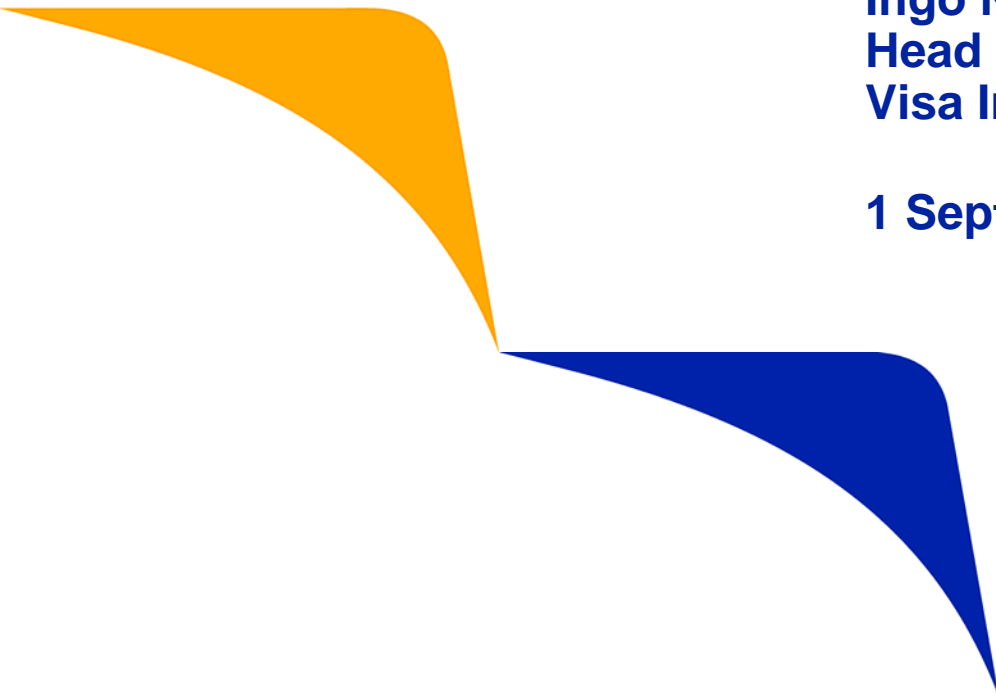




Innovation in Payment Card Fraud Management

**Ingo Noka
Head of Country Risk Management
Visa International**

1 September 2010



Notice of Disclaimer



Case studies, statistics, research and recommendations are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. When implementing any new strategy or practice, you should consult with your legal counsel to determine what laws and regulations may apply to your specific circumstances. The actual costs, savings and benefits of any recommendations or programs may vary based upon your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties and assumptions that are difficult to predict or quantify. Assumptions were made by us in light of our experience and our perceptions of historical trends, current conditions and expected future developments and other factors that we believe are appropriate under the circumstance. Recommendations are subject to risks and uncertainties, which may cause actual and future results and trends to differ materially from the assumptions or recommendations. Visa is not responsible for your use of the information contained herein (including errors, omissions, inaccuracy or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use. Visa makes no warranty, express or implied, and explicitly disclaims the warranties of merchantability and fitness for a particular purpose, any warranty of non-infringement of any third party's intellectual property rights, any warranty that the information will meet the requirements of a client, or any warranty that the information is updated and will be error free. To the extent permitted by applicable law, Visa shall not be liable to a client or any third party for any damages under any theory of law, including, without limitation, any special, consequential, incidental or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, even if advised of the possibility of such damages.

