

Accountancy Update

December 2009

“One of our laptops is missing” - The risks of data loss and how to prevent it

The European Consumer Commissioner has recently described personal data as “*the new oil of the internet and the new currency of the digital world*”. However, if data is handled incorrectly, lost or misused it can quickly become a toxic liability for companies and bring them to the attention of the regulators with adverse financial and reputational consequences. In this article, we consider what lessons can be learned from previous reported breaches, what practical tips organisations can follow to help prevent data losses, what the regulators’ approach is to the issue of lost data and what to do if a breach occurs.. [More...](#)



Case notes

Legal Professional Privilege does not extend beyond the legal profession

The High Court in *Prudential Plc & Anor v Special Commissioner* held that legal professional privilege (LPP) does not extend to accountants. Although the case confirms what was already considered to be the standard position – that legal advice from accountants is not subject to LPP – it serves as a useful reminder given the emphasis on disclosure by HMRC and the increasingly aggressive approach taken by HMRC to compel production of documents. [More...](#)

No more speculative foreign regulator requests for documents? Accountants must disclose documents requested by a foreign regulator, but only those which fall within the foreign regulator’s pleaded case

In this case, for the first time, a party who would have been prejudiced by disclosure being made by another firm has challenged the decision by the FSA to co-operate with an overseas regulator. Given the increase in requests from regulators for documents, the High Court’s guidance is of assistance in determining whether a request should be met, or challenged. Following the decision, there appears to be considerable scope to challenge requests [More...](#)

Round-up

Our Round-up section includes reports on the continuing discussion relating to audit firms providing non-audit services and the changes the AADB has made to its Accountancy Scheme. [More...](#)

[View all](#)

Firm news

We are delighted to announce the addition of Jonathan Levy to the partnership... [More...](#)

Any comments or queries?

Jane Howard
+44 (0)20 3060 6888
jane.howard@rpc.co.uk

Maria Oats
+44 (0)20 3060 6862
maria.oats@rpc.co.uk

“One of our laptops is missing” - The risks of data loss and how to prevent it

The European Consumer Commissioner has recently described personal data as *“the new oil of the internet and the new currency of the digital world”*. However, if data is handled incorrectly, lost or misused it can quickly become a toxic liability for companies and bring them to the attention of the regulators with adverse financial and reputational consequences. In this article, we consider what lessons can be learned from previous reported breaches, what practical tips organisations can follow to help prevent data losses, what the regulators’ approach is to the issue of lost data and what to do if a breach occurs.

Data losses and/or unauthorised access to data can be the result of a number of factors including technical security failures, stolen equipment, hacking, an employee losing a laptop or papers, or rogue employees actively misusing data (eg the recent incident where a T-Mobile employee sold customer data to rival companies.)

T-Mobile are not alone however. One needs only to glance at recent newspaper headlines...

“HSBC fined £3m by the FSA over data security”, “FSA fines Nationwide £980k for information security lapses”, “ICO raps insurance firms for data breaches”...

These show that the problem of data losses (and its consequences) are very real in the financial sector.

Regulatory Bodies – FSA/ICO

The main regulatory bodies to be aware of are the Financial Services Authority (FSA) and the Information Commissioner’s Office (ICO) who enforce and monitor compliance with the Data Protection Act 1998 (DPA).

The DPA includes a set of “good information handling” principles which apply to the use and holding of personal data (ie data that can be used to identify a living individual). The seventh of these principles requires data controllers to take *“appropriate technical and organisational measures to protect personal information against unlawful or unauthorised use or disclosure and accidental loss, destruction or damage”*.

With respect to data breaches, the FSA’s remit can be seen to go wider than the ICO’s. This is because the FSA has a statutory objective to reduce financial crime. The FSA will therefore be interested not only in any loss of personal data but any loss of data which could be used to access account details (ie credit card details) and any data which could be used for impersonation or to create a false identity (names, dates of birth, NI numbers). This would extend to data about companies which is not “personal data” for the purpose of the DPA. The FSA is also concerned about precautions to ensure the security of price sensitive inside information.



