

Model answers

Note: these are not meant to be definitive or comprehensive answers, nor are they legal advice. They are merely suggestions to stimulate discussion on the information security issues arising from the scenario described above.

1. Main information security concerns:

- The server was not properly sanitized by deleting all the personal data before it was disposed of
- This appears to be in breach of the UK's Data Protection Act
- While the former Graphic Data employee appears to be largely to blame for the incident, Graphic Data and the banks share responsibility
- How did the server come to be sold on eBay by a former employee and what has happened to the other missing computer?

2. Potential impacts on those involved:

The banks concerned	Graphic Data	Bank customers	Andrew Chapman	Former Graphic Data employee
Bad public relations leading to share price damage and lost business? Costs to investigate and resolve the specific incident, including updates to policies, procedures and other controls Dealing with irate and concerned customers Prosecution for breaching the Data Protection Act?	Same as the banks ... plus more serious commercial damage including likely defection of major corporate customers, and perhaps legal action by the banks	Privacy violation Identity theft Loss of trust in the banks	Positive public exposure by disclosing the incident Loss of the server to the Police if it is seized as evidence	Prosecution under the Data Protection Act and perhaps the Theft Act? Negative public exposure leading perhaps to shame and career damage

3. Potential banking executive response:

- First of all, the facts need to be clarified. The Police should be called in to gather evidence, investigate and establish exactly what happened, and most importantly to track down the second missing server.
- The relationship with Graphic Data is clearly in question. Hopefully, there was a legally-binding contractual commitment on GD to protect the bank's data from this and other kinds of security incident. The 'liabilities' section of the contract may well be enacted. The bank should seek legal and commercial advice on its position and options (e.g. is it still sending data to GD? Are there alternative service providers it could use instead? If it is already using other service providers, are those relationships covered by legally-binding contracts with suitable security and liability clauses?).
- Repairing damaged customer relations would be a commercial priority, along with cancelling and replacing the credit cards of those individuals whose data has been exposed etc.

Note: this case is based on a [news story](#) reported by the Daily Mail on 25th August 2008.