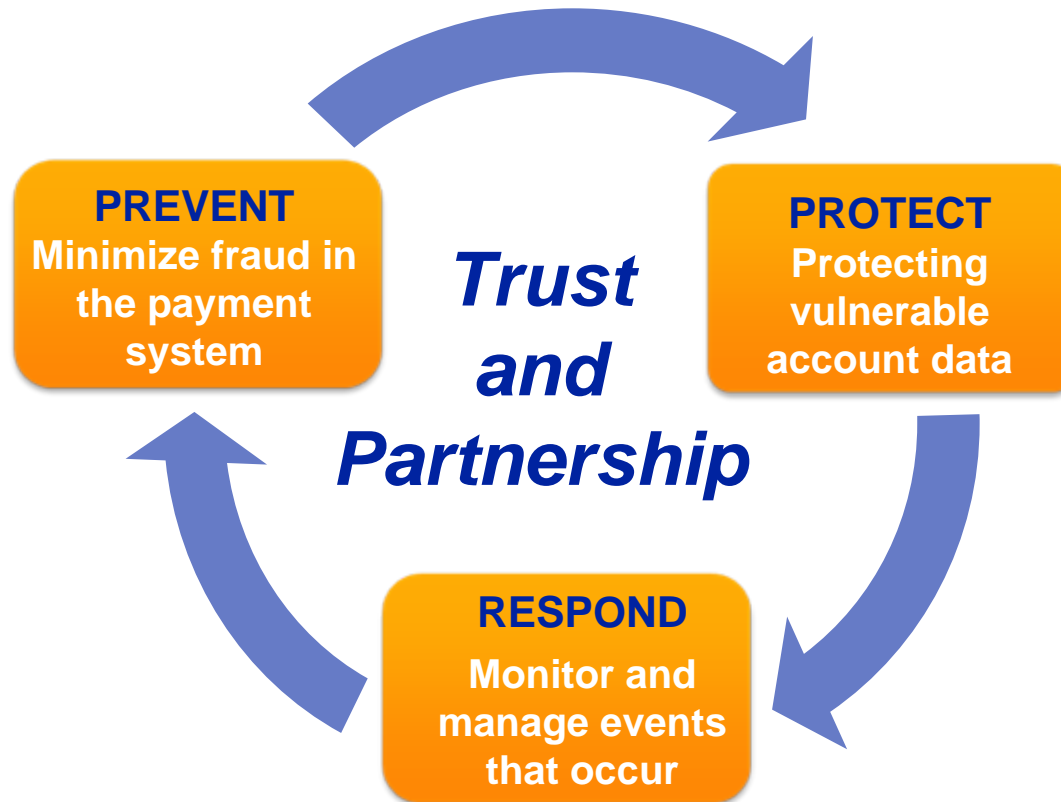
Please be advised that the information provided here may constitute material nonpublic information under U.S. federal securities laws and that purchasing or selling securities of Visa Inc. while being aware of material nonpublic information would constitute a violation of applicable U.S. federal securities laws.

Agenda



- Payments Systems Risk Strategy
- Authentication Vision and Direction
- Globally Aligned Focus

Maintaining and enhancing stakeholder trust in Visa as the most secure way to pay and be paid



Risk Strategic Overview



PREVENT

Minimize fraud in the payment system

- Advanced Authorization
- Visa Risk Manager
- EMV Chip Cards
- Authentication and Data Devaluation
- Verified by Visa/3d Secure

PROTECT

Protecting vulnerable account data

- PCI DSS / PA-DSS
- PIN Security / PED / TDES
- Data Elimination
- Data Field Encryption
- Card Manufacturer / Personalizer Security
- PCI Security Standards Council

RESPOND

Monitor and manage events that occur

- Rapid Compromise Response and Investigations
- Compromised Account Management System
- Compromise Recovery – GCAR, ADCR, DCRS
- Merchant Fraud/Chargeback Monitoring Programs
- Transaction Alerts



