Global Payment Risk Trends and Visa's Risk Strategy

Michael E. Smith
Head, Global Payment System Risk

China Payment Security Training & Workshop
28 February 2014, Beijing

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. You should consult with your legal counsel to determine what laws and regulations may apply to your 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. 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. 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.

Forward Looking Statements

These presentations contain forward-looking statements within the meaning of the U.S. Private Securities Litigation Reform Act of 1995. These statements can be identified by the terms “objective,” “goal,” “strategy,” “opportunities,” “continue," “can,” "will" and similar references to the future. Examples of such forward-looking statements include, but are not limited to, statements we make about our corporate strategy and product results, goals, plans and objectives. By their nature, forward-looking statements: (i) speak only as of the date they are made, (ii) are neither statements of historical fact nor guarantees of future performance and (iii) are subject to risks, uncertainties, assumptions and changes in circumstances that are difficult to predict or quantify. Therefore, actual results could differ materially and adversely from those forward-looking statements because of a variety of factors, including: the impact of new laws, regulations and marketplace barriers; developments in litigation or government enforcement; economic factors; industry developments; system developments; loss of organizational effectiveness or key employees; failure to effectively develop products and businesses; Visa Europe’s exercise of their put option, and the other factors discussed in our most recent Annual Report on Form 10-K filed with the U.S. Securities and Exchange Commission. You should not place undue reliance on such statements.

Visa's Vision

The world's best way to pay and be paid, for everyone, everywhere

Visa Brand Promise

Global Acceptance

Reliable

Convenient

Secure

Better Money

Visa Payments Landscape

Protecting the payment system is a strategic priority and a shared responsibility

Source: Figures are from 4Q13 FY operational performance data except number of financial institutions and ATMs.
Note: Figures are rounded, exclude Visa Europe and are as of 30 September 2013 unless otherwise noted.

1. As of 30 June 2013
2. Includes payments and cash transactions
3. As of 30 June 2013. As reported by client financial institutions and therefore may be subject to change; includes ATMs in the Visa Europe territory

Global Payment System Risk – Top Trends

1. Growing CNP Fraud Challenges

2. Increasing and Shifting Data Compromises

3. New Participants and Services Bring New Risks

Strengthening China's Payment Infrastructure

Through a multi-layered approach

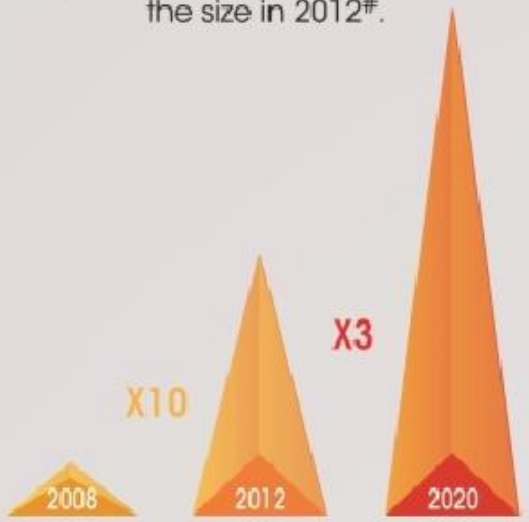
Vision: *The most trustworthy and secure way to pay and be paid, decisively taking smart risks to achieve business objectives*

Mission: *Build and enhance stakeholder trust in Visa as the most secure way to pay and be paid*

1. Growing CNP Fraud Challenges

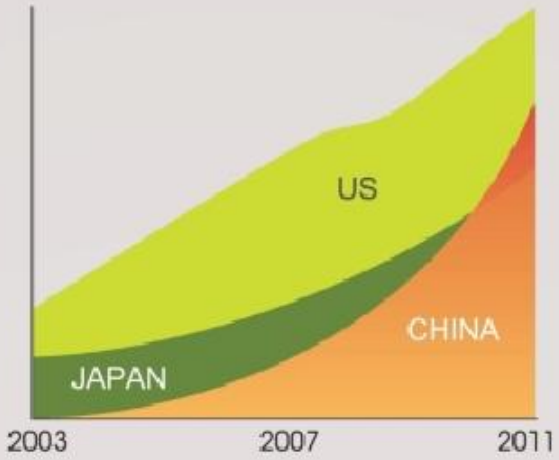
Increasing eCommerce activities in China

By 2020, the size of online shopping transactions in China will reach RMB 2.5 trillion, which is approximately 3 times of the size in 2012#.



