The Direct Marketing Commission

Enforcing Higher Industry Standards

Annual Report

2014/2015

About The Direct Marketing Commision

The Direct Marketing Commission (DMC) is the body which enforces the DMA Code and forms part of, and is funded by the Association and the Advertising Standards Board of Finance (ASBOF). The DMA Code and DMC are established to give effective protection to recipients, users and practitioners of one-to-one marketing, ensuring that companies observe high standards of integrity and trade fairly with their customers and with each other. This is processed through the investigation of complaints, direct marketing issues and practices, and providing guidance to consumers. The DMC and DMA have also recognised the potential value of shared research or other action to build marketing understanding, awareness of industry standards and compliance.

The DMC comprises an independent Chief Commissioner, two independent Commissioners and two industry Commissioners. Independent Commissioners serve on a paid basis and industry Commissioners serve on a voluntary basis. Decisions which relate to the adjudication of complaints about a member of the DMA are taken independently by the DMC and its decisions are final. Where the DMC concludes that a member is in breach of the Code the member is entitled to appeal against the ruling. The DMC's current Appeals Commissioner is John Bridgeman CBE TD, who is appointed by the Board of the DMA.

The DMC will address any complaints against DMA members where the complaint is within the scope of the DMA Code. If the complaint is not covered by the Code, it is referred to another relevant organisation. The Secretariat of the DMC aims to confirm receipt of all complaints within two working days and aims to achieve at least 65% satisfaction levels with the action taken by the DMC in relation to cases dealt with by formal or informal procedures. Every complainant is informed of the action taken and/or the outcome of investigations. In addition, the DMC aims to complete 80% of formal adjudications within three months of the first dialogue with a DMA member or any other party and register and progress complaints within seven working days. The DMC aims to have no cases reversed after action by the Independent Appeals Commissioner and no successful judicial reviews or legal challenges, and makes available key trend information on complaints as required.

Minutes of the DMC Board meetings are published on the DMC website.

About the Commissioners

George Kidd: (Chief Commissioner)

In addition to his role at the Direct Marketing Commission, George is a Board member of the Council for Licensed Conveyancers, Chair of the UK Public Affairs Council and Chief Executive of the Online Dating Association. George was formerly Chief Executive of PhonepayPlus, the national regulatory body for the 'premium-rate' phone-pay phone content market and a Director in the Cabinet Office responsible for regulatory policy and practices. He served as British Consul in Chicago for five years and his earlier career was with the Trade and Industry Department, mostly on international trade matters.

Dr Simon Davey: (independent member)

Simon runs independent management consultancy Omega Alpha, working with organisations as a Change Leader to optimise processes and change cultures, bottom up and top down, to achieve better social and economic returns.

He has developed and led educational programmes including Emerging Scholars (ESIP) and has a long history of work with disadvantaged young people. His work with charities focuses on the ethical and effective application of data and information management for social outcomes.

Rosaleen Hubbard: (independent member)

Rosaleen Hubbard is the founder and Senior Partner of Towerhouse Consulting LLP, a law firm specialising in the provision of legal and policy advice to business and regulated sectors. She is named by Who's Who Legal as one of the UK's leading telecoms regulatory lawyers.

Rosaleen has a particular interest in consumer policy. She was a founding Council member of The Ombudsman Service. She is a graduate of the Aston School of Business and qualified as a solicitor in 1986.

David Coupe: (industry member)

David Coupe has had a 25-year career at global information services company Experian. He joined in 1983 as an Account Manager and became Managing Director for the UK in 1995 and Managing Director of International Marketing Services in 2002. David is a Fellow of the Institute of Direct Marketing, and a former Chairman of the DMA from 2003 to 2005. He is now a Non-Executive Director of data governance specialists DQM Group, and a Trustee of the DM Trust Ltd.

