Transaction Network Services

Security

Tiffany Trent-Abram
VP, Global Product Management

November 6th, 2015

Bringing Global Credibility and History

TNS Specializes in
Managed Network Connectivity and
Value-Added Communications Services

for

- ✓ Payments
- ✓ Telco
- ✓ Financial Services

Securely Delivering 8 Billion Enterprise Transactions Daily

Global Scope and Reach

- Clients in 65+ countries
- 1000+ employees
- Headquartered in Reston, Virginia
- Offices in 17 countries

Founded in 1990 ♦ Privately held with backing from Siris Capital Group

TNS Partners / Customers

Transaction Network Services

Supplying Security Expertise

TNS Provides Security Expertise Your Business Can Rely On

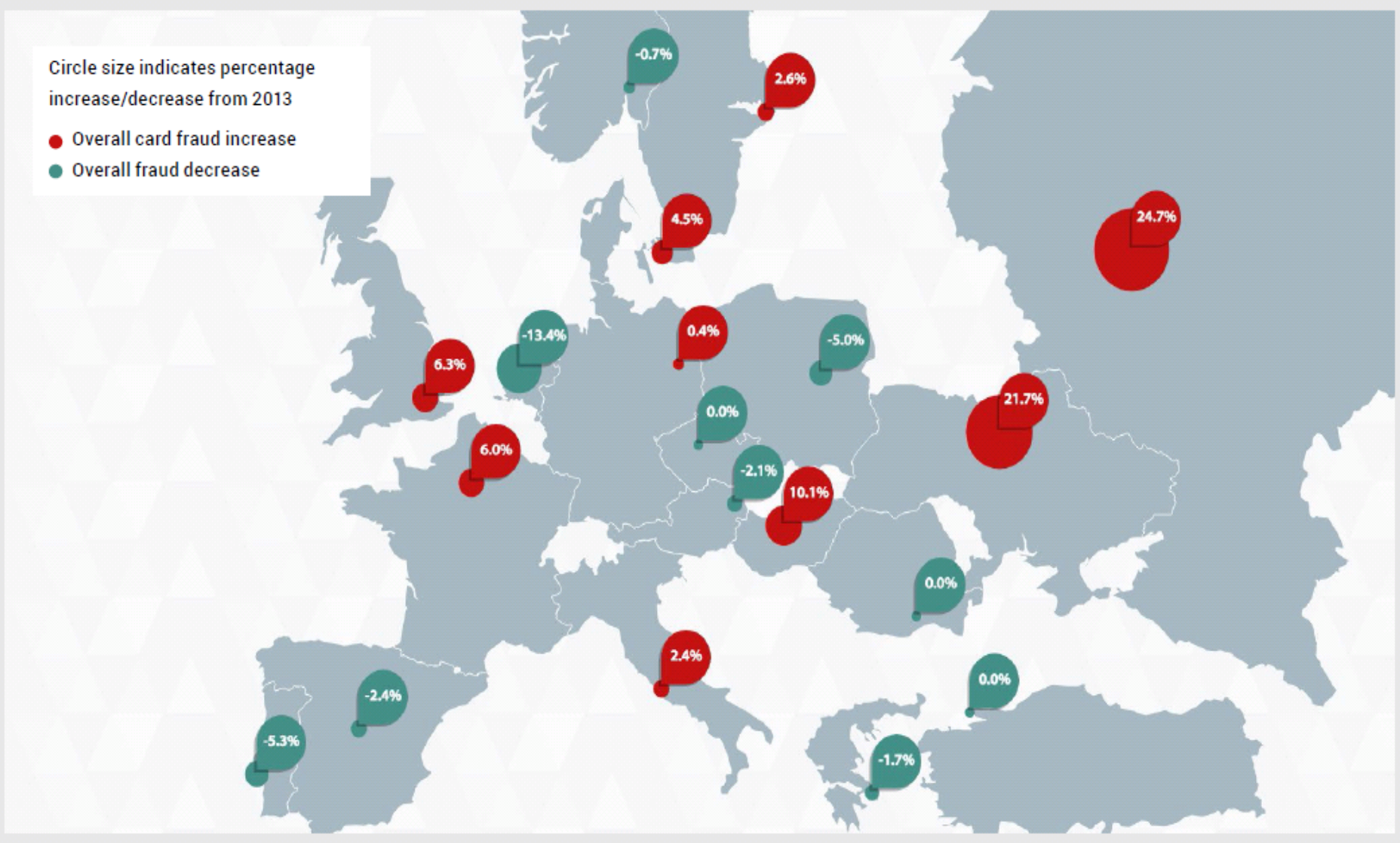
- Real-time security monitoring of in-flight data to detect and resolve problems earlier
- Products developed to secure transactions from the point of capture to processing
- Team of resources dedicated to monitoring and protecting the network