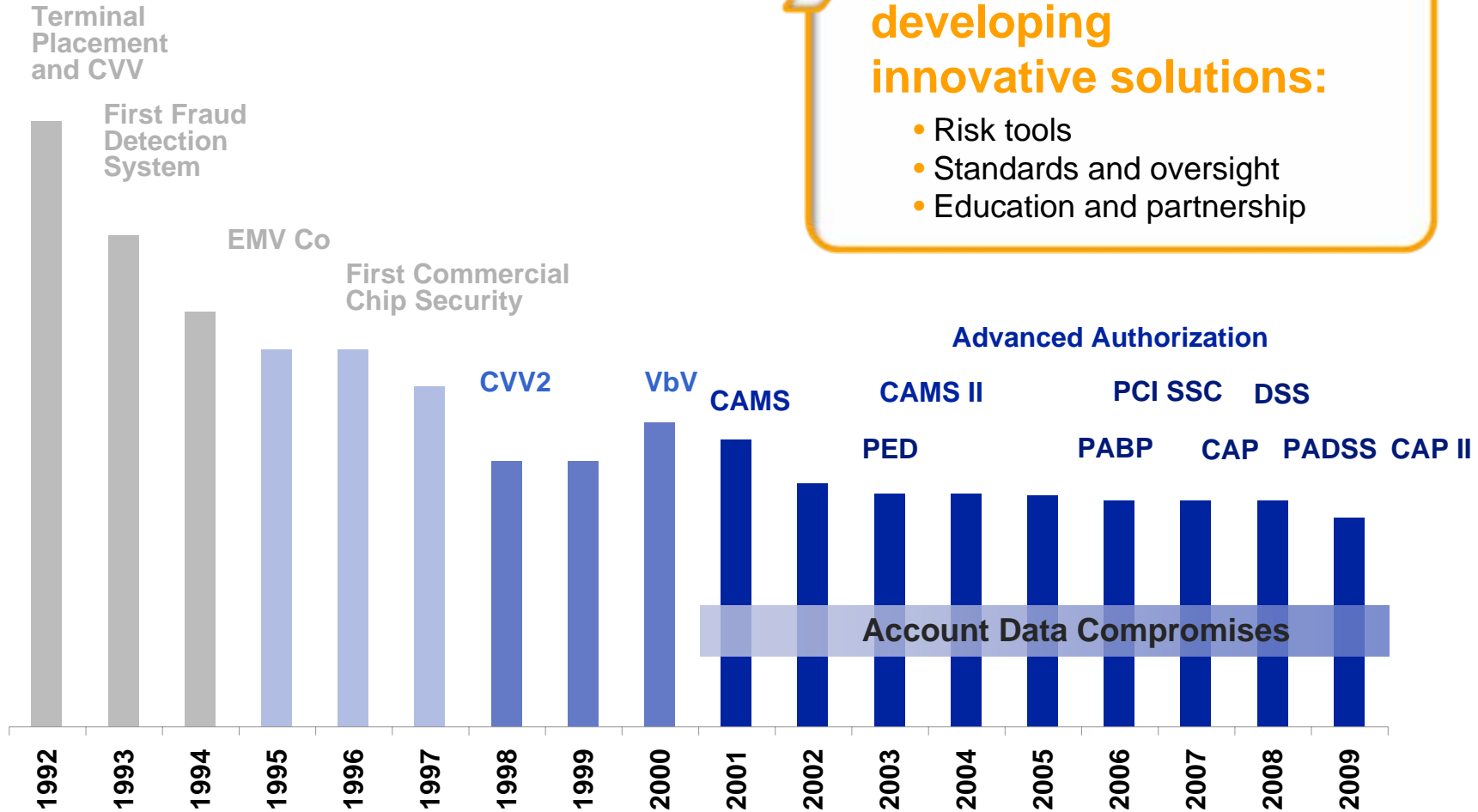
Partner with Clients and Stakeholders

- Partner with Law Enforcement and Industry Trade Groups
- Promote Security Awareness through Education and Training
- Educate Legislators and Regulators

Controlling Fraud Through Innovation



Global Fraud to Sales Rate



Visa has led in developing innovative solutions:

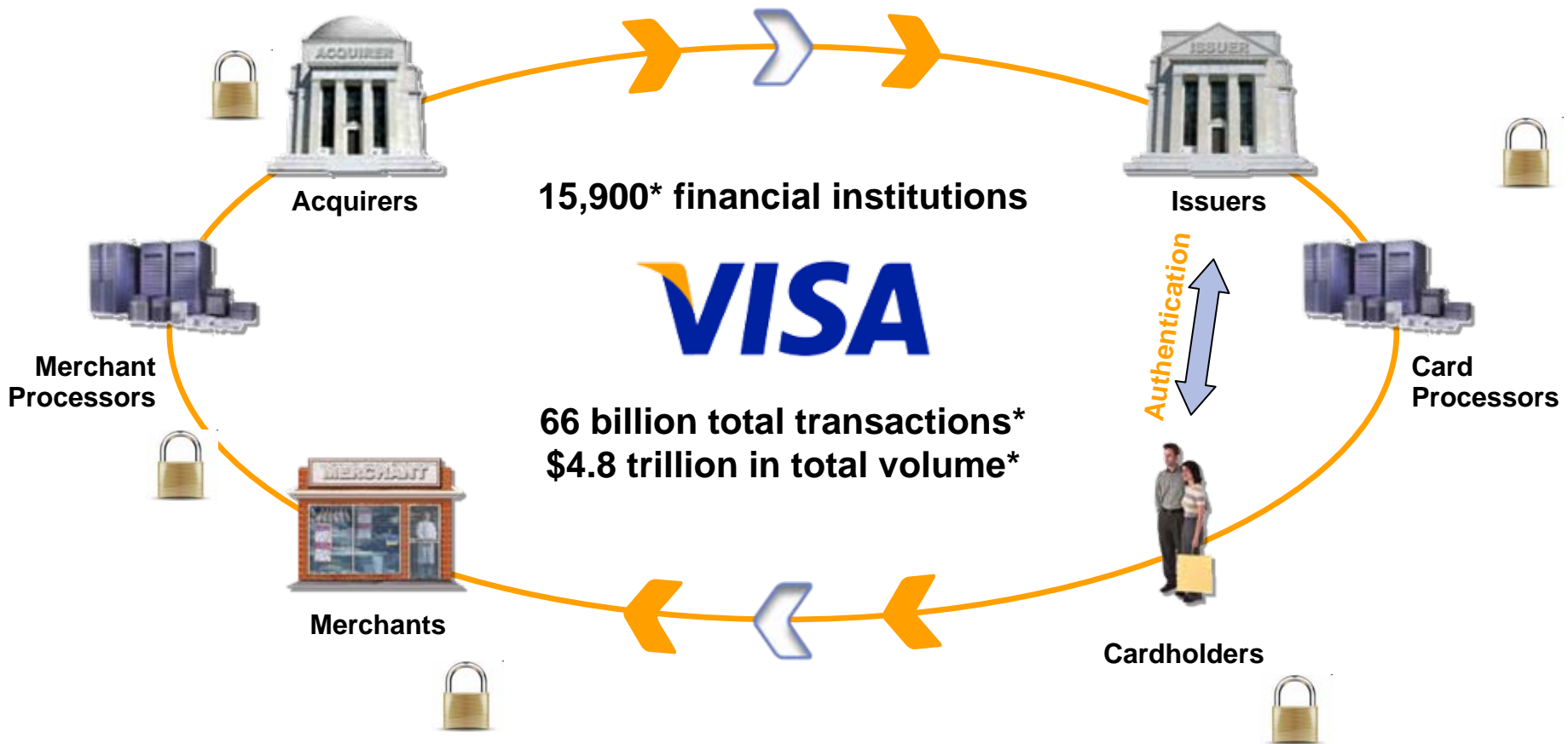
- Risk tools
- Standards and oversight
- Education and partnership

Source: Visa TC40 Fraud Reporting (as of March 2010)