Danny Meadows-Klue: (industry member)

Danny Meadows-Klue is Chief Executive of the Digital Strategy Consulting group, President of the Digital Training Academy. He founded the IAB digital association in the UK, and was chairman or CEO for a decade, helping launch and develop it in more than 20 countries. As publisher of the UK's first online newspaper (Telegraph.co.uk), he helped launch dozens of online magazines before moving to NBC as a VP for digital content and products. He led in building the initial standards and frameworks for digital marketing self-regulation, and advised government departments on policies to help grow the digital economy. As an accomplished writer and broadcaster he has been an active commentator on the digital marketing industry for over 20 years and has lectured on digital strategy in more than 50 countries at universities, as well as through the www.DigitalTrainingAcademy.com marketing coaching group. Through Digital Strategy Consulting, he helps organisations like Unilever create their digital strategies and drive digital transformation.

Chief Commissioner's Report

I am pleased to introduce our 2014/5 Annual Report.

Sad and high profile examples in the charity sector of people receiving hundreds of marketing calls, mails and contacts have shone light on what can happen when cold-callers, websites and others ask for our consent to marketing.

We report this year on a number of cases with shared characteristics and on how these can result in consumer anger or more serious outcomes. Again and again we have seen cases where members of the public have given some form of consent to their personal information being shared for marketing purposes, where their data was then sold or rented on through various data brokers followed by marketing approaches and cold-calls, e-mails or texts from businesses or charities they do not know and did not expect to hear from.

We try to unpick what happened, dissect events and see where things go wrong. This is an important part of what we do if we are to make a real difference in terms of making sure marketing messages and offers are relevant and not an unexpected and unwanted intrusion.

There is a need to look beyond data-files and the ways in which technologies make millions of calls, texts and mails possible and to understand the frustration and upset that marketing calls in particular can have on individuals, particularly those of us who might not understand how these calls come about and how they can be vulnerable to sales pitches or requests to share more information. We try to address both sides of the matter in our investigations. In past reports and elsewhere in this document we refer to "data journeys" - the ways in which the data we share travels through lead generation companies, brokers and agents highlights where and why things can go wrong.

The journeys generally start with some process of persuading the public to give consent to marketing. The consent can be obtained on websites where users are on-line for other reasons – to enter a competition, to buy travel tickets or to search for an insurance deal. People doing these things are unlikely to be aware that they are giving their consent to their data being sold on to third parties. They did not go on-line with this in mind.

The same can happen with lifestyle surveys and other 'research-type' calls where the core aim is to obtain people's permission for further calls from the companies who fund the surveys. The calls often come from sub-contract or affiliate businesses overseas. Millions of calls are made every year to people on the Telephone Preference Service based on some consent the call recipient might or might not have given in surveys five or ten years ago, even though the people called have never picked-up or taken part in a survey since that time. In other cases we have seen offshore call centres calling UK numbers that are TPS registered either on the basis they are not bound by UK laws or based on the claim, which we reject, that the calls are 'research' and not made for marketing purposes.

In some cases we saw what felt like sensitive personal data about health or incomes sold on without the seller or buyers giving careful thought as to how their marketing could anger or scare people in terms of the information held on them.

It's simply not good enough to blur or hide important messages about the consents being taken. Consent is something people give, not something that is taken.

It's simply not good enough for UK businesses to use offshore call centres who are not going to respect people's express wish not to receive unsolicited calls.

And it's simply not good enough for people to buy and sell data if they have no means of satisfying themselves that the people involved have given consent for their information to be shared in the way proposed. 'Data' is not just some aggregated and anonymised package of information. It is personal information on individual members of the public and needs to be treated accordingly.

We made this clear in a number of adjudications during the year. But we saw a need to go beyond addressing the behaviours of individual businesses and look at whether their practices were really different from what has become normal when businesses are looking to generate leads, secure consents and sell data. It has led us to a number of headline messages shared with the DMA.

We say lifestyle survey calls are direct marketing calls and that they cannot be made to TPS registrants unless the caller has agreed to calls from that business.