PCI Security Standards Council™
PARTICIPATING ORGANIZATION

- ✓ Highly secure network across all connectivity and device types
- ✓ PCI Level 1 compliant solutions
- ✓ PCI Security Standards Organization participating member
- ✓ Dedicated SSL and IP connectivity
- ✓ Distributed Denial of Service (DDoS) protection
- ✓ POS terminal authentication
- ✓ Single-source access to best-in-class encryption and tokenization services

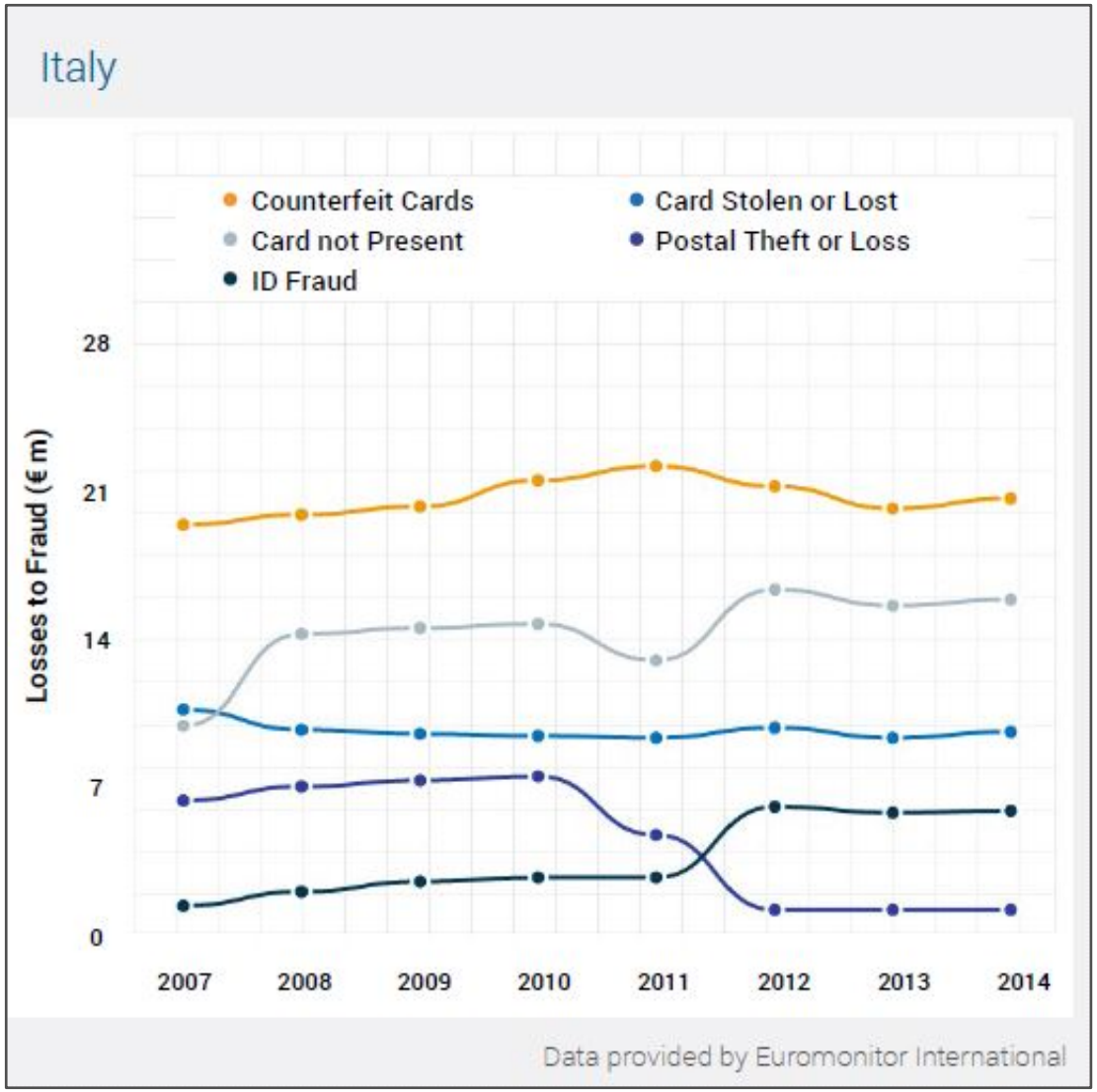
Security Trends

European Fraud Changes 2013 - 2014



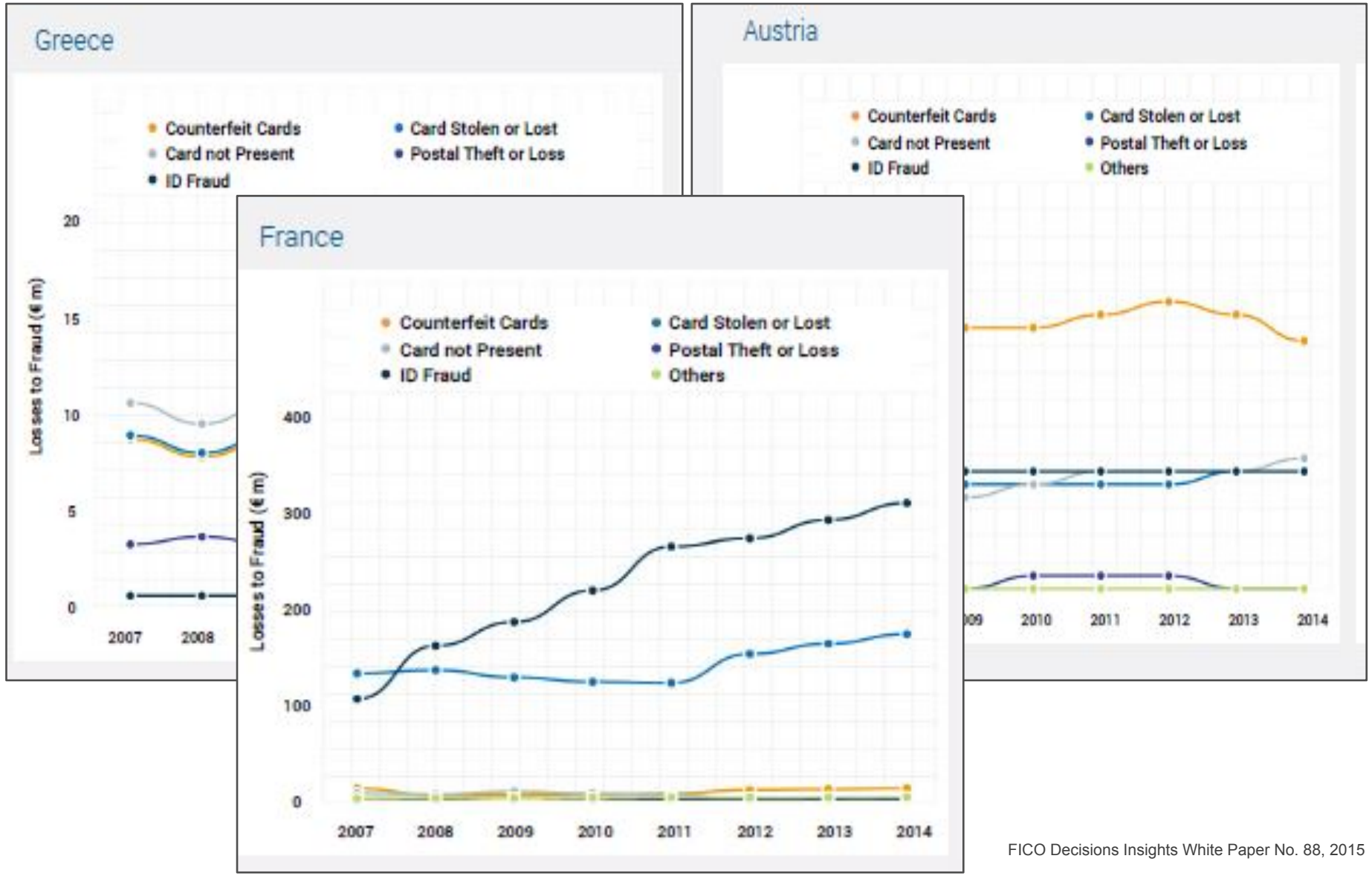
FICO Decisions Insights White Paper No. 88, Figure 1, 2015

Italian Market Fraud Trends



FICO Decisions Insights White Paper No. 88, 2015

Western Europe Fraud Trends



FICO Decisions Insights White Paper No. 88, 2015

The Meaning & Costs of PCI Compliance

What is PCI-DSS?

