Cyber Update:

Byte-Sized Regular Updates on Cyber Liability Issues

Deal reached between EU and US to replace Safe Harbor

The European Union and the United States have agreed a new framework for transfers of personal data. It will be called the EU-US Privacy Shield. It replaces the Safe Harbor scheme which was declared invalid by the European Court of Justice in October 2015.

The new framework will include the following elements:

- **Strong obligations on companies handling Europeans' personal data and robust enforcement**: US companies wishing to import personal data from Europe will need to commit to robust obligations on how personal data is processed and individual rights are guaranteed.

- **Clear safeguards and transparency obligations on U.S. government access**: The US has given the EU written assurances that the access of public authorities for law enforcement and national security will be subject to clear limitations, safeguards and oversight mechanisms. These exceptions must be used only to the extent necessary and proportionate.

- **Effective protection of EU citizens' rights with several redress possibilities**: Any citizen who considers that their data has been misused under the new arrangement will have several redress possibilities.

Details of the arrangement still need to be finalised and we expect further information in the coming weeks.

US court refuses to dismiss Travelers cyber defence case

A US District Court in Utah has refused to dismiss a bad faith claim by Federal Recovery Services against Travelers, despite finding Travelers was under no duty to defend the insured under its CyberFirst policy.

In 2012, Global Fitness Holdings issued proceedings against FRS alleging that it had intentionally misused the account information of GFH’s customers. FRS sought a defence and indemnity from Travelers under its cyber policy. Travelers provided a defence subject to a reservation of rights.

Travelers was not obliged to defend FRS as:

“While the policy covers errors, omissions and negligent acts, Global’s claims against Defendants allege far different justifications for the data to be withheld.

“Global does not allege that defendants withheld the data because of an error, omission or negligence.” On the contrary, it alleges FRS “knowingly withheld this information and refused to turn it over until Global met certain demands”.

Despite the earlier finding in Travelers’ favour, the judge refused summary judgment on the issue of whether Travelers inappropriately required FRS to first receive proceedings before initiating a claim and whether the insurer failed to “diligently investigate, fairly evaluate, and promptly and reasonably communicate with [FRS] since the claim was initially tendered in December 2012.”

The Judge went on to say:

“Defendants provide expert testimony stating that Travelers’ conduct did not measure up to the standard required for insurance claim investigations . . . Here, the narrow issue of whether Travelers inappropriately required the filing of suit papers in contravention of the CyberFirst Policy provisions, which may have resulted in a dilatory denial of defense causing severe financial consequences to the Defendants, is a factual issue and may be submitted to the jury.”

This case is a reminder of the importance of insurers promptly investigating and responding to claims even where coverage is disputed.

“While the policy covers errors, omissions and negligent acts, Global’s claims against Defendants allege far different justifications for the data to be withheld...”
Lloyd’s of London announces core data requirements for cyber insurance

Lloyd’s of London, together with AIR Worldwide and RMS, has announced a set of common core data requirements for cyber risks.

The common core data requirements will help it track exposures and should assist underwriters to better develop policies covering cyber risks and liability.

Tom Bolt, Lloyd’s Director of Performance Management, said:

"Cyber insurance is an important new area of coverage and it is essential that we have good quality standardised data to track exposures . . . The cyber insurance industry is showing real innovation and demonstrates the ability of insurers to develop policies to cover modern, complex risks. Due to the growing importance of this risk class, quality standardised exposure data is critical for increased levels of insurance coverage and better risk modelling . . . models for cyber risks are still developing and need the industry to work collectively so that risk can accurately be calculated."

The common core data requirements are available at: http://www.lloyds.com/cybercoredata

Hedge Fund Standards Board reports on first cyber-attack simulation

The Hedge Fund Standards Board (HFSB), the standard setting body for the hedge fund industry, recently held its first table top cyber-attack simulation for hedge fund managers in London.

The objective of the simulation was to explore the response of managers to three realistic cyber-attack scenarios:

+ Data theft and leakage of internal sensitive data;

+ Financial infrastructure attack; and

+ Crypto ransomware.
Key insights from the simulation were:

+ Confusion over responsibilities can prevent an effective response. Managers should not consider cyber security as just an “IT” issue, given the legal, compliance, investor relations and reputational issues involved.

+ Certain types of cyber-attacks may exceed a manager’s internal response capabilities. Managers need to be prepared to quickly access external legal and IT expertise.

+ Preparation in advance, through a cyber-security incident response plan, is important. This planning establishes responsibilities, pre-identifies external resources and speeds decisions should there be an actual incident.


Information Commissioner reports on risk to companies that fail to keep data safe

The Information Commissioner’s Office commissioned a YouGov poll to mark European Data Protection Day. It showed that 20% of people would definitely stop using a company’s services after hearing news of a data breach, while 57% would consider stopping.

The Information Commissioner said:

“Companies that play fast and loose with people’s personal information risk the wrath of the ICO and that means fines of up to £500,000.

A heavy fine is bad enough, but the time, energy and money it takes to rebuild customer confidence can be as severe a punishment as the fine itself.

The knock on effect of a data breach can be devastating for a company. Getting hit with a fine is one thing, but when customers start taking their business – and their money – elsewhere, that can be a real body blow.”

February 2016

For further information please contact:

James Hutchinson
Partner
T: +44 (0) 20 7469 0408
E: j.hutchinson@beale-law.com

Follow our cyber team on twitter @cyberclaims