We say we do not believe it is consistent with privacy laws or reasonable from a consumer point of view to keep attempting calls years after consent was given if there has been no contact. Our starting point is that lifestyle companies must make real contact and refresh consent within a year or stop calling people on the TPS.

We say those who buy and sell data as brokers and intermediaries are responsible if the data they trade does not have the necessary consents. It is not good enough for a broker to say they bought and sold in good faith or that they could not check and could not assume responsibilities because of confidentiality clauses set by others. The DMA Code says members are responsible for the proper sourcing, consents and cleansing of the data they trade. The Code also says members are responsible for the actions of suppliers, sub-contractors and affiliates. We want to make clear we will apply these rules as a package. We are likely to see it as a serious breach of the DMA Code if things go wrong and members tell us they simply relied on the assurances of others that consent had been given for the use of data, but did nothing to check that this was true.

We say there is need for far greater clarity when seeking people's agreement that their data can be shared. As said, consent should be asked for, not taken.

We say data professionals should act and be treated accordingly - no-one should breach data and privacy rules but businesses that specialise in collecting, processing and selling should know how to do this properly. No system or process is totally incident-proof but there is little excuse when those who work in data do not understand or follow the rules.

These are things we can address case-by-case if that is necessary but we have been delighted to see how the DMA has responded to our findings and the ways in which they are working to build awareness, compliance and public trust.

Complaints History

This year, we recorded 262 complaints made against businesses operating in the direct marketing arena. Out of this number, the Commission Secretariat examined 48 consumer complaints and 12 business-to-business complaints which involved members of the DMA. Complaints which appeared within the remit of other statutory or self-regulatory bodies were referred to these bodies wherever appropriate.

When we investigate complaints, we follow established procedures to ensure that we look at each case fairly and proportionately. We look at whether there are possible breaches of the DMA Code and if so, whether or not the issue concerned is specific to the individual complainant or perhaps a symptom of a wider and more systemic problem. When we find serious breaches of the Code, repeated breaches or ongoing complaints against a business, we will progress towards a formal investigation. Where we see an issue that may have a significant impact on other consumers, we may take formal action even if we have received very few or perhaps only a single complaint. We aim to provide the DMA with feedback on our findings if it seems the problems we were seeing may have become common practice, where there may be a case for changes in DMA membership or compliance activity and where the DMA could use its ability to give wide distribution to messages about Code compliance and how the Commission is interpreting the DMA Code.

During this period the Daily Mail ran a number of articles on businesses involved in the buying and selling of data, including allegedly sensitive financial (pension) and medical data. The article highlighted the problems of data supply chains where personal data is traded without thought to the permissions, source and cleanliness of the data.

During the year in question, the Commission Board formally investigated five businesses and found two in breach of the DMA Code. Each case threw up issues that affect many or all of those in the market and the general public, not just those who brought complaints to us.

Harvesting consents

In one of the cases, this was as a result of the newspaper allegations referred to in the above paragraph. The business ceased to trade shortly after publication of the article but we proceeded with an adjudication and published the outcome on the Commission website. The business is no longer in membership of the DMA in any form. The DMA had asked the Commission to consider the circumstances around the buying and selling of alleged sensitive financial data by the company. The company had co-operated with our enquiries, but they were unable or unwilling to disclose the sources of the data supplied to them and though they provided a number of sample consent forms from their data suppliers, many of these were found to be vague and not compliant with regulatory guidance. Many of the suppliers were web businesses offering price comparison and "find-a-quote" services for insurance services. Those online would have had no reason to assume they were being "asked" to give consent to the re-sale of their data. In some cases the suppliers were running web based services where anyone using the service had, in effect, to give consent to their data being shared with third parties simply and automatically by virtue of being on the site. These businesses are outside of DMA membership but the DMA members using them have a responsibility for their behaviour. It was not acceptable for the DMA member to buy and use data without knowing whether it had been obtained honestly or through confusion or deception.

