SIDLEY AUSTIN LLP

SIDLEY

BEIJING BRUSSELS CHICAGO DALLAS FRANKFURT GENEVA HONG KONG LONDON LOS ANGELES NEW YORK PALO ALTO SAN FRANCISCO SHANGHAI SINGAPORE SYDNEY TOKYO WASHINGTON, D.C.

Data Protection for the Financial Services Sector

John Casanova and William Long

15 October 2010

Agenda

- Introduction
- Data Protection in Financial Services Sector
- General Concepts under the Data Protection Directive
- Data Security, Outsourcing and Data Breaches
- Processing for Compliance and Risk Management
- Enforcement
- Comments/Questions

Data Protection in Financial Services

Issues which create unique data protection challenges in the Financial Services Sector include:

- Subject to multiple supervisory regimes – FSA, ICO, DPA, Payment Schemes, EU Member State laws and US and other foreign Regulators (e.g. SEC)
- Global nature of the industry – global flows of data, complex outsourcing arrangements involving off-shoring and cloud computing
- Bank secrecy, customer confidentiality obligations and payment card industry data security standards (PCIDSS)
- Dealing with compliance and risk management through AML customer due diligence, carrying out credit checks, use of whistle-blowing hotlines, employee monitoring and recording of customer calls

EU and UK Legal and Regulatory Framework

- Key Legislation:
  - European Union Data Protection Directive (95/46/EC) implemented in UK by Data Protection Act 1998 (DPA)
  - ePrivacy Directive (2002/58/EC) with new ePrivacy Directive to be implemented in June 2011
  - UK's FSA rulebook – systems and controls requirements
  - Section 18 of UK's Computer Misuse Act 1990 – creates offence of unauthorised access to computer material
  - English common law aspects such as Bank Secrecy – see Tournier v National Provincial and Union Bank of England
  - Payment Card Industry Data Security Standards (PCI DSS)
  - EU Data Protection Directive to be reformed – likely to include a principle of accountability

UK Supervisory Framework

FSA

- Financial Services Authority (FSA) – wide jurisdiction, regulates activities of authorised firms and the use of customer data
- Firms' responsibilities in this area are defined in FSA's Principles for Businesses and Systems and Controls Sourcebook (SYSC)
- Principle 2 - firm must conduct its business with due skill, care and diligence
- Principle 3 - firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems
- FSA Rule SYSC 3.2.6R - 'a firm must take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the regulatory system and for countering the risk that the firm might be used to further financial crime'

UK Supervisory Framework

ICO

- Information Commissioner's Office (ICO) – responsible for ensuring firms comply with the Data Protection Act (DPA)
- ICO has provided detailed guidance on relevant areas such as outsourcing, disclosure of data, data transfers from the EEA, subject access requests, etc.
- Various offences can be committed under the DPA including failure to notify the ICO where required, unauthorised obtaining or disclosure of personal data and failure to comply with any enforcement notice
- In addition a data controller can face a civil action from a data subject who suffers damage or distress as a result of non-compliance with the DPA
- New monetary penalty powers since April 2010 of up to £500,000 for serious contravention likely to cause substantial damage or distress

Recent Security Breaches

- Catalogue of recent security breaches involving customer data
  - 2007 US data breach potentially exposed 46 million credit card accounts
  - 2008 mobile operator lost device with 17 million German customer records
  - 2009 hackers stole more than 130 million credit and debit card numbers from US acquirer
- Recent UK FSA fines have been significant
  - 2007 UK Building Society fined £980,000 for lapses in security where laptop stolen
  - 2008 UK Life Insurance Group fined over £1.2 million for loss by fraudsters
  - 2009 UK Insurance Group fined over £3.2 million for security breach

New monetary penalty powers for ICO

- From April 6, 2010 the ICO can impose penalties of up to £500,000 for serious contravention of the DPA's eight principles
- ICO will take pragmatic and proportionate approach
- There are a number of procedural steps before a penalty can be imposed, including ability to make representations
- In imposing the penalty ICO will consider:
  - Severity of data breach
  - Likelihood of substantial damage and distress
  - Whether breach was deliberate or reckless
  - What reasonable steps were taken to prevent breaches
  - Organisation's financial resources, sector and size
- ICO statutory guidance – deterrence and elimination of financial gain or other benefits as a result of breach