The **Payment Card Industry Data Security Standards** (PCI-DSS) are regulations that were created to ensure safe handling of sensitive information and to protect cardholder data.

PCI Intent: Protect Cardholder data from inappropriate disclosure

PCI – Who does it affect?

- Anyone who transmits, processes or stores payment card data
- Examples…
  - Merchants
    - Online
    - In-store
  - Service Providers
    - Payment Gateways
    - IT Service Providers
    - Web Hosting Providers
    - Teleco's
  - Emerging Payment Solutions
    - Mobile Wallets

The core of PCI-DSS is a group of principles and accompanying requirements, around which the specific elements of the DSS are organized:

- Maintain a Secure Network
  - Requirement 1: Install and maintain a firewall configuration to protect cardholder data
  - Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect Cardholder Data
  - Requirement 3: Protect stored cardholder data
  - Requirement 4: Encrypt transmission of cardholder data across open, public networks
- Maintain a Vulnerability Management Program
  - Requirement 5: Use and regularly update anti-virus software
  - Requirement 6: Develop and maintain secure systems and applications
- Implement Strong Access Control Measures
  - Requirement 7: Restrict access to cardholder data by business need-to-know
  - Requirement 8: Assign a unique ID to each person with computer access
  - Requirement 9: Restrict physical access to cardholder data
- Regularly Monitor and Test Networks
  - Requirement 10: Track and monitor all access to network resources and cardholder data
  - Requirement 11: Regularly test security systems and processes
- Maintain an Information Security Policy
  - Requirement 12: Maintain a policy that addresses information security

Associated Costs

- You have invested a LOT of time and effort
  - Preparation takes a lot of time
  - You read the PCI-DSS only to realize you need a team of people to understand it
  - You convinced your developers to read the PCI-DSS
  - You hired a Qualified Security Assessor
- Goes beyond your internal environment – 3rd party connections are included in scope
- **Average costs of PCI compliance is estimated at 1.7M Euros annually**
- And fines are now assessed for non-compliance

PCI Enforcement Plan

Risk Management | Data Security 5 June 2014

Visa Introduces Enhanced PCI DSS Enforcement Plan

AP, Canada, CEMEA, LAC, U.S. | *Acquirers, Issuers, Processors, Merchants, Agents*

The vast majority of merchants, VisaNet processors and third party agents have already validated Payment Card

PCI DSS Enforcement Plan

Visa encourages clients to work with their noncompliant or overdue Level 1 and Level 2 merchants and service providers immediately to obtain either validation documentation or a remediation plan.

Visa clients whose merchants or service providers have not fulfilled their annual PCI DSS compliance validation requirement or qualified for the Visa Technology Innovation Program (TIP)[1] may be subject to the following actions, as specified in the *Visa International Operating Regulations*:

- Assessment of PCI DSS noncompliance fines (ID#: 0008193)
- Implementation of risk reduction measures (ID#s: 0003687, 0005057 and 0025869)

Fines will be assessed beginning **1 January 2015** for noncompliant or overdue level 1 and level 2 merchants and service providers without a remediation plan and will appear on the 25 January 2015 Global Member Billing Statement. For merchants, the fines will apply to the primary acquirer with the most transactions for the merchant.

Entities with overdue PCI DSS validation or that have never validated PCI DSS compliance must submit a remediation plan to their Visa clients. Visa clients are responsible for reviewing and accepting the remediation plan. If the Visa client accepts the remediation plan, it must provide Visa with the Qualified Security Assessor (QSA) company name (if applicable) and the planned validation date to suspend fine assessments. Visa reserves the right to review and reject a remediation plan.

