Legal risks faced by financial institutions and the evolving regulatory landscape in the EU and US
### Legal risks faced by financial institutions

<table>
<thead>
<tr>
<th>Risk</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business interruption (loss of opportunity/profit)</td>
<td></td>
</tr>
<tr>
<td>Damage to market reputation (e.g. share price)</td>
<td></td>
</tr>
<tr>
<td>Litigation (contractual claims, statutory claims)</td>
<td></td>
</tr>
<tr>
<td>Fines and other regulatory action (e.g. undertakings, audits)</td>
<td></td>
</tr>
<tr>
<td>Fraud (financial loss)</td>
<td></td>
</tr>
<tr>
<td>Damage to reputation with customers/consumers (complaints, loss of business)</td>
<td></td>
</tr>
<tr>
<td>Costs (compensation, internal time costs and out-of-pocket expenses, e.g. advice)</td>
<td></td>
</tr>
<tr>
<td>Loss of commercially sensitive information or intellectual property</td>
<td></td>
</tr>
</tbody>
</table>
Legal risks faced by financial institutions

Before an attack
- Failure to identify risks and plan
- Failure to prevent

- Ensure security and integrity
- Implement policies and practices
- Risk assessment and mitigation
Legal risks faced by financial institutions

Ensure security and integrity

Data Protection Act 1998
- Principle 7: appropriate technical measures

FSA Rules
- SYSC: Systems and controls
- FCA Principles for Businesses –
  - 1: Integrity
  - 2: Skill, care, diligence
  - 6: Customer interests

Contracts
- Customer or supplier?
- Security obligations
- No viruses/malware
- Good industry practice

Confidentiality
- Bank confidentiality
Legal risks faced by financial institutions

**Implement policies and practices**

**Data Protection Act**
- Principle 7: appropriate organisational measures (e.g. cyber response, employment policies)
- Principles 3/5: retention
- Appointment of DPO?

**FSA Rules**
- SYSC: systems and controls
- FCA Principles for Businesses - 3: adequate risk management systems

**Contracts**
- Security obligations
- Governance and records
- Policies and procedures
- Business continuity

**Best practice**
- ISO standards (27000 series)
- BIS Guidance
- ENISA and EC3
- Culture

**Contracts**
- Security obligations
- Governance and records
- Policies and procedures
- Business continuity

**FSA Rules**
- SYSC: systems and controls
- FCA Principles for Businesses - 3: adequate risk management systems

**Data Protection Act**
- Principle 7: appropriate organisational measures (e.g. cyber response, employment policies)
- Principles 3/5: retention
- Appointment of DPO?
Legal risks faced by financial institutions

Data Protection Act 1998
- Principle 4: data not kept for longer than necessary

Draft Regulation?
- Privacy impact assessments

FSA Rules
- Systems and controls
- Integrity
- Service continuity

Risk assessment and mitigation

Contracts
- Audits; testing; certification
- Contractual due diligence

Insurance
- Cyber-attacks

© Allen & Overy 2013
Legal risks faced by financial institutions

After an attack

- Failure to report
- Failure to respond

- Incident reporting

- Litigation and enforcement action

- Taking positive action
Legal risks faced by financial institutions

Data Protection Act 1998
- No obligation to report to ICO
- ICO guidance: notification of serious breaches

FSA Rules
- FCA Principles for Businesses – 11: Notification to FCA
- IT security; Fraud; irregularities

Contracts
- Notification of counterparty
- Security breach
- Breach of agreement

Law enforcement
- Reporting criminal offences
- Fraud
- Computer Misuse Act
Legal risks faced by financial institutions

Data Protection Act 1998
- Enforcement notices
- Undertakings
- Fines (up to £500k)
- Civil claims

Draft Regulation
- Up to 2% of annual worldwide turnover

FSA Rules
- Fines (unlimited)
- E.g. HSBC, Zurich, Nationwide

Contracts
- Defending civil claims
- Limitations on liability and force majeure ("reasonable control" / governmental acts)

