



TOKENIZATION IS ONE INNOVATIVE TECHNOLOGY THAT BANKS USE TO PROTECT CUSTOMERS FROM FRAUD

OTHER TECHNOLOGIES



EMV CHIP
creates unique cryptogram for each transaction



ENCRYPTION
Codes data so that only verified parties can read it

3 WAYS TO PAY



ONLINE
MOBILE OR WEB



SMART PHONES
NFC, QR, Bluetooth



CARD

3 TYPES OF FRAUD

45% CARD NOT PRESENT

Account data is used (primarily at online retailers)
Fought by encryption and tokenization



38% COUNTERFEIT

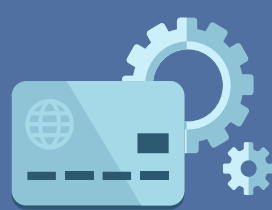
Card duplicated using account data
Fought by both encryption and EMV



13% LOST/STOLEN

Fought by signature or pin

WHY USE TOKENIZATION?



PERSONAL ACCOUNT NUMBER
USABLE IF STOLEN

=



TOKEN
USELESS TO THIEVES

- Replaces sensitive customer account data with a secure alternative, or a token
A token is a unique number that is useless if stolen
- Takes place instantly behind the scenes and requires no action by the customer
- Runs on payments systems that are in use today

HOW ARE TOKENS ISSUED?

When a customer makes a transaction, their account number passes through the network



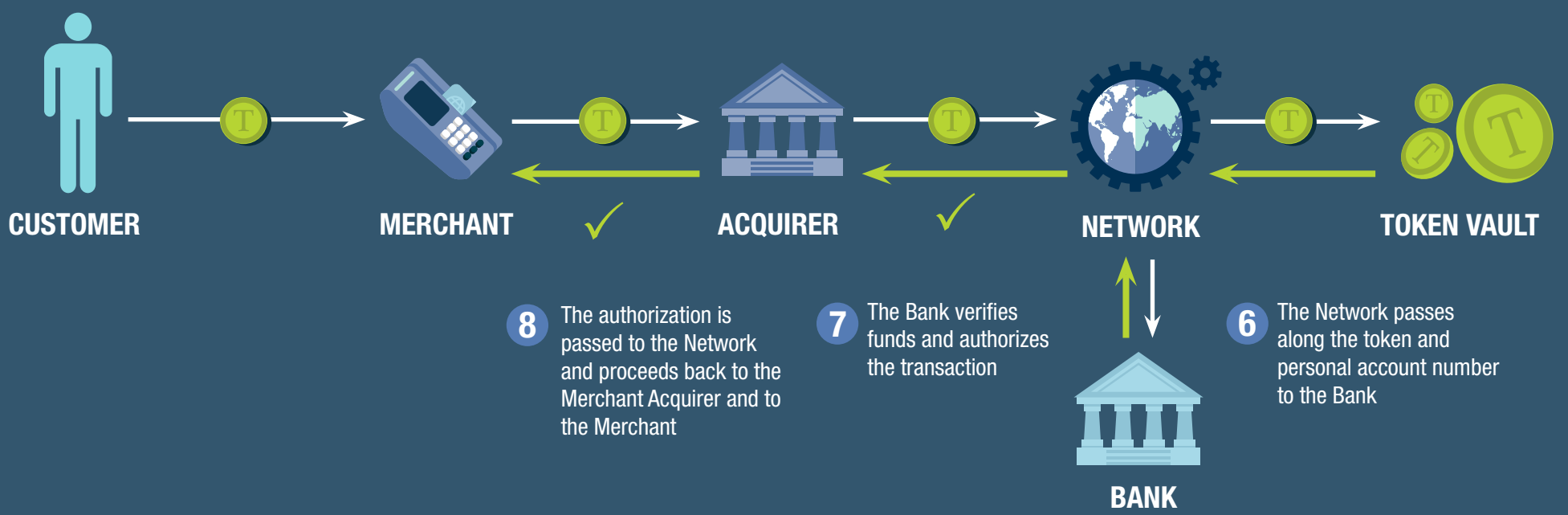
The network verifies the account information with the bank

The network issues a token to replace the account number



HOW DOES A TOKENIZED TRANSACTION WORK?

- When paying—either via online purchase or tap-to-pay—the token goes to the Merchant
- The Merchant passes the token along to their Merchant Acquirer
- The Merchant Acquirer passes the token to the Network
- Once passed to the Network, the data is within the secure bank vault
- The network consults its "Token Vault" to match the token with the customer's account number



TOKENS ARE USELESS IF STOLEN

Tokens can be configured so that they are only good for transactions that fit specific criteria

Even if the retailer systems are compromised, thieves can only get tokenized data. Since tokenized data is useless to a fraudster, the customer is protected despite the data breach.



GOOD FOR A SET PERIOD OF TIME



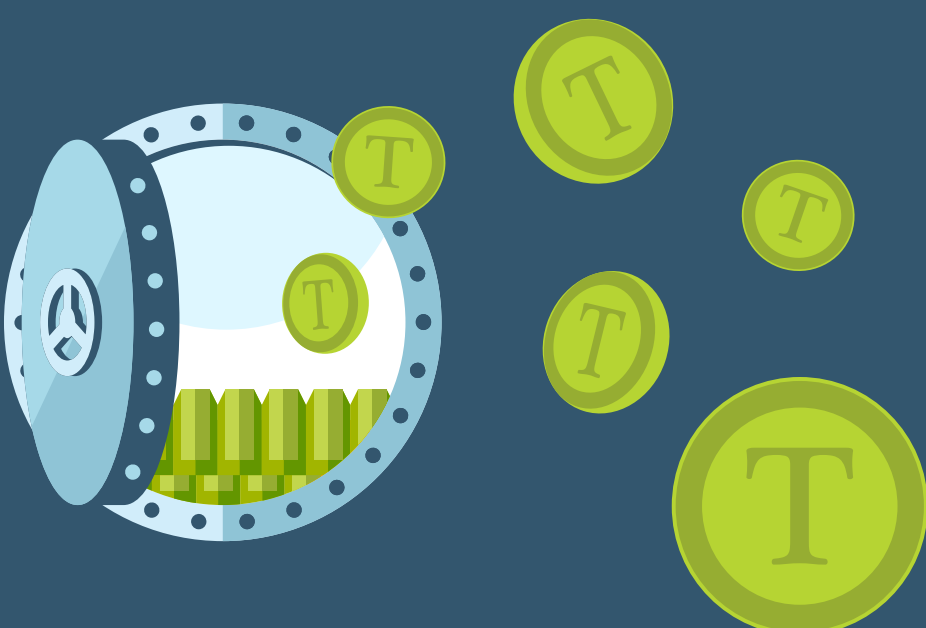
GOOD ONLY FROM A SPECIFIC RETAILER



GOOD FOR ONLY A CERTAIN DOLLAR AMOUNT



After a data breach, if a token is used elsewhere, the network can detect the token as stolen and will reject the fraudulent transaction.



Although customers may not see it, banks are adopting many invisible technologies to protect against fraud. Tokenization is one technology that banks are using to protect customers when they pay online or with their smart phone.

To learn more, visit aba.com/PaymentsandCyber.