The Cost of Data Breaches Are Rising

- The average cost paid for each lost or stolen record containing sensitive and confidential information increased 6 percent, jumping from $145 in 2014 to $154 in 2015

Cost of Data Breaches Rising Globally, Says '2015 Cost of a Data Breach Study: Global Analysis' May 2015

- Global Payments in 2014 – 1.5 million card numbers and other information stolen in a security breach. Estimated direct cost –

  $291,000,000.00

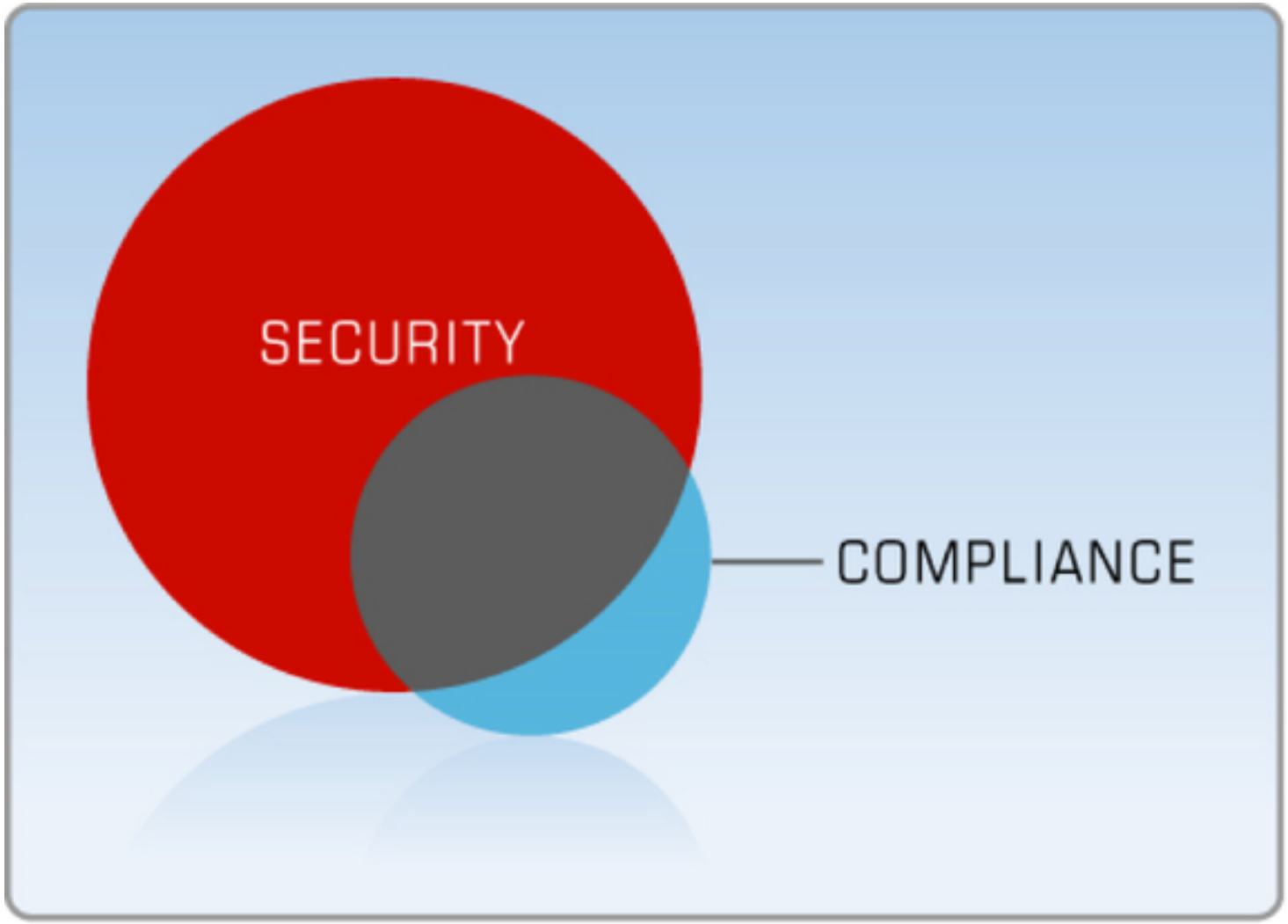
- Zappos! – 24 million records including partial credit card numbers illegally accessed. Estimated direct cost-