Taking action
- Injunctive relief
- Reputation management

Litigation and enforcement action
The evolving regulatory framework
The evolving regulatory framework

– Criminal law
  – Patchwork of national criminal laws
  – Proposed Directive on “Attacks Against Information Systems”
  – Causes of action: Computer Misuse Act; Breach of Statutory Duty; Fraud Act 2006; Breach of confidence; Data Protection Act 1998; Privacy and Electronic Communications (EC Directive) Regulations 2003; Protection from Harassment Act 1997; Trespass to Goods / Conversion; Unlawful interference with trade; Conspiracy; Encouraging or assisting the commission of an offence; Serious Crime Act 2007.

– Regulation
  – Proposed Directive concerning measures to ensure a high common level of network and information security (NIS) across the EU
  – UK Government cyber security strategy; no specific legislative proposals
  – US Executive Order
The evolving regulatory framework (EU)

What?

- EC proposal for a Directive on “Attacks Against Information Systems” proposed on 30 September 2010

Why?

- Aimed at harmonising the criminalisation of specific conducts

When?

- On 20 June 2012, the Directive was approved by the European Council and has been forwarded to the European Parliament for its formal approval but Parliament has not yet given formal approval

How?

- New offences: unlawful interference, illegal access, illegal interceptions, large-scale cyber-attacks such as DDoS attacks and botnet attacks, producers of trojan horses and malware, aiding & abetting etc.
<table>
<thead>
<tr>
<th>The evolving regulatory framework (EU)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>What?</strong></td>
</tr>
<tr>
<td>- EC proposed Directive concerning measures to ensure a high common level of network and information security (NIS) across the EU</td>
</tr>
<tr>
<td><strong>Why?</strong></td>
</tr>
<tr>
<td>- Aimed at harmonising the prevention of NIS risks and incidents, the response to NIS incidents and the mitigation of their impact</td>
</tr>
<tr>
<td><strong>When?</strong></td>
</tr>
<tr>
<td>- Published on 7 February 2013</td>
</tr>
<tr>
<td><strong>How?</strong></td>
</tr>
<tr>
<td>- “appropriate technical and organisational measures to manage risks…”</td>
</tr>
</tbody>
</table>
The evolving regulatory framework

| What? | – EC proposed Directive concerning measures to ensure a high common level of network and information security (NIS) across the EU |
| Why? | – Aimed at harmonising the prevention of NIS risks and incidents, the response to NIS incidents and the mitigation of their impact |
| When? | – Published on 7 February 2013 |
| How? | – “notify to the competent authority incidents having a significant impact on the security of the core services they provide”  
– “competent authority may inform the public or require the market operators to do so, where it determines that disclosure of the incident is in the public interest….” |
The evolving regulatory framework (EU)

- **European Network and Information Security Agency (ENISA)**
  - Based in Cyprus
  - Centre of network and information security expertise for the EU, its member states, the private sector and Europe’s citizens
  - Advice; recommendations; good practice

- **European Cybercrime Centre (EC3)**
  - Started operations on 11 January 2013
  - Part of the European Police Office (EUROPOL); to act as the focal point in the fight against cybercrime in the EU
  - To pool European cybercrime expertise, provide support to cybercrime investigations and become the collective voice of European cybercrime investigators across law enforcement and the judiciary
The evolving regulatory framework (UK)

– Cybersecurity Information Sharing Partnership (CISP)
  – Will enable the government and industry to share information on current threats and managing incidences.
  – Pilot involving 160 companies across 5 sectors – defence, finance, pharmaceuticals, energy and telecommunications – opened to companies within critical national infrastructure sectors in 2013.
  – Plans to extend the service to small and medium-sized businesses, in a 2nd phase.