Additionally, there was insufficient evidence to substantiate the company's claim that they did screen their data every 28 days against the Telephone Preference Service as claimed and as required in the DMA Code. Commissioners therefore upheld a breach of the Code rule 3.11 which states when buying or renting personal data, members must satisfy themselves that the data has been properly sourced, permissioned and cleaned. In this case the member company breached parallel requirements: failing to ensure their data suppliers provided adequate consent and for not substantiating that they had checked this data against the TPS before offering it to third parties.

> **Your pension secrets sold to conmen for five pence: On eve of pensions revolution, an exposé that will horrify every family in the land**

Data and its sensitivities

In another case which was prompted by national newspaper attention the Commission had to consider the sourcing and uses of what the press alleged to be sensitive medical data. The company had co-operated fully with the DMC and explained their due diligence arrangements in relation to their customers. The company provided information making clear they did not seek or offer information that might be described as "medical records".

The Commission did not find evidence that the company's actions and processes had breached rules of the DMA.

But the investigation did highlight some issues around their relationship with their data suppliers, and lessons in terms of how best to deal with data that might be considered sensitive from a consumer's point of view. It would be worrying if data suppliers and brokers were blind to and indifferent to what is to be done with the data they supply. This care should go beyond what is formally defined as sensitive personal information and into some broader care over what can and cannot be done with the data supplied.

After Mail exposes trade in sensitive pension details... Now they are selling your health secrets

Is secrecy making compliance harder and putting honest traders at risk?

In the two investigations prompted by media reporting the Commission was concerned that confidentiality agreements between the broker and its suppliers meant that they could not reveal or may not know the actual source of the data they were buying and then selling on. Whilst one company used reliable and trusted suppliers and undertook due diligence on the data they bought and sold, in an extended value chain this was a worry as it meant there was a limit as to the assurances that could be given to buyers on the provenance of the data. In the other case the company knew where the data was coming from but did nothing to make sure it was coming to them with the consents necessary for it to be tradeable. DMA members are responsible for the actions of their suppliers when it comes to sourcing data and securing the necessary permissions for its use. This might seem tough on brokers who may be smallish intermediaries sitting between data sources and those who ask their broker to supply data for a campaign. But this responsibility cannot be set aside. This highlights the critical importance of brokers exercising real due diligence over who they are prepared to buy from and sell to.

Managing users and playing fair when services move on-line

In a case raised earlier in this financial year, we received a complaint from a consumer who had unwittingly signed up over two years previously to membership of a discount club. The complainant's membership fee had risen substantially in the second year of membership seemingly without notification. The Commissioners considered whether the company was complying with rules regarding the clarity of the sign up process which was conducted over the telephone, the ongoing renewal process, and their customer service. The Commission concluded the company's arrangements were not fair and reasonable and upheld a breach of Clause 3.21 of the fourth edition of the DMA Code. The particular worry was that the company had moved from a mail delivery subscription service to an online service. In the process it had failed to see the importance of engaging with existing customers and their rights to fair notice of price changes and changes in the offering while focusing on the new on-line clientele.

Claims management prospecting

We also investigated a claims management business in the light of a penalty imposed by the regulator for calls about PPI claims made to registrants on the Telephone Preference Service. Whilst we had not received complaints from individuals at the Commission, it was clear that the business had been the subject of TPS complaints for some time. It was also clear that due diligence had not been carried out adequately on its suppliers and introducers and the member had not taken responsibility for those providers.

The Commissioners believed that the reputation of one to one marketing and claims management businesses had been damaged by the collective action of claims management businesses in blanket-calling the public or allowing their sub-contract lead-generation suppliers to do so, but that the individual member company had belatedly accepted its responsibility for marketing calls made by their introducers. The Commission looked at the relevance of its previous adjudications on member companies that had or had not been the subject of regulator action and considered the scale and nature of those wrongdoings and whether the companies took mitigating action; they also took into account the changes the company had made to its management and organisational structure and its data supply arrangements. The member company committed to a programme of reforms and to review these with the DMA compliance team and submit a report in six months of any ongoing TPS complaints, remedial actions and future plans. At an industry level the challenge is to make all businesses understand their liability for the behaviour of their suppliers and to take effective enforcement action to make this happen.