2008-2020 Online Shopping Transaction Growth in China*

By 2015, China will exceed US and become the largest online shopping market in the world



2003-2011 Global Online Retail Market

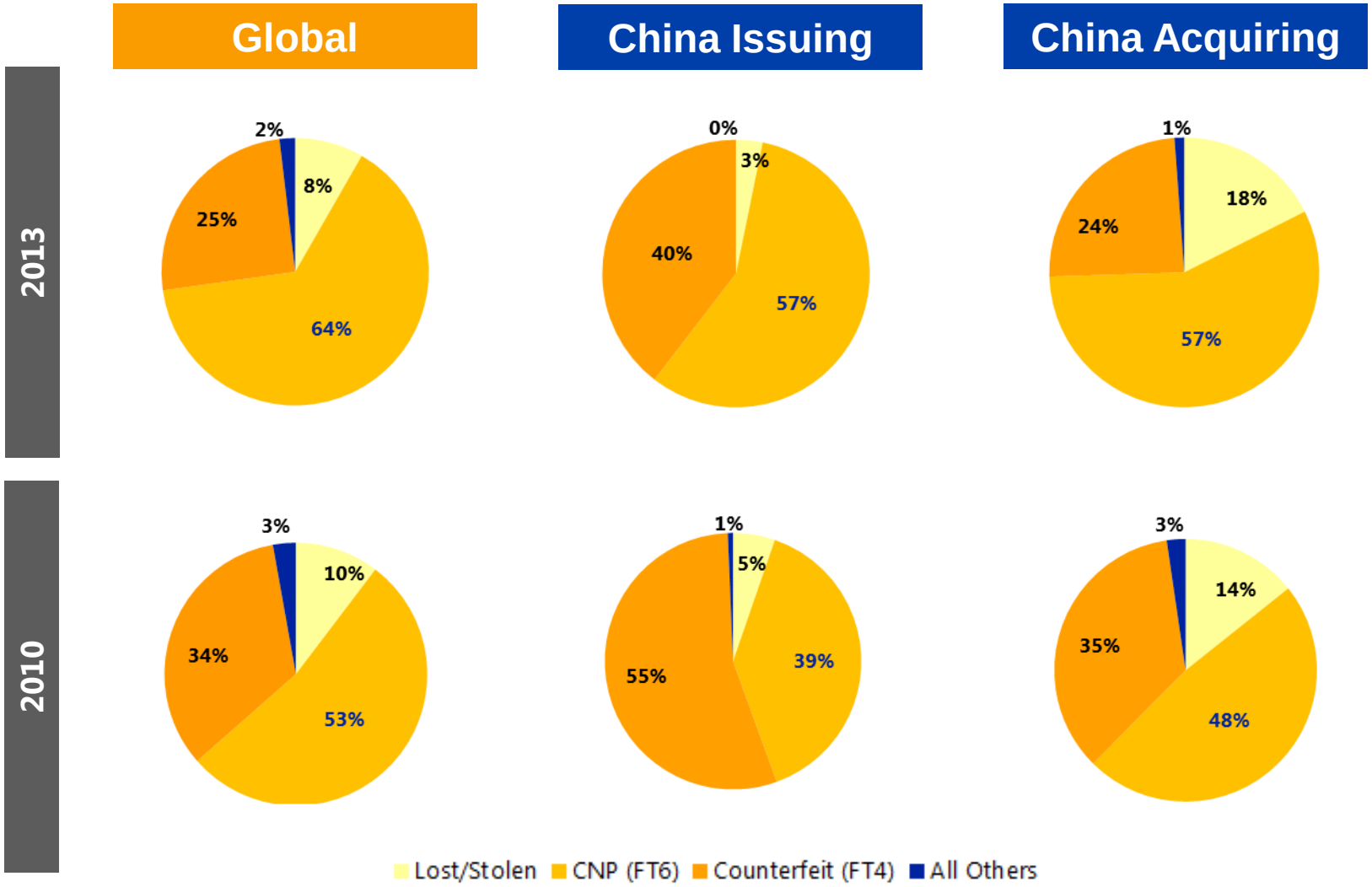
China's eCommerce penetration has already surpassed the US

In 2012, China's eCommerce trade sales was 6.3% of total retail amount, while US's was only 5%^

Source: China Internet Network Information Center (CNNIC) "2012 Online Shopping Market in China Research Report", March 2013.
iClick Interactive Asia Limited, "China eCommerce Analysis Report 2013"

1. Growing CNP Fraud Challenges

Global and China cross-border fraud trends



Source: VisaNet Data up to end 3Q2013.