General Concepts under Data Protection Directive

The Directive governs the ***processing*** by ***data controllers*** of ***personal data*** relating to ***data subjects***

- Processing – all encompassing term which covers collection, analysis, storage, archiving and deletion
- Data Controller – person who determines the purpose and manner of processing personal data
- Data Processor – person who processes personal data on behalf of the data controller
- Personal Data – data which can identify a living individual (e.g. personal details such as name, address, contact details, etc.)
- Data Subjects – individuals whose data is processed
- Recent guidance by EU's Article 29 Working Party (set up under Article 29 of Directive 95/46/EC) on interpretation of "data controller" and "data processor" places emphasis on factual influence test

Grounds for Processing Personal Data

Processing of personal data is **prohibited** unless it meets certain conditions which include among others:

- consent has been given by the data subject
- it is necessary for the performance of a contract to which the data subject is a party
- it is necessary for compliance with any legal obligation to which the data controller is subject
- it is necessary for the purposes of the legitimate interests pursued by the data subject except where processing is unwarranted by reason of prejudice to legitimate interests of the data subject
- in the case of *Totalise Plc v Motley Fool Ltd [2003]* disclosure of the identity of an anonymous message board poster who had made defamatory remarks about Totalise Plc was permitted under Section 35 DPA - information required for prospective legal proceedings or to obtain legal advice

Grounds for Processing Sensitive Personal Data

- Sensitive personal data includes data relating to race or ethnic origin, political opinions, health, sexual life, religious and other beliefs, trade union membership and commission or alleged commission of an offence
- Sensitive personal data will only be processed fairly and lawfully as required by the first data protection principle if at least one of a number of conditions in Schedule 3 DPA is satisfied
- Grounds include:
  - explicit consent of the data subject
  - processing is necessary for purposes of exercising right or obligation imposed by law in connection with employment
  - processing is necessary for purpose of legal proceedings obtaining legal advice or establishing, exercising or defending legal rights
- Certain Orders have been made under the DPA which allow the processing of sensitive personal data in certain limited insurance contexts

Data Processing Principles

Eight data protection principles set out in Part I of Schedule 1 to the DPA must be complied with when processing personal data:

- Fairly and lawfully processed - at least one of the conditions in Schedule 2 of DPA is met, (consent, compliance with legal obligation and legitimate interest)
- Processed for limited purposes - obtained only for one or more specified and lawful purposes and not processed in any manner incompatible with that purpose.
- Adequate, relevant and not excessive - compiling too much information should be avoided, but must ensure information is sufficient for purpose.
- Accurate and kept up to date - data controller take reasonable steps to ensure the accuracy of data
- Not kept for longer than necessary
- Processed in line with data subject's rights (e.g. right of access, right to correct data and block processing in certain circumstances)
- Implement appropriate technical and organisational security measures
- No transfer of personal data to countries outside the EEA which do not provide an adequate level of protection (e.g. the US)

Data Transfers from the EEA

- The EU's Data Protection Directive prohibits transfers of personal data to countries not considered to have adequate data protection laws e.g. the US unless certain exemptions apply
- Transfer v Transmission – there is no definition of transfer under the directive
- Websites Accessed Globally – Bodil Lindquist v Kamaralagaren (2003)
- Swift Case involving transfers to the US Treasury
- Applying the Adequacy Test
- Exemptions to data transfer restrictions include:
  - Consent: however consent must be freely given
  - Model contracts: a set of standard EU approved clauses between the data exporter and importer
  - Binding corporate rules: a global company code based on European data protection principles
  - US Safe Harbor: scheme where US companies may certify compliance with EU based principles
  - Possibly where the transfer is necessary in legal proceedings, obtaining legal advice, or establishing, exercising or defending legal rights

Data Transfer from the EEA – Determining Adequacy

How does one determine adequacy? Information Commissioner guidance suggests 4 step approach.

