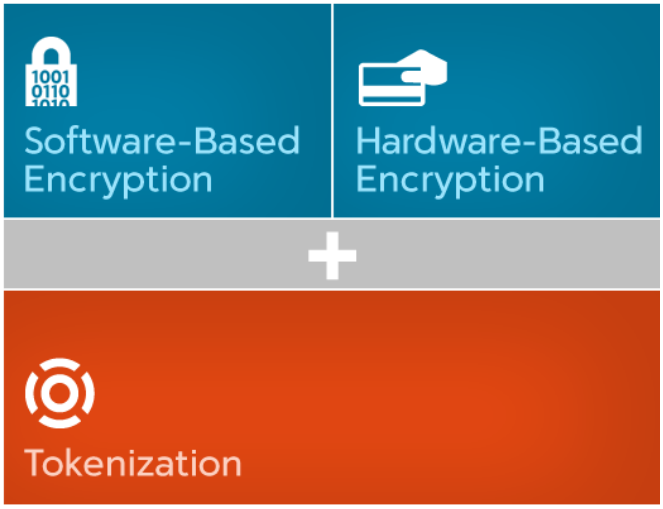
First Data™

Software-based Encryption

With asymmetric encryption supported by RSA technology, data is secured at the merchant point-of-sale (POS) with the Public Key and can only be decrypted by the Private Key held at First Data. The encrypted data is indecipherable, does not resemble the original data format and works on most existing POS terminals and systems.

Hardware-based Encryption

Hardware-based, format-preserving encryption–available through the TransArmor solution, VeriFone edition—secures payment card data on a tamper-resistant device before it enters the merchant environment in a format that other applications interpret as valid card data. In VeriFone's format-preserving encryption, the algorithm encrypts data so that the output is in the same length and character set as the input, which is beneficial for bin routing and coding/certification.



Tokenization Technology

Tokenization is a form of data substitution replacing sensitive values with non-sensitive token values. Post-authorization transactions are handled via RSA's SafeProxy tokenization service, which returns a token with the transaction's authorization to the merchant. A token can then be stored in the merchant environment in place of the primary account number (PAN) making it possible for a merchant to process follow-on transactions, without having to store customer's account data in the clear.

→ Removes need for merchant to retain PANs in card data environment (CDE)

→ Tokens are non-reversible and are not mathematically derived from PAN

→ Tokens cannot be used by an unauthorized party to conduct fraudulent transactions

→ Tokens match the format of the initiating PAN

→ Tokens do not overlap major brand (Visa, MC, AMEX, Discover) BIN ranges (first digit is 0-2 or 7-9)

→ Tokens are card-based, meaning a merchant will always get the same token back for a specific PAN

→ Tokens share last four digits with corresponding PAN

Legacy Data Conversion

Beyond encrypting and tokenizing data for transactions at the point of sale, merchants also need to consider the risk of stored primary account numbers (PAN) in their card data environment. To help prevent potential breaches and reduce PCI scope and maintenance costs, merchants can obtain an additional service offering, Legacy Data Conversion.

In this optional service, merchant's legacy or stored PAN data is completely removed from the card data environment (CDE) and replaced with TransArmor tokens. The tokens can then be used similarly to any other TransArmor token to perform customer analytics and understand consumer buying behavior.

Payment Solutions for Maximum Performance

Around the world every day, First Data makes payment transactions secure, fast and easy for merchants, financial institutions and their customers. We leverage our unparalleled product portfolio and expertise to deliver processing solutions that drive customer revenue and profitability. Whether the payment is by debit or credit, gift card, check or mobile phone, online or at the point of sale, First Data helps you maximize value for your business.

FOR MORE INFORMATION
contact Mike Gilmore
at (800) 824-1594
sales@ignitepaymentschipcard.com

[1] Interview with CoalFireSystems [2] Interview with SecurityMetrics. [3] Verizon, 2011 Data Breach Investigations Report, Verizon Business RISK Team in cooperation with the U.S. Secret Service, 2010 [4] Letter to Bob Russo of the PCI Security Standards Council from the National Retail Federation, et. al., June 9, 2009. [5] Ponemon Institute, LLC, 2010 Annual Study: U.S. Cost of a Data Breach, March 2011