



IBM India

DSCI

Best Practices in Data Security & Privacy

"This document contains information that is proprietary and confidential to IBM Daksh Business Process Services Pvt. Limited. No part of it may be circulated, quoted, or reproduced for distribution without prior written approval from IBM Daksh Business Process Services Pvt. Limited."

© 2007 IBM Corporation

- **Your Name and your Organization**
- **Your Contact Details (Phone Number, e-mail id)**
- **Top 10 Data Security & Privacy Challenges faced in the Banking Industry**
- **For each challenge, please list whether this continues to be a challenge or whether you have a solution for it**
- **Please pass it to the DSCI staff**




Jesse Woodson James*
(September 5, 1847 – April 3, 1882)

An [American outlaw](#), [gang leader](#), [bank](#) and [train robber](#), and [murderer](#) from the state of [Missouri](#) and the most famous member of the [James-Younger Gang](#). Already a celebrity when he was alive, he became a legendary figure of the [Wild West](#) after his death.

Source*: Wikipedia

- Phishing
- Pharming
- SQL Injection
- Advance Fee Frauds
- Hacking
- DOS
- Website Defacement
- Man-in-the middle
- Credit Card Frauds
- Wire Transfer frauds
- ...

Online bank fraud up, but total card fraud falls for first time

by Ian Grant 
Wednesday 10 March 2010 08:55

Online banking fraud losses rose by 14% to £59.7m in 2009, but overall card fraud dropped 28% to £440.3m - the first decrease since 2006 - according to figures from bankers.

UK Payments, which represents payment settlement firms, said fraud on debit and credit cards fell by more than a quarter in 2009 to £440.3m, and counterfeit card fraud (skimming and cloning) fell by over half. Cheque fraud fell 29% from £41.9m to £29.8m, it said in its report for 2009.

Bankers attributed the decline to a combination of the move to chip and Pin, greater use of sophisticated fraud detection tools by banks and retailers, and the work of the Dedicated Cheque and Plastic Crime Unit (DCPCU), the banking-sponsored special police unit.

Bankers said the rise in online banking losses was due to criminals using more sophisticated methods to target online banking customers. This included malware that attacked vulnerable PCs. There were also more than 51,000 phishing incidents in 2009, up 16% on 2008.

Banks measured phone banking fraud losses for the first time, which totalled £12.1m. Customers were duped using cold calling or fake e-mails into disclosing security details, which were then used to defraud them.

Cheque fraud losses decreased from £41.9m in 2008 to £29.8m in 2009, helped by a 29% fall in the use of cheques. UK Payments said the UK domestic cheque guarantee card scheme would close on 30 June 2011.

David Cooper, chairman of the fraud control steering group, said card fraud remained the main focus of criminal activity. "We will continue working with law enforcement, retailers, consumers and the Home Office to tackle fraud head-on," he said.

Bankers said chip and Pin had helped cut fraud on lost and stolen cards to its lowest level for two decades and counterfeit card fraud losses were the lowest since 1999. Losses at UK retailers have fallen by two-thirds since 2004; lost and stolen card fraud was down 58% between 2004 and 2009; and mail non-receipt fraud had fallen by 91% since 2004, they said.

The introduction of MasterCard SecureCode and Verified by Visa authentication systems helped cut card-not-present fraud by 19% - the first decrease ever.



Online Banking Frauds (2009) Increase by 14% to £60m

- Phishing
- Pharming
- Phone banking (social engineering)

Credit Card Frauds (2009) Dropped by 28% to £440m

- Chip & Pin
- Fraud Detection tools
- Dedicated Cheque & Plastic Crime Unit, Banking sponsored special Police cell