- **Step 1** - establish whether country exporting to is subject to presumption of adequacy
- **Step 2** - consider the type of transfer, e.g. transfer to a third party processor
- **Step 3** – conduct an overall assessment of adequacy including General Adequacy Criteria and Legal Adequacy Criteria
- **Step 4** – consider application of any of the exemptions

Data Transfers from the EEA - Consent

- Data Transfers can be made with consent of the individual but consent must be:
  - Freely given
  - Specific
  - Informed
- Inform Data Subjects of reasons for transfer and, if possible, the countries involved
- Identify risks
- Consent not encouraged for systematic transfers

Data Transfers from the EEA - Model Contract Clauses

- Two main forms of Model Contract
  - between a data controller and a data processor
  - between a data controller and a data controller
- 2004 Alternative Model Contract
- Main problems with the existing model clauses:
  - administrative burden on data controllers
  - cannot generally be varied
  - model contracts difficult to administer for complex organisations
  - difficulties when using sub-processors
- WP 161 - March 2009 opinion from Article 29 Working Party on use of Model Contracts with sub-processors and recommended new model contract for processors and multi-layered sub-processing

Data Transfers from the EEA – US Safe Harbor

US Safe Harbor

- Enforced by US Federal Trade Commission and US Department of Transportation
- Seven Safe Harbor principles include:
  - **Notice** - notify data subjects of the purposes
  - **Choice** - data subjects to be given choice to opt-out of disclosure of data
  - **Onward Transfer** - third parties who receive the data must subscribe to the Safe Harbor Principles
  - **Access** - data subjects are entitled to access their data
  - **Security** - must take reasonable security precautions
  - **Data Integrity** – data must be relevant and complete
  - **Enforcement** – there must be resolution procedures in place to investigate and resolve complaints and award damages
- Not available to financial services companies that fall outside of the Federal Trade Commission Act i.e. banks, savings and loans and credit unions
- German data protection authorities (so-called Düsseldorfer Kreis) passed a resolution on 28/29 April 2010 setting stricter due diligence requirements for the personal data transfer under the Safe Harbor principles

Data Transfers from the EEA - Binding Corporate Rules

- BCRs provide a global code of practice based on EU data protection standards to allow the transfer of personal data
- BCRs recommended to apply throughout the whole group and must be binding
- Advantages of BCRs are that they allow companies to establish adequate safeguards without the administrative complexities of model contracts, flexible so can be tailored
- Disadvantages of BCRs had included complexity in putting together application, cumbersome authorisation process and recommended application to the whole group

Data Transfers from the EEA - Binding Corporate Rules

- Article 29 Working Party have issued a BCR guidance toolbox:
  - WP153 – checklist of principles which must be satisfied when formulating BCRs
  - WP154 – example framework for BCRs with list of documents to be submitted to DPAs
  - WP155 – frequently asked question with regards to BCRs
- Evidence required that BCRs are binding - WP 108 suggests:
  - use of binding corporate or contractual rules enforced against members of the group
  - unilateral declarations or undertakings given by the parent and binding on members of the group
  - incorporation through other regulatory measures e.g. in statutory codes
  - incorporation of rules within general business principles backed by policies, audits and sanctions

Managing Data Protection Requirements Globally

- Determine data flows within the group through use of questionnaires, interviews and audits
- Determine legal and regulatory requirements through internal legal resource, external information resources, such as Data guidance, and through use of local counsel
- Put in place data protection programme including any required registrations, adoption of appropriate internal and external policies, security measures, contract requirements with sub-contractors, employee training and audit mechanisms

Data Security Requirements

- EU Data Protection Directive
  - Implemented by national laws
  - Applies to all "controllers" of personal data
  - Article 17: Security of Processing
- Data Protection Act 1998 (DPA) – seventh data protection principle includes the requirements that data controllers take appropriate technical and organisational measures to keep data safe and ensure data are not retained longer than necessary
- FSA data security requirements – principles and rules
- Information Commissioner's Office (ICO) data protection guidance notes and codes of practice
- ISO 27001 and 27002 – international code of practice for information security management

Good and Bad Behaviours (1)