1. Growing CNP Fraud Challenges

Implementing the strategy in China

Visa Advanced Authorization,

Visa Risk Manager

Verified by Visa

Visa Merchant Trace System

CyberSource

2. Increasing and Shifting Data Compromises

Fraud patterns evolve to take advantage of vulnerabilities

Fraudsters target the weakest link and can evolve quickly

2. Increasing and Shifting Data Compromises

Criminals have evolved to keep pace with the changing landscape

	1980	1990	2000	Current
Target	Cardholders	Small Merchants	Merchants / Agents	Merchants / Agents
Profile	Individuals	Team	Organized	International
Fraud Type	Lost & Stolen	Skimming	Data Compromise	Cross-border Data Compromise

2. Increasing and Shifting Data Compromises

However, data breach attack methods have remained relatively stable

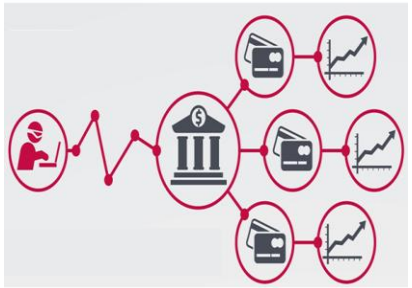
	2010	2011	2012	2013
1	Default credentials	Default credentials	Malware attack through insecure remote access service	Malware attack through insecure remote access service
2	Malware attack through insecure remote access service	Malware attack through insecure remote access service	Default credentials	Default credentials
3	SQL Injection	SQL Injection	Storage of unnecessary data	Social engineering attacks
4	Social engineering attacks	Limited or no event monitoring or logging	Limited or no event monitoring or logging	Physical device tampering
5	Physical device tampering	Social engineering attacks	SQL Injection	SQL Injection

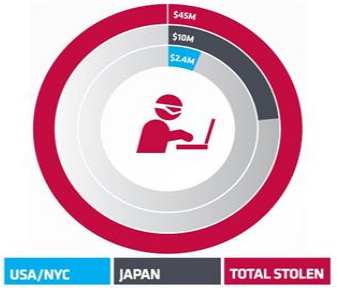
Source: 2010, 2011, 2012 and 2013 Verizon Data Breach Investigation Reports

2. Increasing and Shifting Data Compromises

Global ATM Cashouts

40,500+ Transactions, 27 Countries, $45M in loss





Phase 1

- **Card processor network intrusion**
- **Override of security protocols and elimination of withdrawal limit**

Phase 2

Distribution of 12 account numbers to "cashing crews" in 27 countries, who then encoded information on magnetic-stripe cards

Phase 3

- **Execution of the global cashout at over 5,000 ATMS worldwide**
- **The attack lasted 10 hours**

The Impact

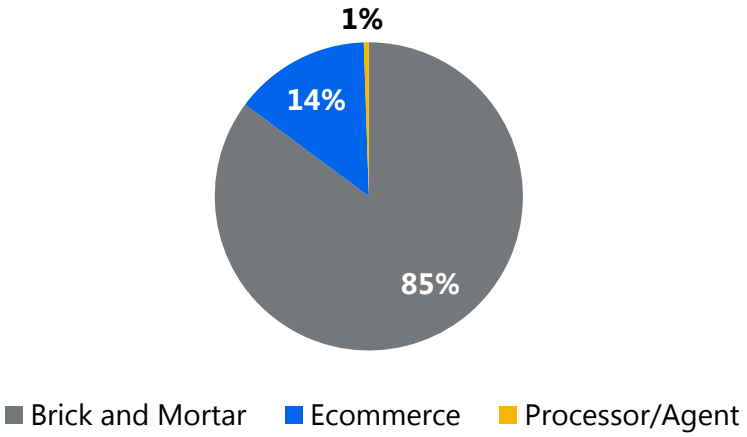
- **Thieves collected $10M in Japan alone, where some banks allow up to $10,000 from a single ATM transaction**
- **In New York City, thieves made 2,904 ATM withdrawals totaling $2.4M in just over 2 hours**

Source: U.S. Department of Justice press release, 9 May 2013; New York Daily News, 10 May 2013
:Infographic from The 41st Parameter. http://www.valuewalk.com/2013/05/atm-cyberattack-worldwide-the-45m-heist-infographic/