Oliver Bray
+44 (0)20 3060 6277
oliver.bray@rpc.co.uk

Jonathan Davies
+44 (0)20 3060 6466
jonathan.davies@rpc.co.uk

[Back to contents](#)

FSA Principle 3 states that a firm “*must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems*”. It was for breach of this general principle that Nationwide Building Society was fined £980k and, more recently, three companies in the HSBC group fined more than £3m.

How to avoid problems – practical tips

Data losses and their consequences are a hot topic at the moment with increasing publicity and regulatory activity in these areas. It is therefore critical that companies look at their data use and risk profile and implement systems to avoid problems with unauthorised access to and/or loss of data.

The ICO states that there is no single magic bullet for this problem but that there will always be three main elements:

- Clear thinking and paperwork (namely putting in place policies, procedures, systems, controls and actively monitoring compliance with these)
- Getting the technology right (including system architecture)
- Focusing on people and behaviour

In order to assist companies in complying with their obligations with respect to personal data, the ICO has published a number of useful guidance notes which can be found in the “Tools and Resources” section on its website www.ico.gov.uk

In addition, in April 2008, the FSA issued detailed guidance on data security entitled “Data Security in Financial Services” which can be found at www.fsa.gov.uk/pubs/other/data_security.pdf.

The guidance contains a number of examples of both good and bad practice.

As you would expect the guidance issued by both regulators covers broadly common ground and they make similar recommendations. From the guidance one can extract certain key principles/ approaches:

1. The first step is to look at the data you hold. How valuable/ sensitive is the data? What damage could be caused if it were lost? What are your security policies? What are your disaster recovery/continuity policies?
2. Secondly, audit your physical security. What access controls are in place (passes, locks, alarms etc)? Do you operate (and enforce) a clean desk policy? Are paper documents locked away at the end of each day? How is paper waste disposed of?
3. What technical security measures are taken? Are there requirements for strong passwords? Firewalls? Anti-spyware? Do you block spam? What are your back up procedures? How do you dispose of equipment?
4. Removable devices (memory sticks etc) should be treated with extreme caution. You should consider banning use of these or at the least controlling access. Above all the regulators are abundantly clear that you must always encrypt any removable devices before they are taken off site. Encryption solutions must meet certain minimum standards and be kept up to date. Be aware that the ICO has expressly stated “*in the future, if laptops*

are stolen from vehicles/public places and encryption software has not been used then enforcement action will be taken.”

5. Also look to the employees (including any temporary or agency personnel). How reliable are they? What checks are carried out at the recruitment stage? What access do they have to data? Could this access be restricted? Does the staff handbook cover use and disclosure of data? Is it up to date? How are staff made aware of policies (and updates)? Are staff properly trained on an ongoing basis? What access do they have to the internet and personal email? Consider if access should be blocked if they also have access to customer data.
6. Consider your contractual arrangements (including any outsourcing). What due diligence do you conduct on third party suppliers (consider not just server hosts but couriers, cleaning agencies, waste disposal etc)? Do you have written agreements in place? Do these deal adequately with use of data, disclosure, security measures? How do you supervise third parties? Do you have audit rights to check that contractual safeguards are being complied with? Do you exercise these?
7. Finally, put in place clear policies and procedures (and document these) which reflect the realities of data use (and the risks of data loss) in your organisation. Where you conduct any regulated activities this must also deal with financial crime risks as well as DPA compliance. This should be a living structure and you should conduct regular internal verification/compliance tests to ensure this structure and any associated documentation is kept up to date/remains appropriate.

What to do if a breach occurs

Of course, as can be seen from the recent T-Mobile incident, it is not always possible to prevent data breaches. So what should you do if a breach occurs?

The immediate priority is to act expeditiously to manage risk and to take all necessary steps to reduce risk or damage to individuals and the integrity of your organisation. The FSA and the ICO do not look favourably on any delay in dealing with data breaches.

You should ensure your organisation has a nominated team (and lead individual) to deal with and manage any data breaches and to look to see how the breach can be contained and data recovered and to assess the ongoing risk.

You should consider how the breach occurred, how many people are affected, how sensitive the data is, what protections were in place (eg encryption) and whether you need to notify.

