The Evolution of Payment Security.

Since the inception of the payments industry, Visa has been a leader in security. As technology has advanced, Visa's innovations have kept pace, helping to steadily reduce fraud rates despite a growing number of data breaches.

**Analog**
Introduction of plastic cards and standards
- 1959: Introduction of the first card made of plastic (previously made of cardboard and celluloid)
- 1970s: Visa adds tamper-resistant signature panel, card embossing, and microprint security features to protect cards from counterfeit

**Electronic**
Development of risk scoring and more advanced fraud systems; industry experiences first processor data breaches
- 1988: Visa Card Recovery Bulletin lists lost, stolen, due-out, over-limit, counterfeit or otherwise problem cards
- 1989: Visa Issuers' Clearinghouse Service provides centralized database of approved and fraudulent card applications
- 1990: Visa uses neural network technology to risk score transactions
- 1994: Visa, Europay, and MasterCard, provide EMV specification for chip cards
- 1995: Visa publishes first set of PIN security requirements that protect cardholder-PINS at POS
- 1996: Visa Address Verification Service allows ecommerce merchants to verify the cardholder’s billing address
- 1997: Credit and debit cardholders are not responsible for fraudulent transactions as a result of Visa Zero Liability
- 1999: Visa introduces Card Verification Value 2 (CVV2), the 3 digit security code used in ecommerce transactions

**Digital**
Advancements in technology allow for development of tokenization and launch of Apple Pay; breaches shift away from processors to merchants
- 2004: Visa joins other networks to form the Payment Card Industry (PCI) Security Standards Council and release the PCI Data Security Standard
- 2005: Visa Advanced Authorization detects potential fraud globally, in real time
- 2009: Visa transaction alerts provide near real-time alerts to consumers when transactions meet certain criteria
- 2010: Visa requires PIN encryption at point-of-sale
- 2011: Michaels breaches (one in 2011, two in 2013) potentially compromise PIN numbers and ~300,000 payment card accounts
- 2012: Visa Consumer Authentication Service improves commerce fraud detection using advanced issuer analytics
- 2013: Risk scoring improvements boost Visa fraud detection up to 130% for debit and 175% for credit transactions

**Next Generation**
Shift from static and knowledge-based solutions that can be stolen or forged to dynamic and more resilient technologies
- **Tokenization**
  - Visa Token Service available for Visa Checkout and "card-on-file" digital merchants
- **Biometrics**
  - Visa publishes biometrics specification for chip card transactions
- **Geolocation**
  - Visa Mobile Location Confirmation matches the location of a registered mobile device to the location of a Visa transaction for more accurate risk scoring
- **Chip**
  - Chip card technology comes to U.S. consumers and businesses
- **Cybersecurity**
  - Visa and FireEye launch Visa Threat Intelligence
- **Encryption**
  - Visa expands merchant incentives to encourage point-to-point encryption through the Visa Technology Innovation Program

**Beyond**
- **Tokenization**
  - Extend tokenization use cases to other channels and new merchant segments
- **Biometrics**
  - Shift to stronger forms of authentication and drive continued uptake of secure biometric verification methods
- **Geolocation**
  - Use mobile phones as a proxy for consumer identity
- **Chip**
  - Continue to drive secure payments with chip technology supporting mobile payments
- **Data Analytics**
  - Increase engagement from all stakeholders in fraud prevention using real-time transaction alerts
  - Continue to broaden use of mobile data in risk scoring
  - Enable an increasing set of stakeholders to use Visa risk scores