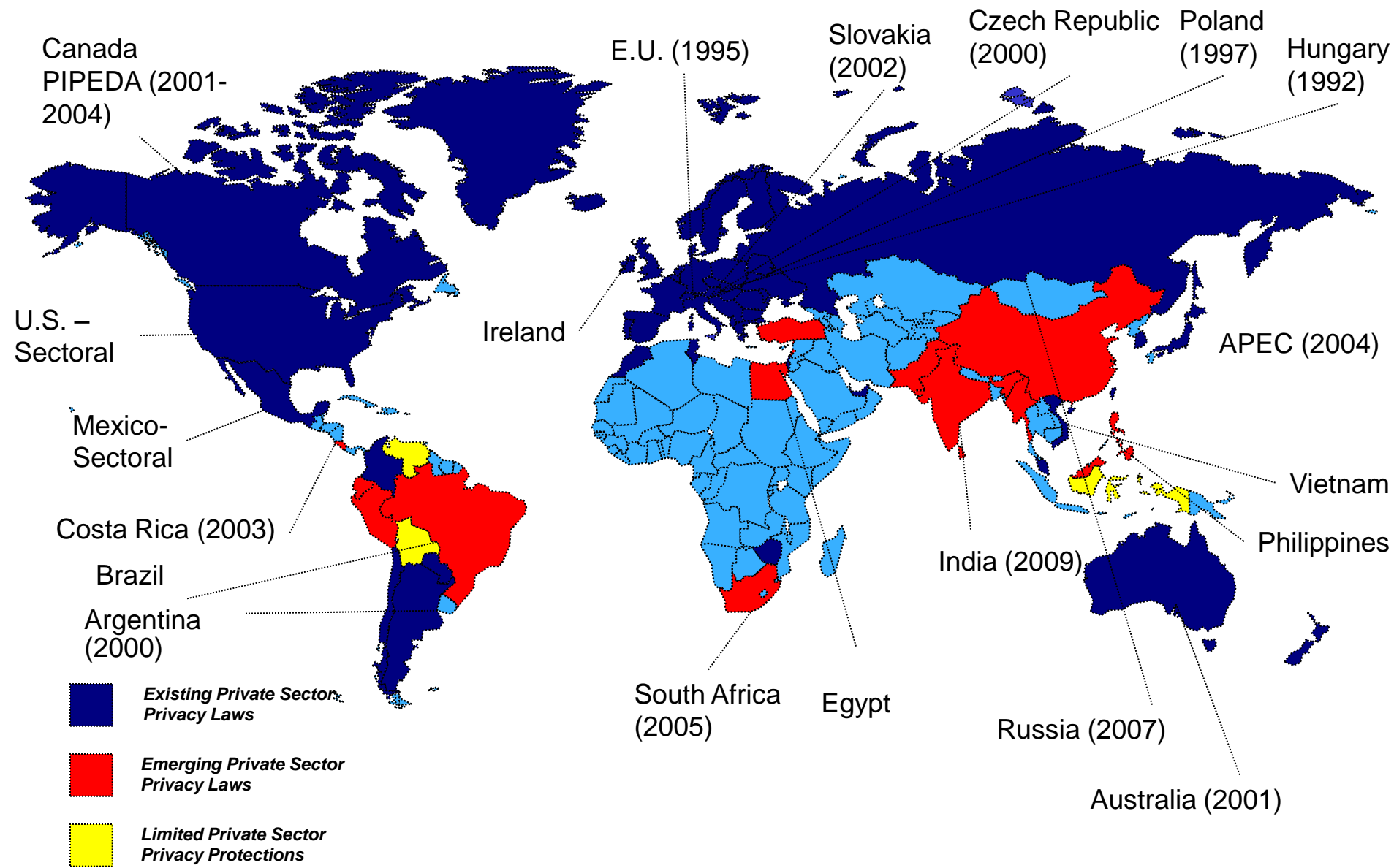
Source: Internet - Banking Frauds 2010

- **Customer Awareness**
- **Secure Application Development**
- **Secure Network & IT infrastructure**
- **Handling sensitive personal information – electronic & paper based**
- **Encryption of data**
- **IT Governance – Auditing, Change Management,**
- **Employee verification**
- **Fraud detection & prevention – analytics**
- **Incident Management**
- **Outsourcing challenges**
- **24*7 availability and BCM**
- **Regulatory Compliance**

- **The Federal Information Security Management Act of 2002 ("FISMA", [44 U.S.C. 3541](#), *et seq.*) is a [United States federal law](#) enacted in 2002 as Title III of the [E-Government Act of 2002](#) (Pub.L. 107-347, 116 Stat. 2899).**
- **FISMA has brought attention within the federal government to [cybersecurity](#) and explicitly emphasized a "risk-based policy for cost-effective security".[\[1\]](#)**
- **FISMA assigns specific responsibilities to [federal agencies](#), the [National Institute of Standards and Technology](#) (NIST) and the [Office of Management and Budget](#) (OMB) in order to strengthen information system security. In particular, FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce information technology security risks to an acceptable level.[\[2\]](#)**
- **FISMA requires agency program officials, chief information officers, and inspectors general (IGs) to conduct annual reviews of the agency's information security program and report the results to [Office of Management and Budget](#) (OMB).**
- **OMB uses this data to assist in its oversight responsibilities and to prepare this annual report to Congress on agency compliance with the act.[\[2\]](#) In FY 2008, federal agencies spent \$6.2 billion securing the government's total information technology investment of approximately \$68 billion or about 9.2 percent of the total information technology portfolio.[\[3\]](#)**
- **According to FISMA, the term *information security* means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality and availability.**

Source: Wikipedia

Complex Global Privacy Landscape



**Body Corporates are liable to the extent of “Unlimited Liability”
for failure to implement ‘reasonable security practices’ to
protect sensitive personal information**

- **Rich experience in Information Security, IT Transformation, Telecom Switching Infrastructure, Intelligent Networking and Broadband Infrastructure.**
- **Security Practices with Data Security Council of India (DSCI).**
- **Manages a program for defining data security and privacy practices towards establishing a self regulation mechanism focused on data protection.**
- **Engaged in DSCI outreach program at national and international platforms for establishing collaboration with different legal and regulatory bodies, data protection authorities, global clients and outsource service providers of all categories including small and medium players.**
- **Prior to joining DSCI, was working with Global Consulting Practice of Tata Consultancy Services (TCS) as a Consultant, Information Risk Management. Executed different security consulting engagements for different clients across globe and in different industry domains. Managed 'Application & Network Security Team'**
- **Worked with a public sector telecom service provider in India, where got an exposure to telecom infrastructure, intelligent networking and Internet backbone infrastructure.**



IBM India

DSCI

Best Practices in Data Security & Privacy

"This document contains information that is proprietary and confidential to IBM Daksh Business Process Services Pvt. Limited. No part of it may be circulated, quoted, or reproduced for distribution without prior written approval from IBM Daksh Business Process Services Pvt. Limited."

© 2007 IBM Corporation