XXVII Bank Security Conference

CELAES 2012

"MITIGATING RISKS AND CONVERTING THEM INTO BUSINESS OPPORTUNITIES"

FIBA

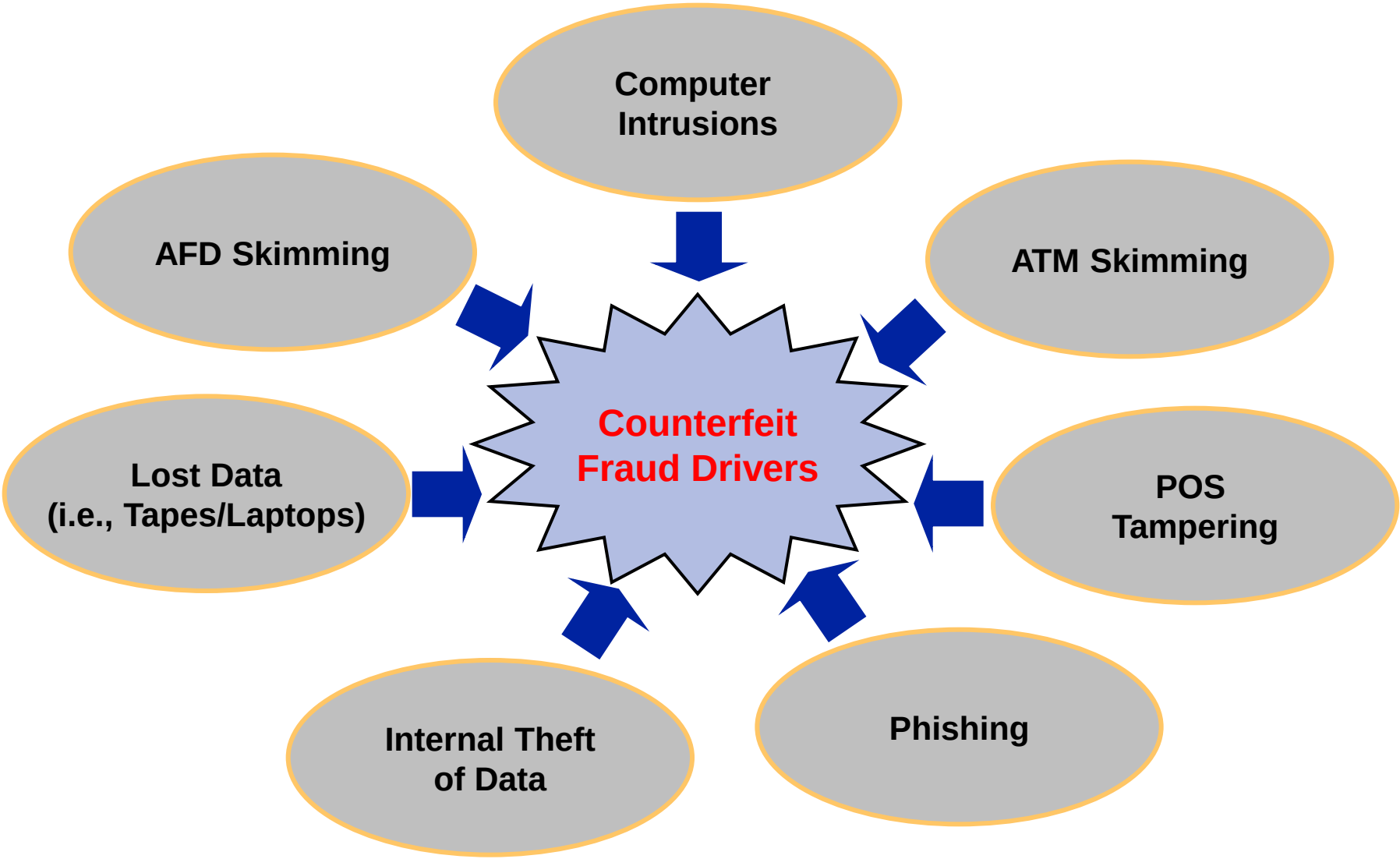
Organized by:

FELABAN

FEDERACION LATINOAMERICANA DE BANCOS

Data Compromise Landscape

Data Compromise Landscape



2012: The Security Challenge

Fraudsters have evolved their business models and migrated between channels, products and geographies

Criminals continue to adapt and challenge the system

- The number of compromise incidents involving cardholder information has grown globally
- Stakeholder costs are increasing
- Security tops consumer concerns
- Regulatory attention and intervention on the rise

Data Thieves are Relentless

Reduce stored card data	Criminals steal data in transit
Drive PCI among large merchants	Criminals targeting small merchants and processors
Implement EMV chip	Fraud migrates to card-not-present and non EMV market

Data Breach Trends – Verizon Report

- 92% of the incidents were discovered by a third party (CPPs)
- 85% of breaches took weeks or more to discover
- 96% of attacks were not highly difficult
- 97% of breaches were avoidable through simple or immediate controls
- In 76% of incidents a third party servicer contributed to the breach

Source: Verizon Business 2012 Data Breach Security Report http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012-press_en_xg.pdf

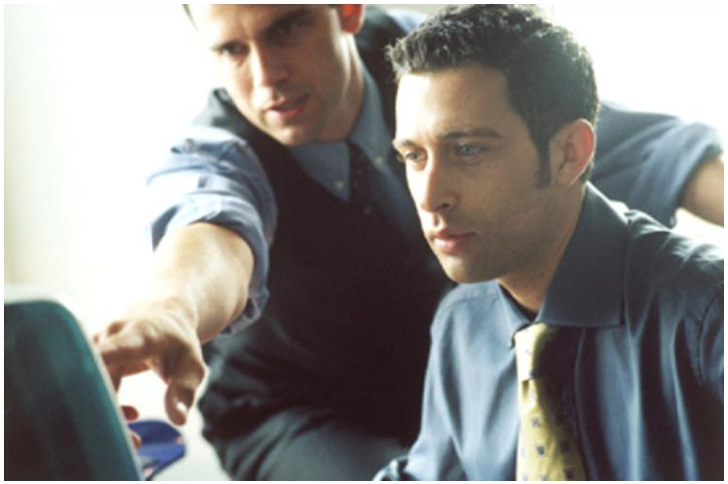
Data Breaches Reported to Visa – 2011

- Number of compromise incidents reported in 2011 increased by 15% from incidents reported in 2010
  - *67% originated from the U.S.*
  - *U.S. reported events up 27% compared to the same period in 2010*
- 97% of U.S. events occurred at small merchants
  - *91% of U.S. incidents are brick & mortar merchants*
  - *81% involve small restaurant merchants*
  - *Restaurant franchises continue to be the leading merchant category impacted for U.S.*

Source: Visa global CAMS reporting 2011

How the Hackers are getting in….

- Remote access
- Default or weak credentials used by 3rd parties
- SQL injections
- No firewall to protect POS systems from inbound and outbound traffic



Malware

Malicious software used to steal data in real-time

- Key loggers
- Packet sniffers
- Memory scrappers

Malware sophistication

- Captures data, creates file and removes duplicate accounts
- Encrypts stolen data into export file
- Built in exfiltration mechanisms to send data to hacker
- Deletes exfiltrated files
- Anti-forensic tools

Basics of Incident Management

Preparation

- Policies and procedures in the event of a compromise

Detection

- Gather evidence

Containment

- Remove compromised system from the network

Eradication

- Rebuild infected systems

Recovery

- Validate the systems have been restored

Follow-up / Lessons learned