A changing world requires evolving security.

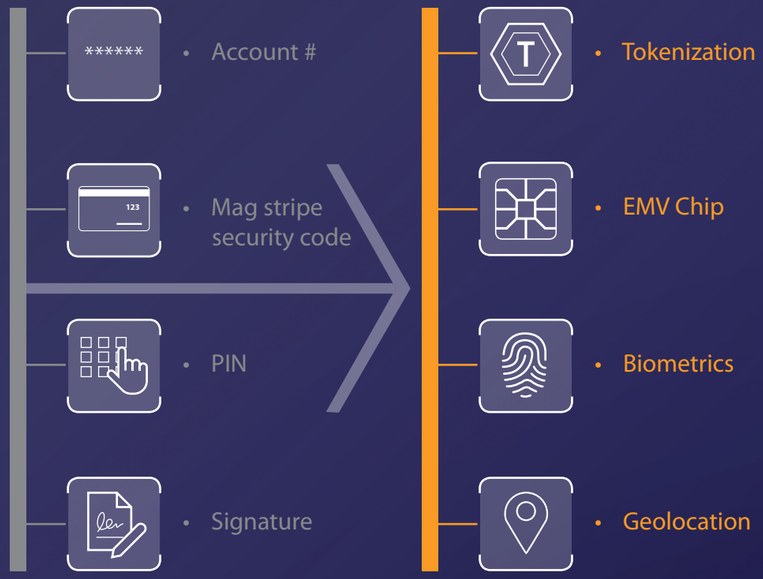
Security must move at the speed of innovation.

For more than 50 years, Visa has helped set the bar for payments security, keeping fraud rates low (about 6 cents out of every $100 transacted with Visa), despite increasing security threats and pressures. This is because Visa is continually advancing our defenses and investing in technologies and strategies to stay ahead of criminals.

To keep consumers and merchants safe and free from liability, we need to change the security discussion.

From static and knowledge-based security instruments that can be stolen or forged.

To stronger and more dynamic technologies that better prevent fraud.



Visa's U.S. Security Roadmap.

Criminals have a number of channels for stealing account data and using it to commit fraud. This multi-faceted threat requires a dynamic approach. With multiple technologies in place for detecting and preventing fraud, Visa is driving security across payments—online, in-store and on-the-go.

Real-time Fraud Analytics:
Evaluates up to 500 data elements in less than a millisecond to spot suspicious transactions as they occur.

Ecommerce and Remote Payments Fraud

Tokenization of Digital Payments
Secures digital data from risk of compromise.

Consumer Transaction Alerts
Message delivered directly via email, text message or mobile banking app to alert enrolled cardholders of suspicious activity on their account.

Dynamic Passcode
One-time code sent to card holder via mobile text or app to uniquely verify a transaction.

Verified by Visa / Visa Consumer Authentication Service
Additional layer of analytics, intelligence, and password security to protect ecommerce transactions.

Encryption
Securely locks sensitive account information as a transaction is processed. The data can't be read or unlocked if stolen or compromised.

Device Identification
Evaluates the unique ID of the device (mobile phone, laptop, etc.) used to make a digital transaction to help identify suspicious transactions.

Counterfeit Fraud

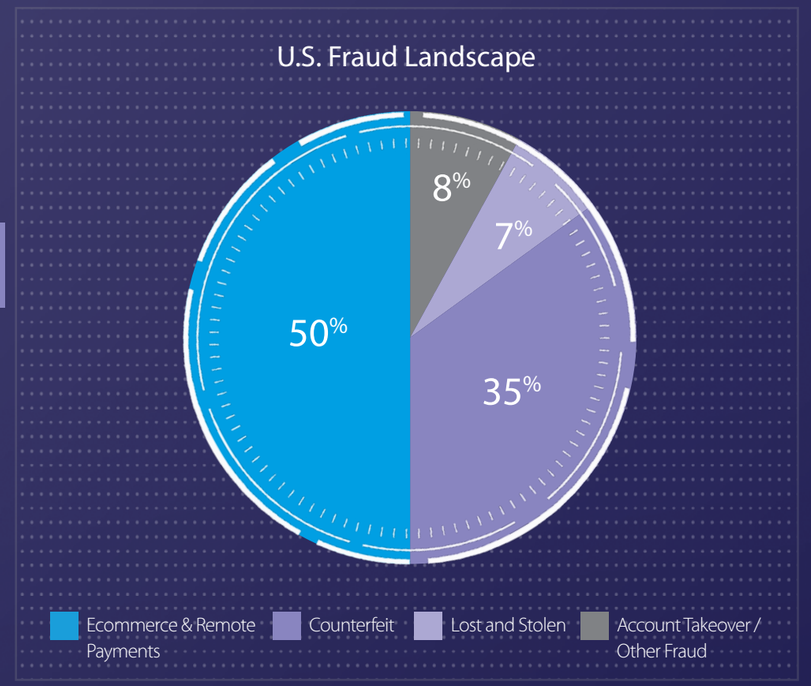
EMV Chip
Prevents counterfeit fraud by generating a one-time use code, making every in-store transaction unique.

Geolocation
Matches a cardholder's mobile phone location with the location of a Visa transaction.

Chip Card Tokenization
Secures digital data from risk of compromise.

Consumer Transaction Alerts
Message delivered directly via email, text message or mobile banking app to alert enrolled cardholders of suspicious activity on their account.

Encryption



Lost and Stolen Fraud

Biometrics
Uses unique consumer identification such as a fingerprint or voice to verify the cardholder.

PIN
Used today for ATM and Debit.

Geolocation

Consumer Transaction Alerts

Account Takeover/Other Fraud

Voice biometric authentication at banking call centers.

Online activity analytics to identify account takeover fraud.

Telephone analytics software to validate customer identity.

Source: Visa Fraud Performance Benchmarking, fraud dollar distribution by fraud type for US domestic fraud excluding cash for calendar year 2015