- FSA Report (2008) "Data Security in Financial Services" sets examples of good and bad practice, including the following
- Governance:
  - Good practice includes appointing senior manager with overall responsibility for data security; reporting to the board; having written data security policies; having detailed plans for reacting to data loss
  - Bad practice includes treating data security as an IT issue and failing to involve key staff and failing to notify customers of data loss in case details are picked up by media
- Managing third party suppliers:
  - Good practice includes conducting due diligence of their security standards at the outset of engagement and carrying out periodic review of the standards
  - Bad practice includes sending unencrypted data to third parties and using unregistered post

Good and Bad Behaviours (2)

- Controls:
  - Good practice includes having specific IT access profiles for each role in the organisation; proactively monitoring staff access to customer data and using software to spot suspicious activity by staff
  - Bad practice includes password sharing; not having clear and consistent procedures for backing up data; allowing access to web-based communication internet sites
- Disposal of customer data
  - Good practice includes limiting production of paper-based customer data; using a third party to shred or incinerate paper-based data; and properly wiping or destroying computer hard drives and portable media as soon as they become obsolete
  - Bad Practice includes poor staff awareness of disposal procedures and stockpiling obsolete hardware for too long and in insecure environments

Meeting Data Security Requirements

- A combination of people, technology and process *(PwC report "Information Security Breaches Survey 2010")*
- Build data flow charts
- Establish management steering group with responsibility, powers and resources to review data handling
- Put in place formal security and data retention policy
- Carry out internal security readiness and risk assessment
- Develop and test data breach response plans
- Make data security everyone's responsibility – staff training and increasing awareness
- Verify that outsourcing contractors are bound by data protection obligations and operate in compliant fashion

Outsourcing and Security

OUTSOURCING:

FSA Requirements SYSC Chapter 8

- Applies to authorised persons when they rely on a third party for the performance of operational functions which are critical for the performance of regulated activities, listed activities or ancillary activities
- Firm must ensure that it takes reasonable steps to avoid undue additional operational risk
  - Duty to notify the FSA when outsourcing an important function
  - Service Provider must possess capacity and authority to carry out activities and protect confidential information
  - Arrangement must be governed by written agreement which enables firm to supervise and assess performance of third party and where appropriate, terminate the arrangement.
  - Service Provider must co-operate with the FSA

Outsourcing and Security

OUTSOURCING:

- Firm remains fully responsible for discharging all of its obligations under the regulatory system and must comply, in particular, with the following conditions:
  - the outsourcing must not result in the delegation by senior personnel of their responsibility
  - the relationship and obligations of the firm towards its clients under the regulatory system must not be altered
  - the conditions with which the firm must comply in order to be authorised, and to remain so, must not be undermined
  - none of the other conditions subject to which the firm's authorisation was granted must be removed or modified
  - it must exercise due skill and care and diligence when entering into, managing or terminating any arrangement for the outsourcing to a service provider of critical or important operational functions or of any relevant services and activities

Outsourcing and Security

OUTSOURCING:

Data Protection Directive imposes specific data protection requirements when processing is outsourced by a controller:

- Processor selected must offer "adequate guarantees" as to security measures;
- Arrangement must be governed by a written agreement requiring controller's instructions before data can be processed;
- Processor must have appropriate technical and organisational procedures in place.

Consider including in contract provisions:

i. Which protect your firm from data protection breaches of the processor; and

ii. Which ensure processor will co-operate when firm receives complaints / enquiries from clients / authorities

Data Breach Notification Requirements (1)

- Currently DPA does not contain express breach-notification rules
- DPA transparency safeguards: notification regime and subject access regime
- ICO guidance on data security breach notification
- FSA – firms (e.g. banks/payment institutions) have an obligation to disclose to the FSA anything relating to the firm of which the FSA would reasonably expect notice and FSA considers it good practice for firms to tell their customers of the data loss
- Other EU countries – e.g. Germany adopted breach notification law in September 2009; France is considering draft proposal for amending the French Data Protection Act

Data Breach Notification Requirements (2)