Notification to Individuals

There is no legal obligation to notify breaches to affected individuals from an ICO perspective. But you should think about whether notification would help the individual (for example, would it allow them to change passwords, cancel credit cards etc). If you are going to notify individuals then you need to consider how to communicate the message and at this point your marketing department/PR agency should be involved.

Notification to the ICO

There is no legal obligation to report breaches to the ICO. However, the ICO considers that serious breaches should be brought to its attention. "Serious Breach" is not defined but you will need to make an assessment based on potential harm to individuals, volume of data lost or accessed and sensitivity of that data. If the loss is likely to cause significant harm there is a presumption that you should report.

Notification should contain all relevant information including:

- Type of information/number of records
- Circumstances of loss/release
- Action taken to minimise effect
- How you investigated the breach
- Whether you have informed any other regulators (ie the FSA) and if so what their response was
- Remedial action taken to prevent future occurrences

Notification to the FSA

FSA rules require the notification of any significant failure in firms' systems and controls. This is likely to include any serious information security lapse, certainly where there is a possibility of improper access to information which could be used for identity theft or other fraud or which is price sensitive – or simply where the lapse indicates a breakdown of proper systems and controls.

Watch this space

Currently the ICO has no power to issue civil monetary penalties. However, the Criminal Justice and Immigration Act 2008 introduced new sections 55A and 55B to the DPA which allow the ICO to issue a monetary penalty for serious contraventions of the DPA likely to cause substantial damage or distress where either (i) the contravention was deliberate; or (ii) the controller knew or ought to have known that there was a risk breach would occur and that it would cause substantial damage/distress and they failed to take reasonable steps to prevent it.

The Ministry of Justice is currently consulting on a proposal for the penalty to be set at a maximum of £500k in order to give the ICO flexibility to deal effectively with a wide range of companies with varying financial resources. It appears likely that these penalties will come into force in the first half of 2010.

Firms that are FSA regulated when the new powers come into force could be potentially exposed to fines from both the FSA and the ICO, and there is no indication that either regulator will give credit for a fine imposed by the other. You have been warned....

Case notes

Legal Professional Privilege does not extend beyond the legal profession

The High Court in *Prudential Plc & Anor v Special Commissioner*¹ held that legal professional privilege (LPP) does not extend to accountants. Although the case confirms what was already considered to be the standard position – that legal advice from accountants is not subject to LPP – it serves as a useful reminder given the emphasis on disclosure by HMRC and the increasingly aggressive approach taken by HMRC to compel production of documents.

The case arose out of a request for documents by HMRC under section 20 of the Taxes Management Act 1970 (section 20 notice). Prudential sought to challenge the section 20 notice on two points, one being that the material sought was subject to LPP.

It had previously been held by the House of Lords in *R v A Special Commissioner, ex p Morgan Grenfell & Co Ltd*² that HMRC could not force disclosure of legal advice provided by members of the legal profession by serving a section 20 notice.

It was accepted that the legal advice provided to Prudential was from accountants who were not members of the legal profession. However, Prudential sought to argue that LPP should extend to accountants providing skilled legal advice about tax law.

Mr Justice Charles dismissed Prudential's arguments, relying on the case of *Wilden Pump Engineering Co v Fusfeld*³, where legal advice on patent law provided by patent agents was held not subject to LPP. The judge held "for LPP to apply to legal advice and assistance it has to be given by a member of the legal profession with exceptions or extensions when the right or privilege arises in litigation, or when litigation is contemplated".

On the basis of the previous authorities on LPP, the judge considered that he could not extend LPP to accountants (or other professionals), as previous authorities linked LPP to the legal profession and not to the purpose and nature of the advice itself. Such an extension could only be made by Parliament.

However, the judge did accept the force of the argument that accountants and lawyers should be given a "level playing field". The judge commented that to achieve parity, not only could Parliament decide that LPP be applied to accountants, but equally a client's right to refuse disclosure on grounds of LPP might be removed.



