

ICO v Darren Hames & David Turley case summary

The complaint

The ICO received a complaint from T-mobile on 16 December 2008. They told us that customer contract renewal data (CRD) was being unlawfully obtained from their customer database by unknown person/s and was then being sold to mobile phone contract re-sellers.

T-Mobile's discovery

T-Mobile staff had for some time suspected that CRD was being disclosed from within the organisation, but they were unable to obtain any compelling evidence of this happening. In early 2008, a T-Mobile customer service manager temporarily replaced a customer's billing details with his own work details to prevent that customer receiving any bills while T-mobile processed a complaint.

In September 2008, the same customer service manager received an unsolicited letter addressed to him at the T-Mobile customer service centre. The letter contained his name, work address and the customer's mobile number - details which could only have come from T-Mobile's customer database. As T-Mobile do not sell on such data, it was clear that someone within the organisation was disclosing the data without consent. T Mobile reported the matter to the ICO and a criminal investigation was immediately instigated.

The ICO's investigation

The ICO's investigators contacted the organisations responsible for sending the marketing material – Chitter Chatter (CC) and Fone House (FH). They gave the ICO a list of data list brokers (organisations which specialise in providing lists of potential customers for specific markets) from whom they bought CRD.

FH and CC buy their lists of customers in data sets. These data sets are in essence spreadsheets with potential customers' names, mobile numbers, addresses and renewal dates. They can run to hundreds of thousands of personal records.

It quickly became apparent that these data sets were being manipulated by the data list brokers, making it possible to disguise the origin of the data by mixing lawfully obtained data - such as that obtained through opt in marketing - with data obtained unlawfully from other sources. This meant it was impossible to compare data supplied by FH and CC with T-Mobile's database.

This created a situation where the seeded data would re-occur in lots of data sets supplied by many different list brokers. Seeds were identified within the T-Mobile database (ten in total), which were used to identify list brokers with common sources of data.

Two of these list brokers - who had initially declined to assist, claiming commercial sensitivity - were served with demand for access notices. These are effectively search warrants with notice (as laid out in schedule 9 of the Data Protection Act). Once the notices were served, both organisations cooperated fully and identified multiple sources.

One of the list brokers - Open Source Research - identified a website called Afiliates4U, a social networking site used by individuals and organisations seeking and trading marketing lists. On searching through the website, the ICO's team found an individual who was offering T-mobile data which he claimed was unavailable from any other source. Further investigation revealed he was an employee of a data list broker who had featured heavily in the ICO's previous enquiries.

At this point the ICO's investigators felt that they were getting close to the source and decided that serving a demand for access - which would give the organisation seven days' notice of their intentions - could put the data at risk of being destroyed.

Therefore, two search warrants were obtained from a circuit judge at Chester Crown Court granting the ICO's investigators the power to enter and search two premises in the Rochester area of Kent. One was the home of the individual who had advertised on the Afiliates4U website, and the other was his employer's commercial premises.

On 23 April 2009 Kent Police - together with the ICO's investigators and a specialist digital imaging team - executed both warrants simultaneously. The individual's home address didn't provide any further evidence and in interview he admitted to "buying in" the data from the internet and fabricating the claim he made that he could obtain previously unused data.

The business, a multi faceted marketing business, admitted to trading in T-mobile data with a database of some 17 million records. They provided evidence of contracts and bona fide business practices indicating they were innocent purchasers buying data in good faith. The business also informed the ICO that they hadn't bought or sold a great deal of T-Mobile data recently but when they had it was only from one source. They identified this source as Peter Sharp of Up Front Data Limited, based in Rochdale.

Again, two search warrants were obtained and on 18 June 2009 the business premises and home address of Mr Sharp were searched. Mr Sharp was located at his home address and would not answer the door which had to be forced in the presence of the police. Mr Sharp was found hiding in his bedroom; a laptop computer was recovered on which significant evidence of trading in T-Mobile data was found. Mr Sharp in interview identified his source as being David Turley of Direct Mobile UK Limited.

T-mobile's investigator immediately recognised Mr Turley's name and confirmed that he was a former sales manager for the company.

Direct Mobile UK Limited was traced to a residential address in Birmingham City Centre, which records indicated was also Mr Turley's home address. Again a search warrant was obtained. On this occasion it transpired the property was let although Mr Turley still received post at the address. Within 10 minutes of leaving the address Mr Turley contacted the ICO's investigators and agreed to be interviewed.

The investigators interviewed Mr Turley on 1 September 2009 in Birmingham; once presented with the evidence against him he admitted buying T-Mobile contract data from a T-Mobile employee who he named as Darren Hames.