- New rules on reporting data security breaches take the form of amendments to 2002 Directive on Privacy and Electronic Communications (e-Privacy Directive) must be implemented by June 2011
- For now applies only to the electronic communications sector
- Definition of "personal data breach"
- Key elements:
  - Duty to notify the relevant national regulator "without undue delay"
  - Duty to notify affected individual if breach is "likely to adversely affect" that individual's privacy except where provider can demonstrate it applied "appropriate technological protection measures" which render data unintelligible to unauthorised users
- March 2008 – ICO published breach disclosure guidance

Dealing with Data Security Breaches

- An organisation should consider:
  - Put in place a security breach team
  - Tell the relevant regulator if you are subject to any requirements from another regulator in relation to the same incident – e.g. ICO endeavours to avoid double jeopardy
  - Prepare evidence of steps taken since becoming aware of the security breach
  - Prepare an explanation of steps, if any taken, to compensate affected individuals
  - Prepare and explanation of the extent of potential reputational harm to you as data controller
  - Consider when and how to communicate with affected individuals

Processing for Compliance and Risk Management purposes

- Many examples:
  - AML / fraud prevention – credit checks
  - OFAC screening
  - Employee monitoring as part of an internal investigation
  - Employee background checks
  - Sarbanes-Oxley whistleblower hotlines
  - Co-operation with regulatory investigations
  - Co-operation with police / prosecuting authorities
  - Litigation disclosure

Data Protection Act vs AML Regulations

AML Requirement

- Person must make a suspicious transaction report if he suspects / knows organisation is involved in money laundering
- Failure to make a report in such circumstances is an offence
- "Tipping-off" (i.e. Warning an individual he/she is subject to a report is also an offence, must not prejudice an investigation

Data Protection and Subject Access Requirements

S7 DPA, following a written request an individual is entitled

- To be informed if data controller is holding personal data
- To be given description of data and to **whom it has been disclosed**
- To be informed of all the information which constitutes personal data
- Data Controller must respond to a written request within 40 days

Treasury Guidance

- Exemption available where disclosure would constitute a tipping-off offence

Processing for Compliance and Risk Management

Bank Secrecy and Customer Confidentiality

- UK does not have specific legislation dealing with Bank Secrecy unlike, for example, USA
- BUT banks owe duties of secrecy and confidentiality under English common / tort law
- Under English common law a bank owes a duty of secrecy to its customers
- Bank can only make disclosures regarding its customers in the following cases *(Tournier case):*
  - compelled to do so by law – includes disclosures which need to be made by the bank to FSA under FSMA but does not apply to foreign law
  - it is in the bank's interests to disclose
  - there is a duty to the public to disclose
  - where the disclosure is made with express / implied consent of the customer

Processing for Compliance and Risk Management

Bank Secrecy and Customer Confidentiality

- Bank's interests require disclosure
  - Bank is able to use confidential information in order to defend itself
- Duty to the public to disclose:
  - Particularly relevant in current environment
  - Court will consider the reasons for which confidential information is being sought
  - Duties of secrecy / confidentiality cannot be used to conceal fraudulent activities
- Disclosure limited to what is necessary to satisfy the public interest

Processing for Compliance and Risk Management

Breach of Confidence

- Banks and other financial institutions have a duty of confidence under tort law
- Duty applies to:
  - information
  - with the quality of confidence
  - imported in circumstances importing an obligation of confidence
- Once again disclosure can be made when it is justified in the public interest
- Financial institution will also owe a duty of confidentiality to its employees
- Human Rights Act (HRA) – Article 8 of the HRA gives individuals a right to privacy
- Claim for breach of confidence can lead to claim for breach of Article 8 as courts are public bodies and must act compatibly with European Convention on Human Rights

Processing for Compliance and Risk Management

Whistleblowing Hotlines

- Product of US Sarbanes-Oxley Act 2002 (SOX):
  - US public companies must provide system which allows employees to report any concerns (in particular in relation to auditing / accounting) of accounting/auditing rules being violated
  - Companies which fail to comply with SOX face heavy fines / de-listing from stock exchange
  - US listed companies should make sure European subsidiaries comply with SOX requirements
- European Developments 2005
  - France: Commission Nationale de l'Informatique et de Libertes (CNIL) decided that hotlines set up by companies with significant US nexus violate French data protection laws
  - Germany: Employment courts determined that in order for a major US company to implement a hotline in a German subsidiary, it must first engage in a dialogue with its work council