[Back to contents](#)

Rachael Healey
+44 (0)20 3060 6029
rachael.healey@rpc.co.uk

Footnotes

- 1 [2009] EWHC 2494.
- 2 [2003] 1 AC 563.
- 3 [1985] FSR 15

[Back to contents](#)

[Back to contents](#)

No more speculative foreign regulator requests for documents? Accountants must disclose documents requested by a foreign regulator, but only those which fall within the foreign regulator's pleaded case

In this case, for the first time, a party who would have been prejudiced by disclosure being made by another firm has challenged the decision by the FSA to co-operate with an overseas regulator. Given the increase in requests from regulators for documents, the High Court's guidance is of assistance in determining whether a request should be met, or challenged. Following the decision, there appears to be considerable scope to challenge requests.

In *Amro International SA v FSA and Others*¹, Amro International SA (Amro) and Creon Management SA (Creon) challenged a FSA request for documents stemming from a request made by the SEC.

The request related to SEC investigations which started in 2002. Amro, a company incorporated in Panama, and Creon, incorporated in BVI, were financing companies (together the claimants). The claimants provided financing via a number of SPVs. A company called Rhino Advisers Incorporated (Rhino), registered in New York, and run by two brothers, Andreas and Thomas Bandian, provided investment advice to Creon and Amro.

The SEC began investigations into Rhino due to suspicions that Rhino had been manipulating shares through short selling. The SEC's investigations focused on one advance to a Pennsylvania company called Sedona in March 2001, which the SEC claimed financially benefitted Amro.

Proceedings brought against Thomas Bandian and Rhino were settled in 2003. In 2006, the SEC commenced proceedings against Andreas Bandian and six others. The SEC had been given a number of extensions of time within which to conclude their disclosure, which had resulted in a final extension being granted in February 2009, due to expire in August 2009.

Following consideration of evidence from a Mr Charron, it became apparent that the Bandian brothers may have had an interest in Amro and Creon. The SEC wanted to further investigate this interest and made a request to the FSA in July 2009 for documents held by Goodman Jones, Amro's and Creon's accountants in London. The request was for "*all documents that relate to Rhino, Amro and Creon and/or Special Purpose Vehicles, for the earlier of the dates of Amro's incorporation or January 1 2000*".

The FSA made initial enquiries about the request from the SEC, and then requested that Goodman Jones voluntarily produce the relevant documents. Goodman Jones refused, on the basis that they would need their clients' consent to produce the documents. The FSA then issued a demand to Goodman Jones under section 165 of the Financial Services and Markets Act 2000,

Footnotes

1 [2009] EWHC 2242

[Back to contents](#)

[Back to contents](#)

requiring them to produce the documents requested by the SEC. Amro and Creon commenced proceedings to challenge the demand on the basis that the notice was too wide and unspecific.

Mr Justice Collins concluded that the request for information was too wide, and should be limited to the SEC's pleaded case, concerning the Sedona transaction in March 2001. Documents relating to Creon and the SPVs were outside the scope of the request, as neither were named parties nor mentioned in the SEC's pleaded case.

Collins J referred to a number of factors which influenced his decision:

- The SEC had delayed in making its request for information. It appeared that the SEC knew of the facts which led to its disclosure request in April 2008, but it was not until July 2009 that it made the request to the FSA. The judge went as far as to say *"the SEC's actions have not been as speedy as they should have been and the FSA has been asked to help them pick up the pieces at the very last moment"*.
- Neither Amro or Creon were party to the US proceedings, and could not defend the allegations they faced. On this point the judge said *"if one looks at this from the point of view of a domestic court, it is questionable whether an application of this sort would be permitted if the claim had not been made and there was in effect no material other than possible suspicion which was relied on to justify the claim being made"*.
- However, the judge did recognise that co-operation between regulators was important, particularly given the financial climate, referring specifically to the IOSCO Multinational Memorandum of Understanding Concerning Consultation and Co-operation and the Exchange of Information.

The judge also provided some useful guidance for the FSA on what it should do when faced with a request from an overseas regulator:

- There was no obligation on the FSA to consult the claimants. At most it may have been appropriate, having sought the SEC's agreement, to ask for the claimants' consent. However, consideration should be given as to whether there is a risk of any dissipation, destruction or loss of documents if agreement is sought.
- The FSA is not under an obligation to question the SEC on the information it requests. The FSA is entitled to rely upon the information provided by an overseas regulator. However, in this case, where the FSA thought it right to make further enquiries, given the response it received, it was necessary to make additional enquiries in order to see precisely upon what the allegations against the claimants were based.