He said he would meet Hames once a month in a public place such as Mcdonalds, and Hames would upload data from a memory stick onto his laptop, for which he was paid in cash. Records later indicated the cash payments as being anything from £2,000 to £5,000 per meeting.

The following day investigators interviewed Darren Hames at the T-Mobile HQ in Hatfield. Once presented with the evidence and Mr Turley's confession, Mr Hames freely admitted his part in the offence.

Unfortunately the ICO is unable to describe in any detail how Hames obtained the data as this information would be potentially damaging to both T-Mobile and other mobile phone service providers.

Outcome

Both Mr Hames and Mr Turley were interviewed under caution. Both defendants in interview admitted that they had unlawfully obtained and sold T-Mobile customer contract renewal data for profit.

Mr Turley was the director of several companies specialising in the sale of marketing data and, more importantly, was a former sales manager for T-Mobile. It is the prosecution case that Mr Turley realised the value of customer contract renewal data and, after he left the employment of T-Mobile, approached a former colleague, Mr Hames, about obtaining this data from T-Mobile. Mr Hames was still employed by T-Mobile at the time of the offences as a sales manager for the West Midlands area.

The prosecution contends that the number of T-Mobile customer records obtained by Hames from the T-Mobile database was 556,355 and that he sold batches of 20 – 30,000 of these records at a time, on at least eight occasions within a 12 month period. Mr Hames admitted in interview that Mr Turley paid him approximately £30,000 for this data.

Mr Turley stated in interview that he then sold the data on for double the price paid to Mr Hames, (20 pence a record as opposed to the 10 pence per record paid). It is the prosecution case that Turley made approximately £60,000 from dealing in the T-Mobile data during the course of a year.

In December 2008 the defendants met and agreed to cease their activity. As a result of these offences T-Mobile has suffered financially through lost customers. It is unable to quantify the amount.

Mr Hames was subject to a clause in his employment contract which prevented him from using or exploiting for any purpose the confidential information controlled by T-Mobile such as customer data. Therefore Mr Hames was breaching his contract of employment in unlawfully obtaining, disclosing and selling the data.

Mr Hames was committed to Chester Crown Court for offences under section 55 of the Data Protection Act 1998, that between 6 December 2007 and 5 December 2008 he obtained personal data

without the data controller's consent, and sold that data on to Mr Turley. He indicated at the Plea and Case Management Hearing that he was going to challenge the prosecution evidence, therefore a four day trial was listed for 23 November 2010. However on the day of the trial Mr Hames changed his plea to guilty. Sentence was adjourned as the prosecution had commenced confiscation proceedings under the Proceeds of Crime Act 2002.

Mr Turley was committed to Chester Crown Court on 18 counts of committing offences under section 55 of the Data Protection Act 1998, between December 2007 and 5 June 2009 for obtaining personal data from Mr Hames without the data controller's consent, and selling that data, trading as Direct Mobile, on to a third party. At the Plea and Case Management Hearing on 22 July 2010 he pleaded guilty to all counts and his sentence was adjourned until the conclusion of Mr Hames' trial and for Proceeds of Crime Act proceedings to take place.

The final confiscation hearing and sentencing is listed for 10 June 2011.

Background

The T-mobile customer database is made up of both contracted and pay as you talk (PAYT) customers. This matter concerns only contracted customers who are usually tied to a contract of between twelve and eighteen months duration. At the expiry of the contract the customer has several options:

- 1) to continue with the existing contract;
- 2) to renegotiate a new contract with their existing service provider;
- 3) to change service provider; or
- 4) to renew the contract through a third party or reseller.

The mobile phone market in the UK is saturated. Recent figures suggest there are 40 million adult mobile phone users already in existence, making the acquisition of new customers extremely difficult. This in turn has created a cut throat market situation with telephone service providers paying contract resellers up to £250 in commission for a new contract, even if that new contract is an existing customer.

Resellers are attracting new customers by targeted aggressive marketing such as unsolicited mail shots and cold calling via their

existing mobile phone number. This kind of marketing is only productive if it is delivered shortly before the expiry date of the existing contract. Therefore the customer name, address, mobile phone number and especially the contract renewal date are vital. The demand for such data has created a lucrative CRD market. As you would expect, the telephone service providers, notwithstanding their data protection obligations, are extremely protective of such customer data due to its obvious commercial value.

Some customer data is legitimately available and can be obtained via marketing surveys; however, this data does not always contain contract renewal data and is often inaccurate when compared to data obtained from the TSPs.