– National Cybercrime Unit
  – The Police Central e-Crime Unit and the Serious Organised Crime Agency (SOCA) are joining together in 2013 to form a National Cyber Crime Unit in the newly-formed National Crime Agency.
  – Will lead the UK’s response to cyber crime both in the UK and internationally and look at ways of preventing cyber crime to protect UK citizens, commerce and our national infrastructure.
  – SOCA is increasing its cyber capability. It is introducing cyber overseas liaison officers and a number of posts dedicated to mainstreaming cyber and digital investigations across the organisation.
The evolving regulatory framework (US)

- US federal law enforcement has made “cyber crime” a priority
- FBI Computer Crime & Intellectual Property Section has legal attaches in embassies abroad to coordinate multi-national investigations
- DOJ Intellectual Property Task Force
- 2008 PRO IP Act gave the DOJ and FBI a mandate to vigorously prosecute intellectual property crimes, but Congress has not appropriated funds for most of its initiatives
The evolving regulatory framework (US)

– February 2013 executive order on cybersecurity:
  – Critical infrastructure includes assets and systems vital to the nation’s physical and economic security and public health and safety
  – Framework for best practices to be developed by Director of the National Institute of Standards and Technology in consultation with industry groups and relevant agencies by October 2013
  – Government will offer incentives to promote voluntary adoption of the framework by critical infrastructure operators
  – Critical infrastructure operators will be eligible to receive classified information about potential threats
The evolving regulatory framework (US)

– **Cyber Intelligence Sharing Act**
  – Aimed at encouraging greater sharing of threat data between the private sector and the federal government
  – CISPA would remove obstacles to greater sharing of malware and other threat data by companies to the government and vice versa
  – Would protect companies from lawsuits related to their sharing of data with the government
  – Faces resistance in the Senate - Democrats want more robust privacy safeguards as well as measures to protect the nation’s most critical computer systems
  – White House has said it will veto the legislation if it does not include stronger privacy protections
The evolving regulatory framework (US)

- Gramm-Leach-Bliley Safeguards Rule and FTC Disposal Rule require information security planning by financial institutions, including prevention of pretexting and precautions in maintenance and destruction of consumer credit information
  - In 2008, FTC settled a Safeguards Rule case against a lender that sold as surplus a hard drive containing 34,000 unencrypted customer loan files with a consent decree that requires training, improved physical and technical safeguards and biennial independent security audits for 10 years
- Other FTC claims
  - In 2006, the FTC obtained a $10 million penalty and $5 million for customer redress from a consumer credit reporting company that violated the FCRA by selling credit reports without sufficient screening, despite notice of fraud, and claiming in its privacy policies that it complied with the FCRA
The evolving regulatory framework (US)

- Customer suits
  - UCC Art. 4A - immunity from liability for honoring fraudulent wire transfers only if the bank has “commercially reasonable” security
  - 1st Circuit recently held a bank responsible for funds stolen by hackers who installed key-logging software on its servers to capture customer passwords because the bank did not follow its own procedures, used security questions too often (so they were more likely to be captured by hackers) and did not notify the customer of unusual activity in its account
  - Increased risk of identity theft from breach may confer standing, but may not satisfy the harm element of causes of action such as negligence
  - 2011 breach of Sony’s Playstation network
    - 75 million customers’ personal data was stolen (and customers were not notified of the theft for several days)
    - Customer class actions claiming negligence, violation of California consumer protection and breach notification laws and unjust enrichment ultimately were dismissed for lack of actual harm and because Sony’s terms of service disclaimed assurances of security
These are presentation slides only. The information within these slides does not constitute definitive advice and should not be used as the basis for giving definitive advice without checking the primary sources.

Allen & Overy means Allen & Overy LLP and/or its affiliated undertakings. The term partner is used to refer to a member of Allen & Overy LLP or an employee or consultant with equivalent standing and qualifications or an individual with equivalent status in one of Allen & Overy LLP’s affiliated undertakings.