Operation BOWLER

Summary of 'mystery shopping' exercise conducted to identify organisations using consumer data to send unsolicited communications

Intelligence Hub – Enforcement February 2016

Background

Operation BOWLER was a proactive, intelligence-gathering exercise. The Operation aimed to identify organisations using consumer data to send unsolicited communications (calls or text messages), and identify organisations potentially breaching the Privacy and Electronic Communications Regulations 2003 (PECR) and/or Data Protection Act 1998 (DPA)

We recently produced a video to demonstrate how personal data being collected and passed between companies may lead to individual being inundated by unsolicited communications. The aim of Operation BOWLER was to replicate the consumer experience, from entering competitions, and completing surveys through to responding to charity appeals. We then kept track of any contact received.

Methodology and limitations

We used 18 basic mobile phones and seeded the telephone numbers with various organisations. 15 of the numbers were seeded on websites, and 3 in response to TV advertising campaigns. The websites selected included survey sites, free prize draws, free offer sites and competition sites. We registered 14 numbers with the Telephone Preference Service. Corresponding email addresses were set up for each mobile telephone. In some cases consent for marketing was provided, and in other cases consent was not given.

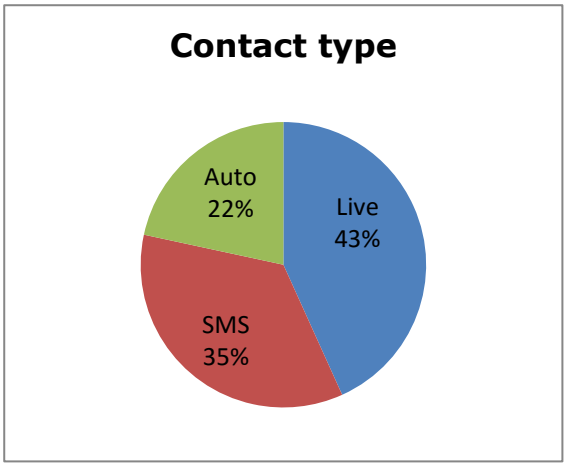
Mobile phones were answered and basic information provided if asked (for example, the officer's first name, the linked email address and our office address). However, staff would not sign-up for products or services. Email inboxes were checked at least weekly. Privacy policies or all websites and associated companies were reviewed and retained.

The Operation ran from April to September 2015. It's important to note that this was a relatively short project. Personal data can exist in a 'data cycle' for at least a decade so, in real-life, individuals may receive many more calls and messages than we did, as numbers may be used in many places over a much longer period of time.

It is also important to note that, as mobile numbers are re-used we are unable to determine whether or not the contact we have received is a direct result of our seeding, unless one of our identifiers is used.

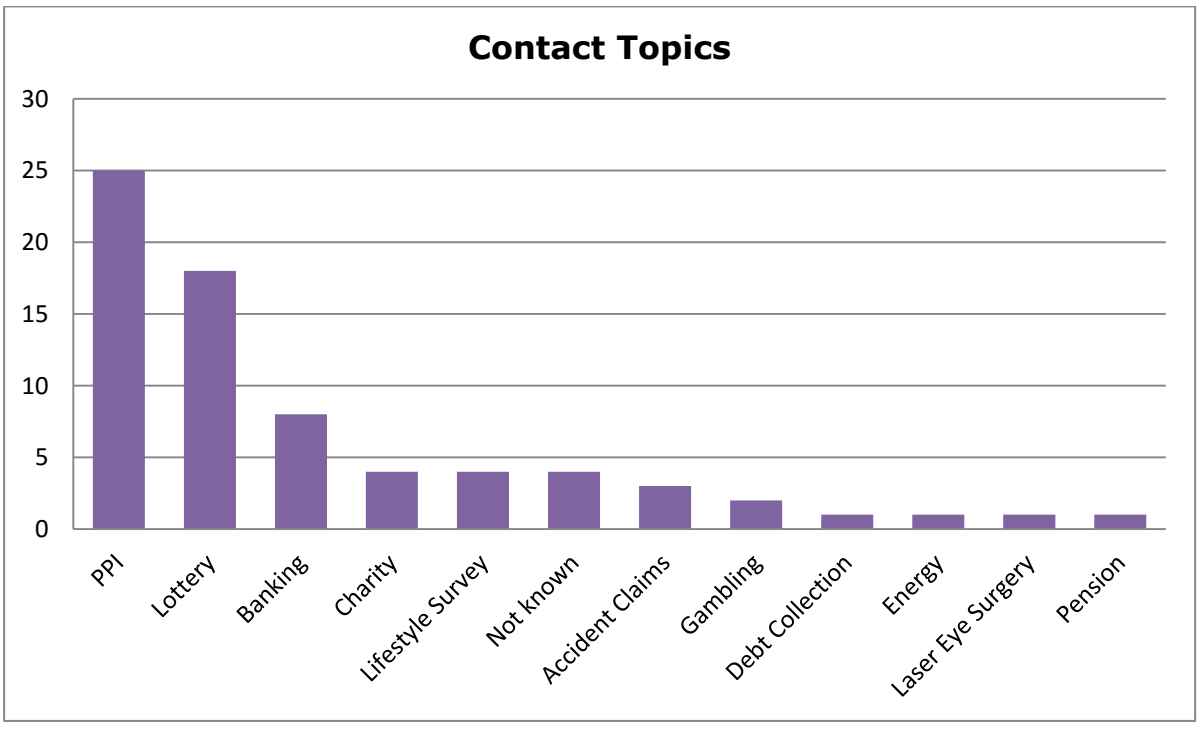
Communications received

We received 32 live calls, 26 text messages and 16 automated calls. These figures do include some missed calls, whereby the contact type has been established by checking the number against numbers reported as concerns to the ICO. These figures do not include the calls and messages received from the mobile networks (in relation to the accounts set up).



Some of the mobile phones didn't receive any contact, whereas one of the phones received 20 contacts alone. This phone wasn't registered with the Telephone Preference Service, and it's important to note that not all of these contacts will have breached PECR.

Some topics of contact received are as you would expect from the concerns reported to the ICO.



We received more contact in relation to lotteries than we would expect, based on concerns received. Across three phones we received seven calls and 11 text messages offering lotteries.

We also received more contact in relation to charities than we would expect based on concerns received. However, this is likely due to our action in seeding numbers in this area.

Four lifestyle survey calls were received. These calls would have likely led to even more contact had we responded to them.

Where we spoke to organisations, we asked them where they had obtained our data from. Answers provided include:

- Recent online survey or completion but couldn't say which one;
- Opted in database for PPI;
- 'Various sources';
- Government have provided a PPI reclaim list as they want to ensure that all who are eligible claim back what they are due;
- PPI linked to mobile numbers and our number was on opted database;
- National databases; and
- Not known.

The lack of transparency as to where data has been obtained is a significant concern.

Outcomes and next steps

The project has led to a number of intelligence and investigative opportunities.

We have been able to corroborate numbers identified in concerns reported to the ICO and also used those contacts to our phones to identify numbers. The intelligence collected has been fed into our investigations.

The work helps us develop our understanding of how lead generation companies operate, enabling us to focus our enforcement and preventative activity accordingly. Updates on this activity are published monthly.

Last month (January 2016) we launched a second stage of this project, with a similar methodology. We will use the intelligence this generates as above and update on this activity via our website.