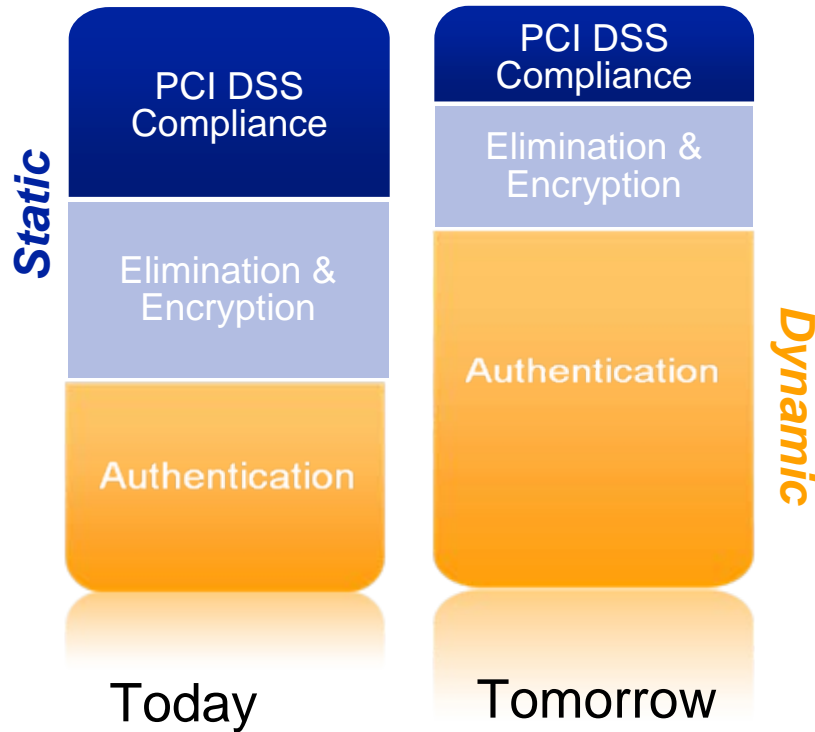
Global Payments Environment



Authentication data travels through multiple stakeholders



* Visa records, 31 March 2010



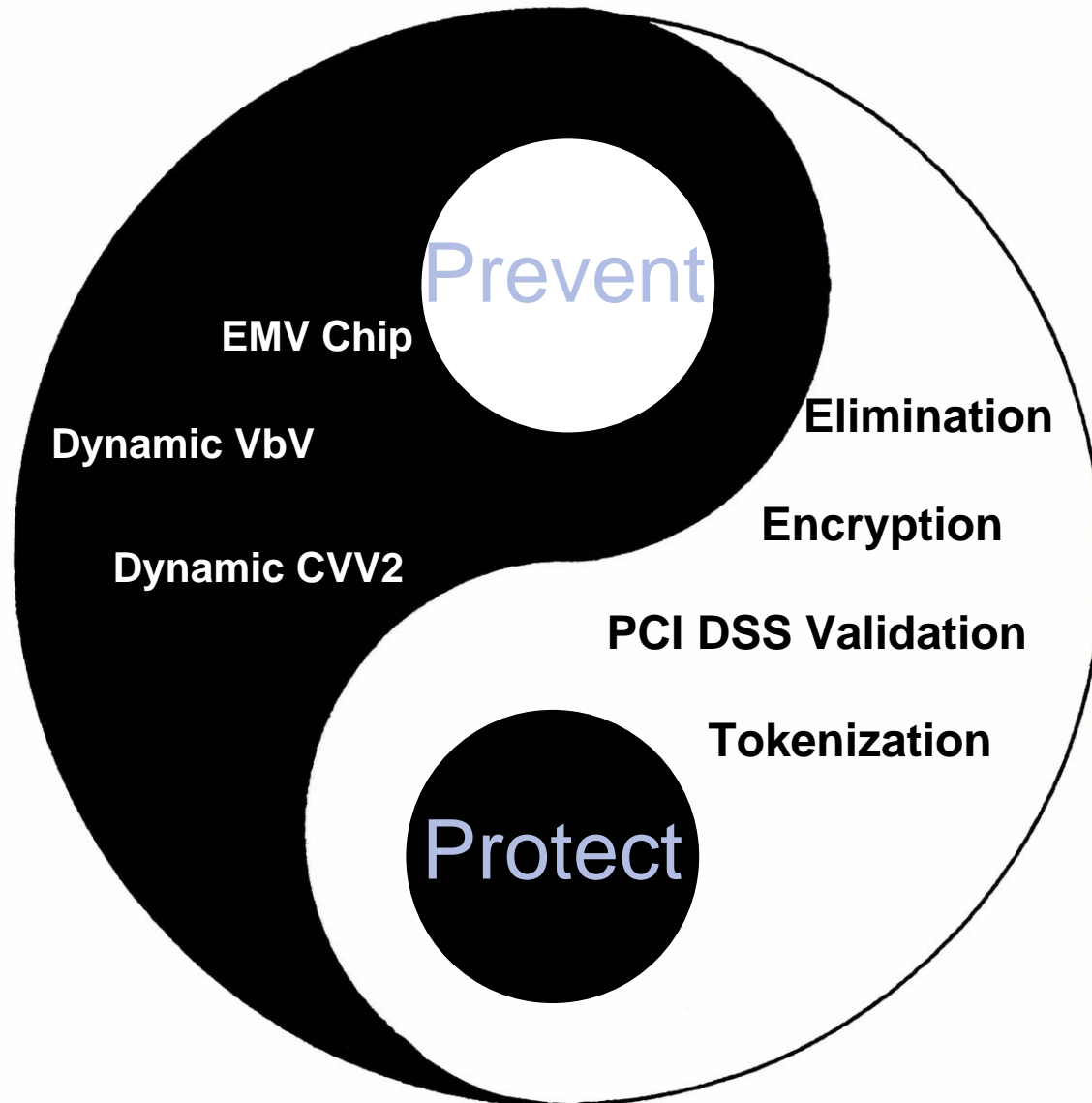
Prevent

- ■ **Devalue** transaction data with dynamic authentication
-

Protect

- ■ **Eliminate** static data
- ■ **Secure** static data

The Zen of Security



Payment Authentication Options



What you have!



Card



Display Card



Fob



Mobile



Tokens

Static / Dynamic

What you know!



Password



PIN



CVV2



Address Verification Service



Verified by Visa

Static / Dynamic

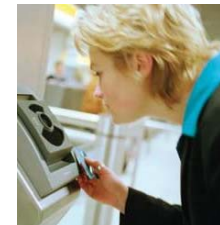
What you are!



Fingerprint



DNA ??



Iris

Unique

Dynamic Authentication - Authentication Technologies



Software OTP Token



DPA Reader



Number Grids/Lists



Display Card



SMS OTP



Hardware Tokens



Biometrics

VbV Dynamic Authentication Implementation Toolkit

Toolkit introduction

- Background
- Purpose & Audience

Common types of e-attacks

Verified by Visa

- How it works
- Drawbacks of Static Authentication

Dynamic authentication

- Benefits
- Authentication technologies

Authentication Technologies



Data Elimination

- 1** Eliminate commercial need for merchant to retain PAN
 - 2** Prohibit acquirers from requiring merchants to store PAN
 - 3** Educate stakeholders on Visa requirements and best practices
-

Encryption

- 1** Lead industry efforts to define a common standard
- 2** PCI DSS scope reduction if applicable
- 3** Provide support to early adopters and target merchant segments

- Replacement of PAN with a 'reference number'
 - Does not refer to a 'hardware token'
- PAN not necessary after the transaction
 - Reversals, hospitality / tipping, logs
 - Use token supplied by the acquirer instead
- Brings systems out of scope of PCI DSS
 - If they only have access to the 'token'
 - Tokenisation system must be secured

1. Dynamic Authentication:

Deploy EMV chip and dynamic CNP solutions

2. Eliminate Card Data:

Don't need it, don't store it

3. Secure Card Data:

PCI DSS compliance, Protect vulnerable data via encryption solutions,

4. Powerful Network Solutions:

Deploy back-office network-based security solutions like Visa AA and alerts

5. Innovation, Leadership & Collaboration:

Partnering to build trust and grow the payments industry



Questions