  $46,560,000,000.00

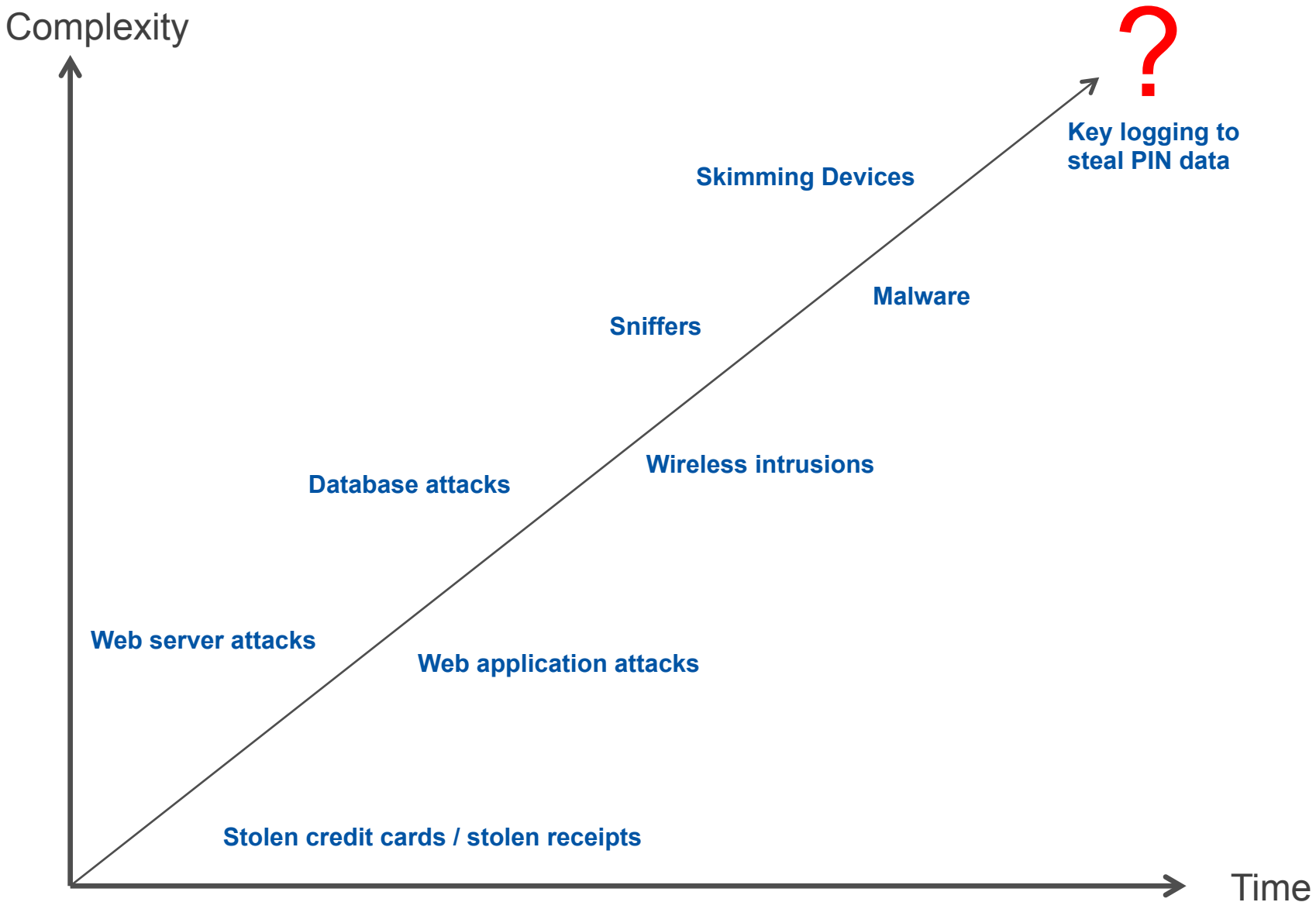
- You don't want your company on this list!

Beyond PCI Compliance

Compliance ≠ Secure

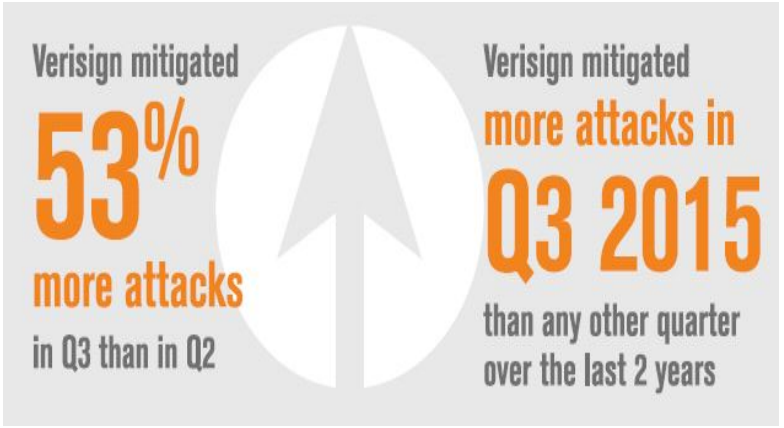


Evolution of Attacks



After you pass PCI compliance audit, what could go wrong?

