

# Three Hats: Customer, Provider, Funder - Outsourcing and Financial Institutions Seminar

7 July 2009

Data Security  
Marc Dautlich



# Data Security in Outsourcing - True or False



- Impregnable information security is virtually impossible

True/False

- Many security incidents are avoidable

True/False

- Compliance risk can be outsourced

True/False

# Data Security Outsourcing - *" Before, During and After"*



- Providing supplier with usable information about the pre-outsourcing security environment *"Before"*
- Identifying a supplier with adequate capabilities *"Before"*
- Creating and agreeing incentives for maintaining/improving security environment post-transition *"During"*
- Monitoring supplier's performance, adjusting incentives/enforcing remedies and managing exit *"After"*

# Legal Context - A Dual Regime?



## **FSA Regime**

FSA Principles:

2 – *“conduct business with due skill, care and diligence”*

3 – *“take reasonable care to organise and control affairs responsibly and effectively, with adequate risk management systems”*

SYSC 6.1.1R *“procedures sufficient to ensure compliance ... with obligations under regulatory system and for countering risk that firm used to further financial crime”*

Treating Customers Fairly initiative

Guidance e.g. “Data Security in Financial Services” April 2008

## **ICO Regime**

DPA 1998 7<sup>th</sup> principle: *“technical and organisational measures ... to prevent unauthorised processing ... and accidental loss”*

Guidance e.g. security breach notification

# Legal Context (continued) - FSA vs. ICO Powers: Comparison



FSA	ICO
Formal investigation	Request for assessment
Public Censure	Information and enforcement notices
Financial penalties	Financial penalties (2010?)
Vary an authorised person's permission or cancel it	Data breach notification (voluntary)
	Good practice assessment (voluntary)

# Legal Context (continued) - FSA vs. ICO Powers: Comparison



FSA	ICO
Formal investigation	Request for assessment
Public Censure	Information and enforcement notices
Financial penalties	Financial penalties (2010?)
Vary an authorised person's permission or cancel it	Data breach notification (voluntary)
	Good practice assessment (voluntary)

# Legal Context (continued) - FSA vs. ICO Powers: Comparison



FSA	ICO
Formal investigation	Request for assessment
Public Censure	Information and enforcement notices
Financial penalties	Financial penalties (2010?)
Vary an authorised person's permission or cancel it	Data breach notification (voluntary)
	Good practice assessment (voluntary)

# Legal Context (continued) - FSA vs. ICO Powers: Comparison



FSA	ICO
Formal investigation	Request for assessment
Public Censure	Information and enforcement notices
Financial penalties	Financial penalties (2010?)
Vary an authorised person's permission or cancel it	Data breach notification (voluntary)
	Good practice assessment (voluntary)

# Legal Context (continued) - Conclusion



- Left hand vs. right hand
  - Co-operation protocol between FSA and ICO
- Mind the gap
  - Regulatory guidance to bridge gap between principles-based regulation and practical security solutions

# Outsourcing to Third Party Suppliers - FSA Data Security Guidance, April 2008



## Before

- “*Over-reliance on contract*”
  - Pre-contract planning
    - assessing supplier’s competence (“*due diligence*”)
    - assessing economics of good information security (“*business case*”)
  - Setting appropriate remedies and liability regime
    - “last man standing” is not the answer

# Outsourcing to Third Party Suppliers - FSA Data Security Guidance (continued)



## During

- “*Insufficient attention to staff vetting*”

→ Due diligence or negotiation needs to reveal answers to questions such as:

- how are third party staff vetted?
- when and who: access to customer data?

→ Exercising governance and audit rights in-flight during transition and delivery

- a question of execution and judgment

# Data Security - Outsourcing Contract Provisions



## During (continued)

- Core obligation provisions
  - e.g. preservation of data integrity/prevention of data loss or corruption
- “Accountable individual” provisions
- Breach notification obligations
- Remedies:
  - restoration of corrupted data
  - an aside on “loss”
  - indemnities
    - unauthorised access to Supplier infrastructure or Customer service environment
    - hacking
    - fraud

# Conclusion and Questions

OLSWANG

- What happened to “*After*”?
- Datonomy: [www.datonomy.blogspot.com](http://www.datonomy.blogspot.com)



# Three Hats: Customer, Provider, Funder - Outsourcing and Financial Institutions Seminar

7 July 2009

Data Security  
Marc Dautlich



For more information  
please contact:

**Marc Dautlich**

+44 (0) 20 7067 3142

[marc.dautlich@olswang.com](mailto:marc.dautlich@olswang.com)