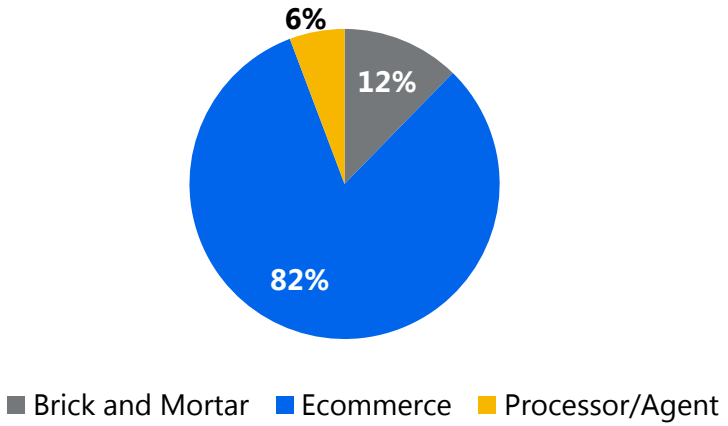
2. Increasing and Shifting Data Compromises

Problems are migrating to static data channels

North America
Data Breaches by Entity Type (2013)



Asia Pacific
Data Breaches by Entity Type (2013)

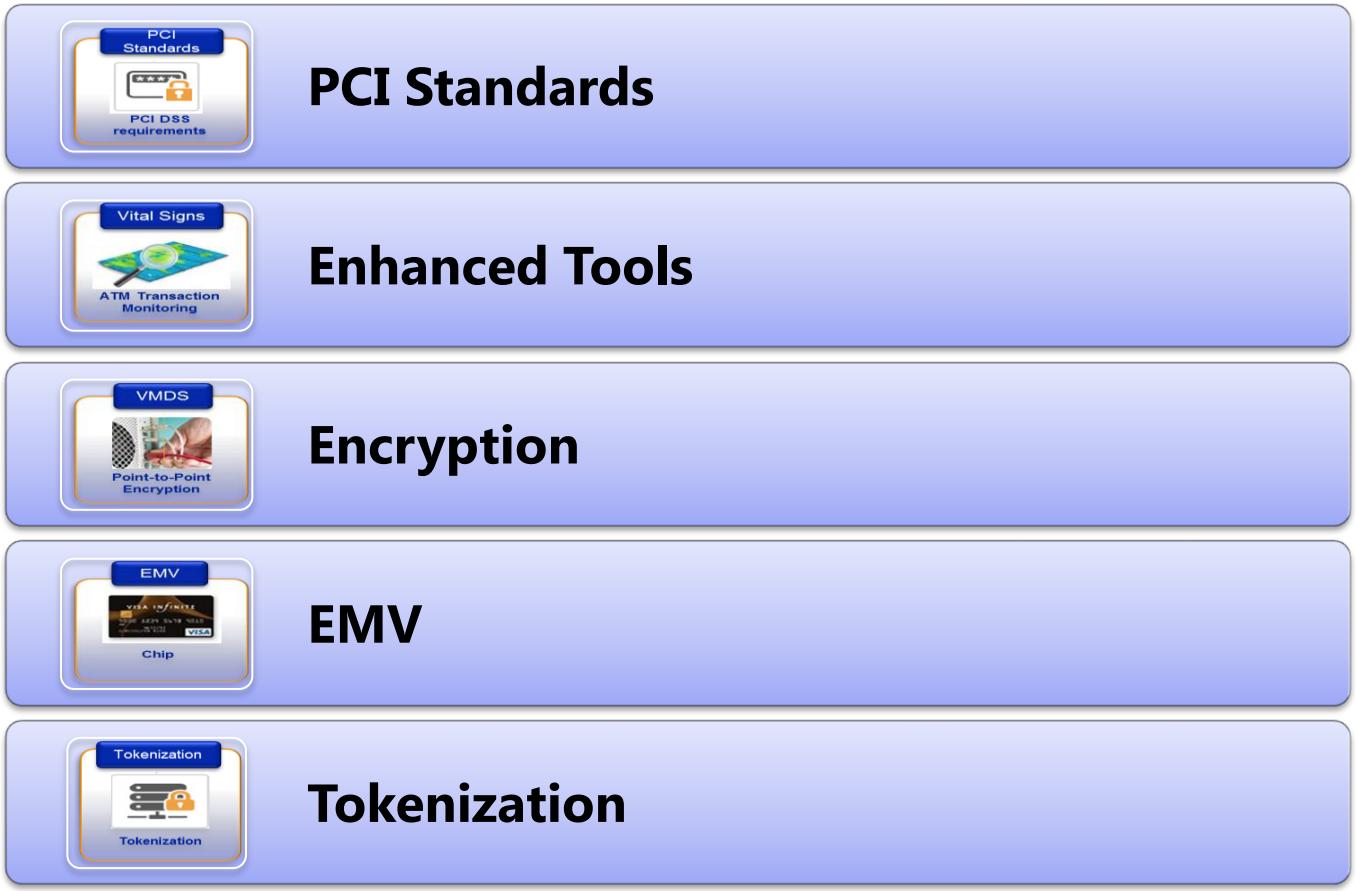


- Breaches in North America occur predominantly at brick and mortar entities.
- In Asia Pacific, where EMV adoption rates are higher, a majority of reported breaches occur at eCommerce entities.
- It takes a multi-layered approach including continued compliance with industry security standards, investments in technology to detect fraud in real-time and the elimination of sensitive data in the payment system through efforts like tokenization.

Source: Visa Compromised Account Management System

2. Increasing and Shifting Data Compromises

Implementing the strategy in China



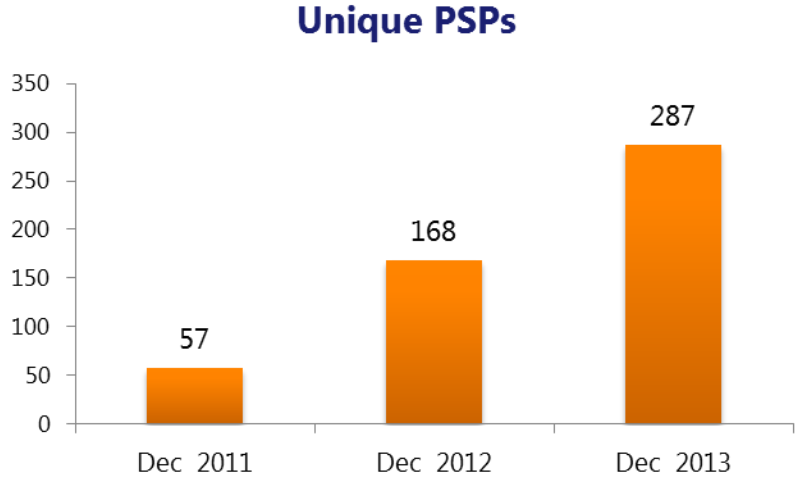
3. New Participants and Services Bring New Risks

Growth in third parties is introducing complexity and risk

VI Agents have grown to 3,852 as of Dec 2013 (up 22% Y-O-Y)

Source: Monthly MXR4134 Series of Agent and ISO Relationship Reports for Visa Inc. and MXR4423_Curr Report, Data is as of December 31, 2013.

VI PSPs have grown to 287 as of Dec 2013 (up 70% Y-O-Y)



Source: Monthly MXR4134 Series of Agent and ISO Relationship Reports for Visa Inc. Data is as of December 31, 2013.

- Increase visibility of payment participants in payment ecosystem.
- Mitigate data security and brand risk posed by third parties by creating transparency through Visa's Registry of Service Providers which broadcast agents' compliance with Visa requirements.