- Human Error / Employee Breaches
  - Every company is one configuration change away from a security breach
- Management Commitment to Security
  - Need buy-in for security protection from the board and executive level
- Third Party Vendor Access Security Controls
  - 63% of the 450 data breaches studied in the Trustwave Global Security Report were “linked to a third-party component of IT System Administrators”



Verisign Q3, 2015 DDoS Attack Trends, 2015

- Sniffers
  - Cardholder data in flight
- DDoS
  - Distributed Denial of Service (DDoS) – attempt to make an online service unavailable by overwhelming it with traffic from multiple sources
  - This is growing at an alarming rate
- Hackers
  - Finding new ways to break into networks

Impact of EMV Adoption in the US

- The Impact of EMV Adoption in the US
- The US EMV liability shift in October 2015 for Point Of Sale, followed by ATM and unmanned petrol terminals in 2017. The US has seen an ***unprecedented increase in attacks on ATMs*** through skimming on both bank-owned and non-bank estate ATMs. This implies that criminals are making the most of mag stripe technology fraud before it becomes far more difficult to get away with it in the US.
- In the UK, FICO has identified a ***25% increase in cross-border fraud on debit cards in 2014,*** compared to 2013. More importantly, it identified that 47% of the fraudulent transactions were taking place in the US — a pattern that, again, seems related to the delay in EMV adoption in the US

FICO Decisions Insights White Paper No. 88, 2015

Distributed Denial of Service (DDoS)

Transaction Network Services

Attacks:

71% of data center operators reported DDoS attacks this year, up dramatically from **45% in 2012**

Verisign Q3, 2014 DDoS Attack Trends, 2014

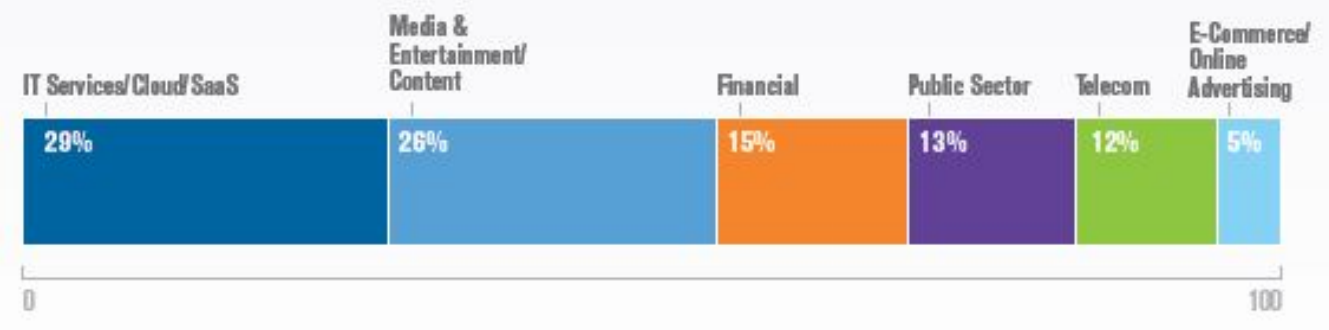
Consequences:

81% of data center operators reported operational expenses due to DDoS attacks

27% reported revenue loss due to DDoS attacks

35% reported customer churn due to DDoS attacks

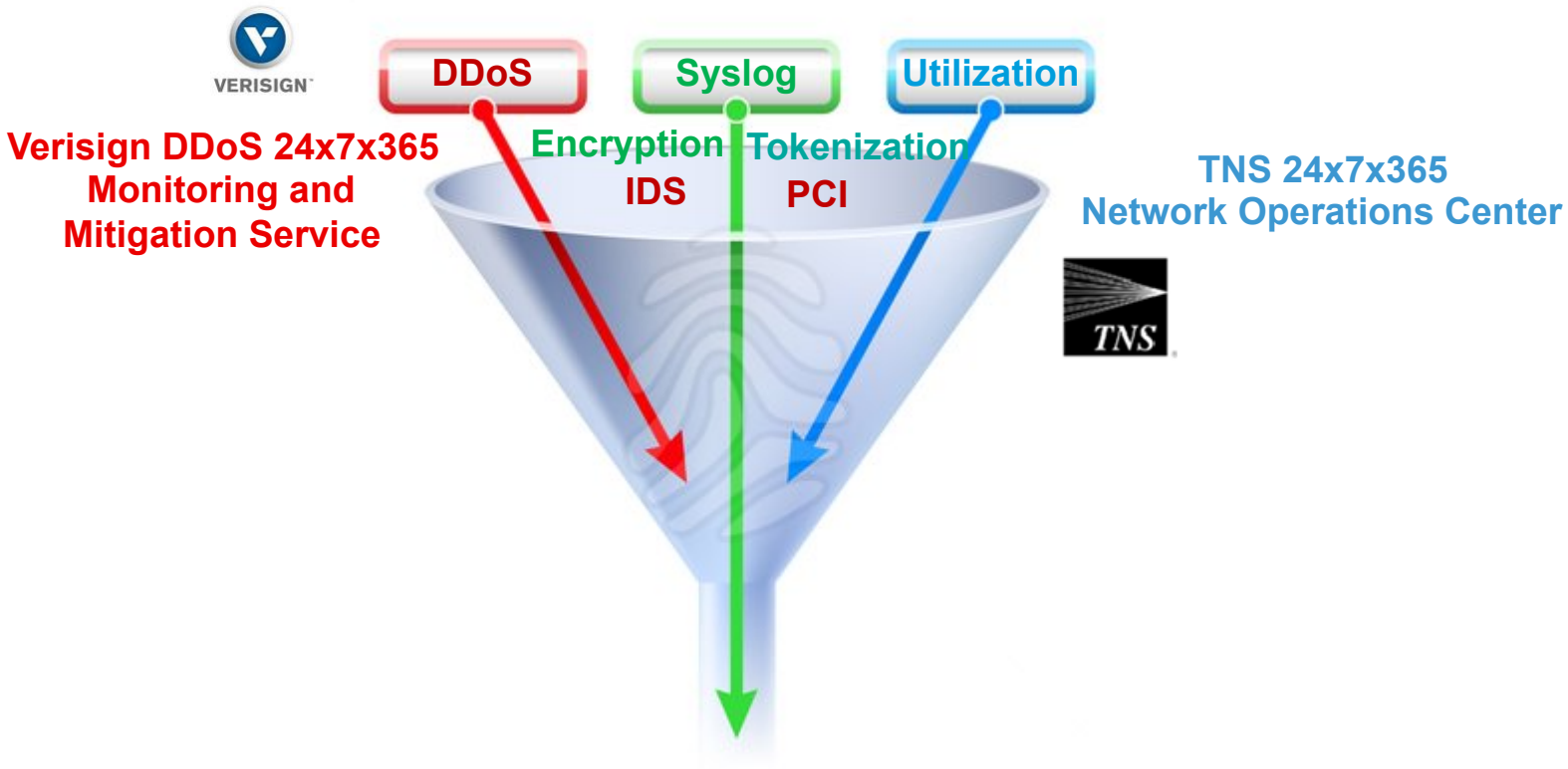
Verisign Q3, 2014 DDoS Attack Trends, 2014



Verisign Q3, 2015 DDoS Attack Trends, 2015

Service and Technologies Used To Safeguard Customer Data

- Security Monitoring
  - Intrusion Detection Systems (IDS)
    - Alien Vault
    - Dell, Siemens, IBM
  - DDoS Monitoring and Mitigation Service
    - Verisign, Cloud Flare, Sitelock, etc
  - Change Auditing
    - File Integrity Monitoring (FIM)
    - Router Configuration Monitoring
      - Tripwire, Trustwave, etc
- Encryption and Tokenization Capabilities
- Vulnerability Management
  - Vulnerability Scanners
  - Web Application Scanners
    - Alien Vault, Tripwire, etc



TNS Global Security

Security Operations Center

(conducts Incident Management on escalated attacks post correlation)

Summary

TNS Helps You Increase Revenue and Reduce Risk - While Saving Time and Money

Global, Secure, Reliable, Flexible and Cost-Effective Solutions

- ✓ Global experience with security and compliance
- ✓ Secure, highly reliable connectivity and value-added services for the payments industry, supporting numerous device types
- ✓ Link to 400+ payments companies globally - with a single connection
- ✓ Continual technology improvements that benefit you - without expensive in-house capital projects

For More Information Call

Giovanni Mistè

Via Pergolesi 2/A, Milano, 20126, Italy

+39 02.481.226.3

gimiste@tnsi.com

www.tnsi.com