Permission to appeal has been granted. However, if the Court of Appeal upholds the High Court's decision, the scope of requests for documents will be substantially restricted, thus limiting the scope for regulators to make speculative requests.

[Back to contents](#)

Round-up

[Back to contents](#)



Audit firms providing non-audit services to listed companies

As part of its report entitled *"Banking Crisis: reforming corporate governance and pay in the City"*, the Treasury Select Committee asked for a review of the appropriateness of auditors providing non-audit services to the entities they audit. Its argument is that investor confidence and trust in audit would be enhanced by a prohibition on audit firms providing non-audit services to the same company. The Auditing Practices Board has issued a Consultation Paper providing the relevant background information and has requested views on this important issue. The email contact address at the APB is h.osullivan@frc-apb.org.uk

Oliver Hincks
+44 (0)20 3060 6347
oliver.hincks@rpc.co.uk

AADB publishes its final changes to its Accountancy Scheme

Following its Consultation Paper (reviewed in our Accountancy Update in March 2008), the Accountancy & Actuarial Discipline Board (AADB) has published its final proposed changes to its Accountancy Scheme. Some of the final provisions differ significantly to those originally proposed. Those that differ include:

- A change to when the tribunal may award costs against the AADB. Originally the tribunal were to have a discretion to award costs where there was found to be misfeasance by anyone associated with the investigation. The final proposal is that the tribunal may award costs where the AADB is found to have acted unreasonably (a much lower threshold test)
- A change to the definition of "misconduct". Originally this was to be changed to a very wide definition but following the responses to the Consultation Paper (including our own response), a narrower definition is proposed

The other key changes which remain as outlined in the Consultation Paper are:

- A two tier test to be applied before a matter proceeds to a disciplinary tribunal – an amended evidential test and a desirability test
- New procedures to appoint tribunal and appeal tribunal members by an independent convener
- A new power to conduct preliminary enquiries before making a decision to investigate
- Changes to the tribunal's voting arrangements

The Executive Counsel of the AADB, Cameron Scott, has also indicated that he intends to petition the Government for new powers which will force companies to co-operate with investigations. Many regulators, including the FSA, and the Solicitors Regulation Authority, already have statutory powers to demand co-operation and Mr Scott wants the AADB to be given similar powers.

Risk management lessons learned from the global banking crisis

The FSA has published a report by the senior supervisors from ten jurisdictions, including the FSA, the Securities and Exchange Commission and the Banque de France. The report was based



Round-up continued...

on interviews with firms and assessments of risk management practices against specific recommendations and observations. The weaknesses that were identified were:

- Failure of boards of directors to establish, measure and adhere to an acceptable level of risk
- Business models that depend too heavily on uninterrupted access to secured financing markets, often at excessively high leverage levels
- Remuneration policies and practices that conflict with the control objectives of the firm
- Inadequate technological infrastructures that prevent effective risk identification and measurement
- Institutional arrangements that confer status and influence on risk-takers at the expense of independent risk managers

Implementation of the Market Participants Group on promoting choice in the UK audit market

The FRC has published its fourth progress report on the implementation of the recommendations of the Market Participants Group. This is the first update since May 2009 and the progress achieved includes:

- The release by the Audit Firm Governance Working Party of a draft of best practice code on the governance of audit firms
- The publication of a summary of responses to the European Commission's consultation on audit firm ownership
- A new consultation on changes to Ethical Standards
- The publication of proposals for alternative business structures

Firm News

Welcome to Jonathan Levy

We are delighted to announce the addition of Jonathan Levy to the partnership, as the new Head of RPC's Tax Disputes Team. Jonathan has a wealth of experience, including a spell as Deputy Head of the International Tax Group at the Inland Revenue Solicitor's Office. He is recognised as a leader in his field by The Legal 500. Jonathan joins RPC from Berwin Leighton Paisner.

