Reducing the Risk of a Data Breach
How small businesses can thwart data thieves
Data breaches are constantly in the news, and recent high profile cases show that no organization is immune—especially as criminals develop increasingly sophisticated methods to exploit vulnerabilities in the payment system.

Studies show that small- and medium-sized businesses are especially vulnerable to being victimized by a data breach—and the lost business and fines that result can be catastrophic. Fortunately, there are simple solutions available that can cost-effectively safeguard sensitive data and reduce the risk of a data breach.

The following pages explain vulnerabilities in the payment process and describe how merchants can mitigate payment security risk.
SENSITIVE DATA AT RISK

During a purchase transaction, payment card data flows through multiple parties and systems in order to be processed. There are two points in the process where sensitive data is vulnerable to theft or exposure:

- Pre-authorization: after the merchant captures the data and it is being transmitted for authorization
- Post-authorization: when the data has been sent back to the merchant and is placed into storage
Fortunately, there are highly effective technologies available to address these two specific points of vulnerability: encryption and tokenization. Encryption mitigates security weaknesses that exist when cardholder data has been captured but not yet authorized. Tokenization addresses security vulnerabilities after a transaction has been authorized.
Whenever card data is in a plain text format—as it is when it’s being captured and transmitted at the POS—it is extremely vulnerable to theft. Merchants can significantly reduce this threat using encryption, which transforms plain text information into a non-readable form called ciphertext.

Data Encryption
Card Data in Plain Text
3456 7890 1112 1314

Algorithm

E4%c/0%v29u8Db4)x7Hw
Ciphertext
Merchants can protect sensitive data after authorization with tokenization, which replaces cardholder data with a sequence of randomly generated numbers. The tokenized number can then be safely stored by the merchant in its back office processes.
Payment security is complex, with risks and vulnerabilities throughout the transaction process. Continuously emerging new data security threats make it essential for merchants to implement solutions to avoid the disastrous consequences of a data breach. Encryption and tokenization solve for mutually-exclusive security weaknesses in the payments process—and in doing so, can also reduce a merchant’s PCI scope and compliance costs.

The First Data TransArmor® solution makes cardholder data significantly more secure by combining encryption and tokenization for superior protection. It is an easy-to-implement payment security service that removes card data completely from the merchant environment, protecting customers’ sensitive information, limiting merchant liability and simplifying PCI compliance.