Processing for Compliance and Risk Management

Whistleblowing Hotlines

Article 29 Data Protection Working Party

- Guidance (1996/Working Paper 117) on whistleblowing schemes operating in the EU:
  - Hotlines should be structured to limit the number of persons entitled to report improprieties and the number of persons who can be incriminated
  - Reports should be on a named and confidential basis
  - Type of information reported limited to accounting / auditing matters
  - Employees should be informed of the existence, purpose and functioning of the hotline
  - Firms must inform an employee if implicated by a hotline report unless doing so would jeopardise the firms investigation
  - Firms must take reasonable precautions to ensure data is secure
  - Firms should establish an internal team dedicated to handling reports
  - If hotline is outsourced, firms must establish a mechanism for complying with EU data transfer rules
  - Firms must comply with applicable local laws / requirements

Processing for Compliance and Risk Management

Whistleblowing Hotlines

Compliance Strategies:

- Narrow the scope of the hotline and prevent employees from submitting complaints on frivolous matters
- Employees using the hotline should be encouraged to provide their personal details
- Inform implicated employees promptly
- Limit the time data can be held
- Restrict transfers of data outside of EEA where possible and if not deal with EU data transfer restrictions
- Implement stringent due diligence and data-processing contracts if outsourcing to a third party
- Require all individuals who handle complaints to enter into confidentiality agreements

Processing for Compliance and Risk Management

Telephone Recording

- DPA
  - interception of employees' communications only if proportionate and in accordance with Data Protection Act principles.
- Regulation of Investigatory Powers Act 2000 (RIPA)
  - offence to intercept communications on a private telecommunication system unless made with the consent or unless other exemptions apply
- FSA Obligations Conduct of Business Sourcebook (COBS):
  - Firms obliged to record telephone conversations and electronic communications to deter market abuse
  - In particular, firms must record telephone/electronic communications with clients regarding transactions / negotiations in financial instruments

Processing for Compliance and Risk Management

Recording Requirements

Application: Following conditions must be met for Recording Requirements for FSA rules to apply:

- Condition 1: Firm carries out Relevant Activities (i.e. received / executes / arranges / carries out / places on behalf of – Client Orders)
- Condition 2: Relevant activities relate to investments traded on a UK recognised stock exchange / EEA regulated market
- Condition 3: Relevant Activities carried out from an establishment in the UK

If conditions are satisfied:

- Firms must take reasonable steps to record and maintain for 6 months telephone and electronic communications (made by an employee or contractor) when concluding an agreement to carry out any Relevant Activity with a client
- Electronic Communications – Fax / Email / Instant Messaging Services
- Limited exemptions:
  - i) Investment Manager
  - ii) Operator of collective investment scheme

Document Disclosure - Litigation and Investigations

- Significant differences between the US and UK approach to discovery and Civil law countries such as France and Germany
- Europe - disclosure is limited to what is needed for the scope of the trial
- Attitude reflected in the nature of “blocking statutes”
- Case Law Developments: Aerospatiale case in 1987 vs MAFF or Executive Life case
- Advisory working party guidance EU data protection requirements and US litigation commented that EU data protection laws do not intrinsically prevent transfers of personal data from the EU for litigation purposes

Document Disclosure - Litigation and Investigations

- Companies must consider the Guidelines in each phase of data processing for litigation purposes
  - Phase 1: Retention
  - Phase 2: Disclosure
  - Phase 3: Onward transfer
  - Phase 4: Secondary use
- Personal data should only be kept for the period of time necessary for the purposes for which it is collected
- Contrast with requirement to retain documents under local law and regulatory requirements or possible future litigation
- Specific or imminent litigation - EU Commission accept data can be retained until conclusion of proceedings
- Recall grounds for processing personal data – Consent/legitimate interest/ legal obligation - an obligation imposed by a foreign legal statute will not be sufficient