- Help client banks enhance Agents' risk controls through Visa's awareness initiatives - training, best practices and threats intelligence.

3. New Participants and Services Bring New Risks

Challenges and controls

Challenges

THIRD PARTY BOARDING

- Limited or no visibility into activities to accurately understand risk exposures

MONITORING

- Inadequate monitoring leading to compliance violations

MANAGEMENT OVERSIGHT

- Lack of engagement by management can lead to compliance lapses that expose institutions to a range of risks

---

Controls

- Establish strong Know-Your-Third Party procedures
- Establish a risk assessment process
- Ensure strong executive management supervision and/or board oversight of compliance programs

- Track consumer complaints
- Exercise audit rights
- Request annual compliance certifications
- Develop a response plan and effective escalation mechanism if there are red flags

- Continuously drive education and awareness

3. New Participants and Services Bring New Risks

Implementing the Strategy in China

Registry of Service Providers

Visa Ready Partner Program

Global Brand Protection Program

Qualified Service Provider Program

Visa's Qualified Service Provider (QSP) Program

Launched in August 2013

Facilitates collaboration with industry and builds a more secure and trusted payment network in China

Helps PSPs in China grow their business and drive stronger performance

Provides essential resources

(e.g., best practices on data protection, fraud prevention and internet security)

Acts as an additional oversight layer to acquirer due diligence

Security is a Shared Responsibility

Thank you