When do consents pass their "use-by" date?

We investigated a member in the lead generation/ lifestyle survey sector. There had been a formal

investigation a year earlier following complaints to the DMC and Telephone Preference Service, and complaints to the TPS had vastly reduced since that time. Further concerns had been raised in relation to the clarity and nature of consents, persistence of calls and suppression procedures and these had been fully addressed. An outstanding concern, however, was the question of 'ageing consent' where consumers may have opted-in some years previously but had not completed a survey in the intervening years, though contact by the company had been attempted. Whilst the member understood that the regulatory guidance was now stricter they believed they were not breaching regulations, as they were only calling consumers who had 'not' opted-out.

Regulatory guidance states, however, that whilst there is no fixed time limit after which consent automatically expires, companies should look at whether it is still reasonable to treat the consent as an ongoing indication of the person's current wishes. This general guidance relating to a consent to an entity and its marketing material feels quite different to an aged consent, not to marketing, but to being surveyed to facilitate marketing.

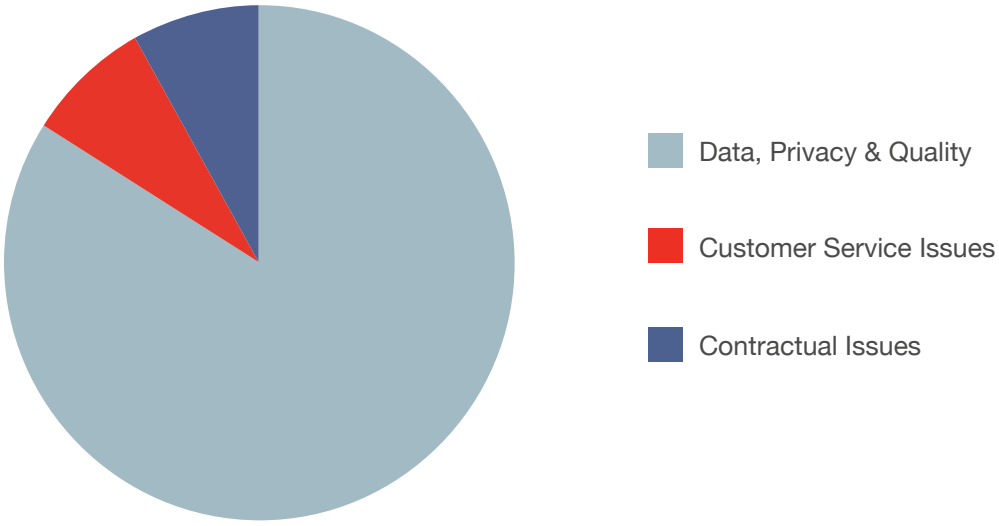
The specific case was closed based on undertakings from the member to review compliance arrangements.

When to accept no means no?