Document Disclosure - Litigation and Investigations

- Processing of data for litigation purposes - justified when in the legitimate interests of the data controller but provided rights of the individual are not overridden
- Individuals must be provided with fair processing information unless limited exceptions apply
- A balancing test must be applied in considering the relevance of the personal data to the litigation and the consequences for the individual
- Must act in a proportionate and fair way
  - determining if the information is relevant to the case;
  - assessing the extent to which personal data is included;
  - considering whether the personal data can be redacted, anonymised or pseudononymised

FSA Enforcement

- Chapter 6 of the Decision Procedure and Penalties Manual (DEPP) sets out guidance on FSA's policy with regard to financial penalties
- FSA policy statement PS10.4 (Enforcement financial penalties), March 2010
  - New five step penalty framework for determining financial penalties
  - Step 1: Disgorgement - FSA will seek to deprive a firm of the financial benefit derived directly from the breach of the FSA rules
  - Step 2: Penalty figure determined reflecting the nature, impact and seriousness of the breach - Depending on the seriousness of the breach, the FSA may impose a penalty of up to 20 per cent of the revenue derived by the firm during the period of the breach
  - Step 3: Adjustment for mitigating and aggravating factors
  - Step 4: Adjustment for deterrence
  - Step 5: Discount for settled cases

FSA Enforcement

- July 2009 – FSA fined insurance group over £3m
- Large amounts of unencrypted personal data sent by post/courier; loss of CD containing personal data of 180,000 policy holders
- FSA says firm did not take reasonable care to establish and maintain effective systems and controls to manage risk relating to data security, specifically risk that customer information might be lost or stolen
- Fine imposed solely on the basis of a breach of Principle 3 although no actual loss identified

FSA Enforcement

- Specific failures by insurance group
  - Unencrypted media sent to third parties
  - Confidential data not properly and securely stored
  - Hard copy data sent to third parties had inadequate security arrangements
  - Entered into contracts with third parties to outsource data security functions (i.e. Confidential waste disposal) without explicitly ensuring the third party had appropriate data security arrangements in place

FSA Enforcement

- December 2007 – Various insurance and pension entities collectively fined £1.26m
- Fraudsters used publicly available information to extract confidential customer information
- FSA found:
  - Failure to undertake adequate assessment of the financial crime risks (in particular in relation to information security)
  - Failure to assess adequacy of existing controls and failure to implement adequate and effective procedures made in November 2006
- Fine imposed solely on the basis of a breach of Principle 3

Enforcement Outlook for 2010/11

- In the consultation paper on fees and levies (CP10/5) published in February 2010, the FSA stated that encouraging regulated firms to improve financial crime systems and controls continues to be one of its key priorities for 2010/11
- In its 2010/11 Business Plan, the FSA reminded regulated firms of its commitment to "credible deterrence" and delivering intensive supervision
- Further high profile cases with higher fines for serious regulatory non-compliance are to be expected

SIDLEY AUSTIN LLP
SIDLEY

Comments/Questions

BEIJING BRUSSELS CHICAGO DALLAS FRANKFURT GENEVA HONG KONG LONDON LOS ANGELES NEW YORK PALO ALTO SAN FRANCISCO SHANGHAI SINGAPORE SYDNEY TOKYO WASHINGTON, D.C.

SIDLEY AUSTIN LLP
SIDLEY

Sidley Austin provides services to meet the needs of clients on three continents. Our London Financial Services Regulatory Practice represents a broad range of financial institutions and related businesses. We act for clients with extensive UK, European and international operations, as well as for clients based in the United States or elsewhere and looking to do business in the UK and the EU.

SIDLEY AUSTIN LLP

SIDLEY

Banking & Financial Services Regulation

John Casanova
jcasanova@sidley.com

William Long
wlong@sidley.com

Sidley Austin LLP
Woolgate Exchange
25 Basinghall Street
London, EC2V 5HA
United Kingdom
T: +44 (0) 20 7360 3600
F: +44 (0) 20 7626 7937

www.sidley.com

BEIJING BRUSSELS CHICAGO DALLAS FRANKFURT GENEVA HONG KONG LONDON LOS ANGELES NEW YORK PALO ALTO SAN FRANCISCO SHANGHAI SINGAPORE SYDNEY TOKYO WASHINGTON, D.C.

4307536