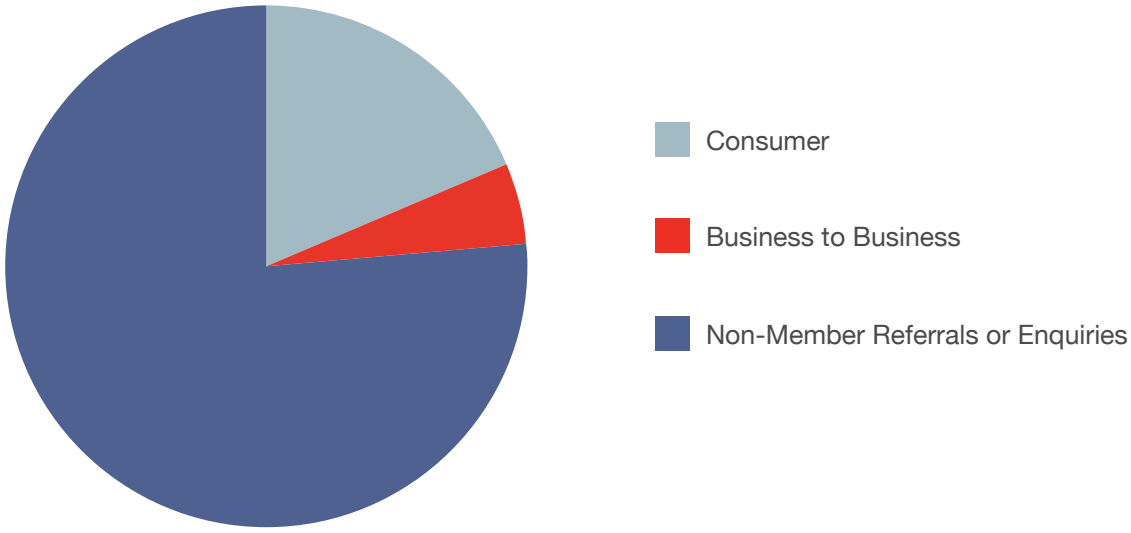
The company was advised to give serious thought to the types of responses received and how these were recorded in terms of Call or Do Not Call listings as we saw no value to the sector and only reputational damage to the community if "leave us alone" and "we are too busy for this nonsense" type responses were not accepted as the removal of consent to call simply because the recipients did not explicitly refer to removal from a list. This too is an issue that the sector has to address across the board: pressing a leading player to improve its practice might cut out millions of "nuisance calls" but more can be done.

Complaint Statistics

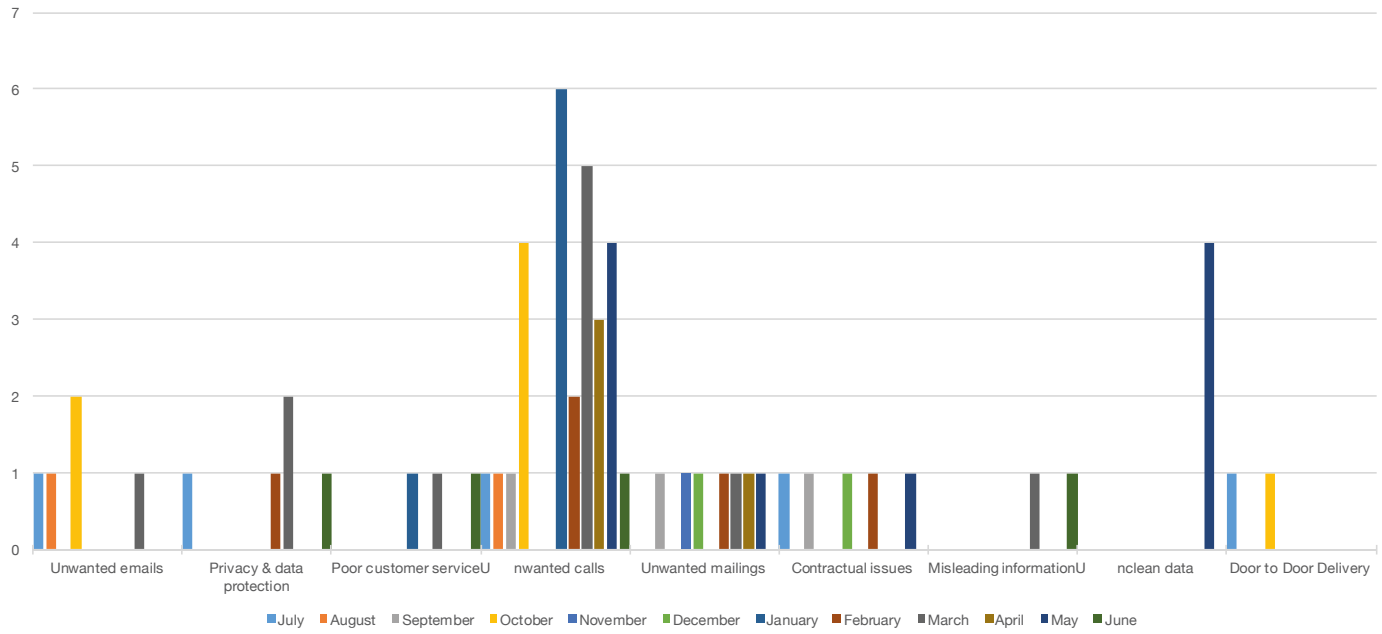
General Nature of Complaints (DMA members)
1st July 2014 – 30th June 2015



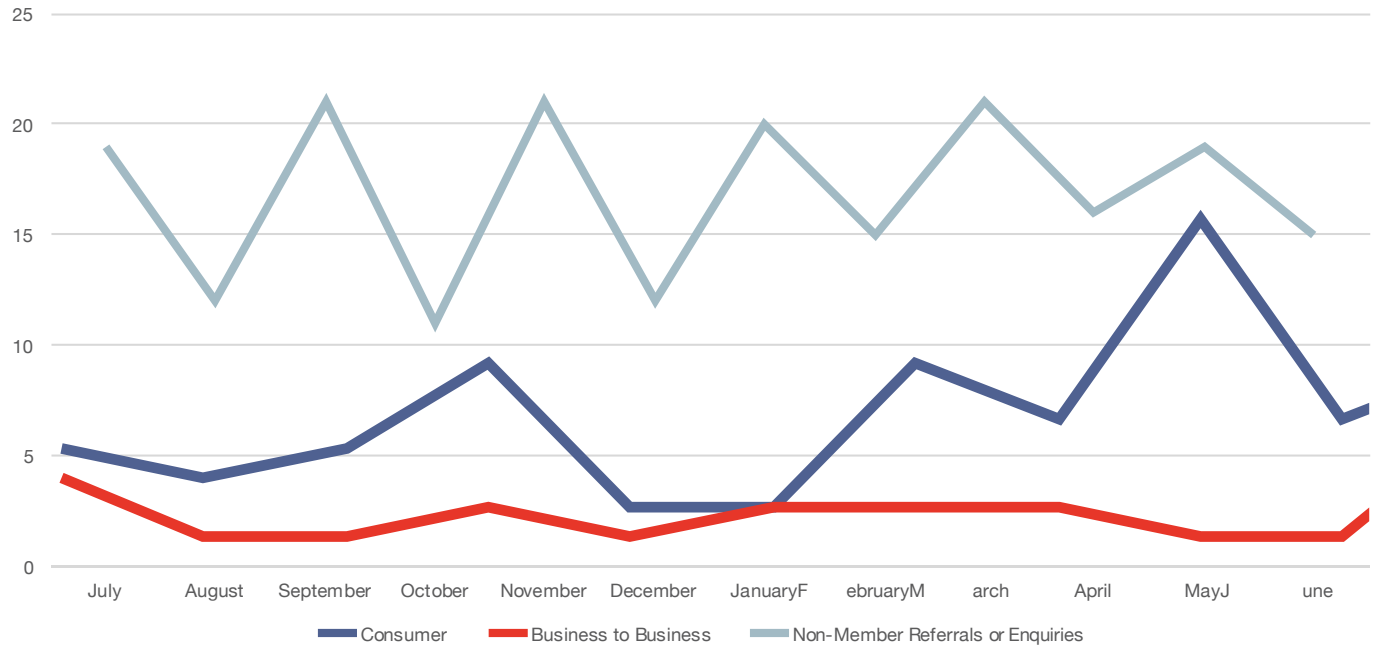
Number of Complaints
1st July 2014 – 30th June 2015



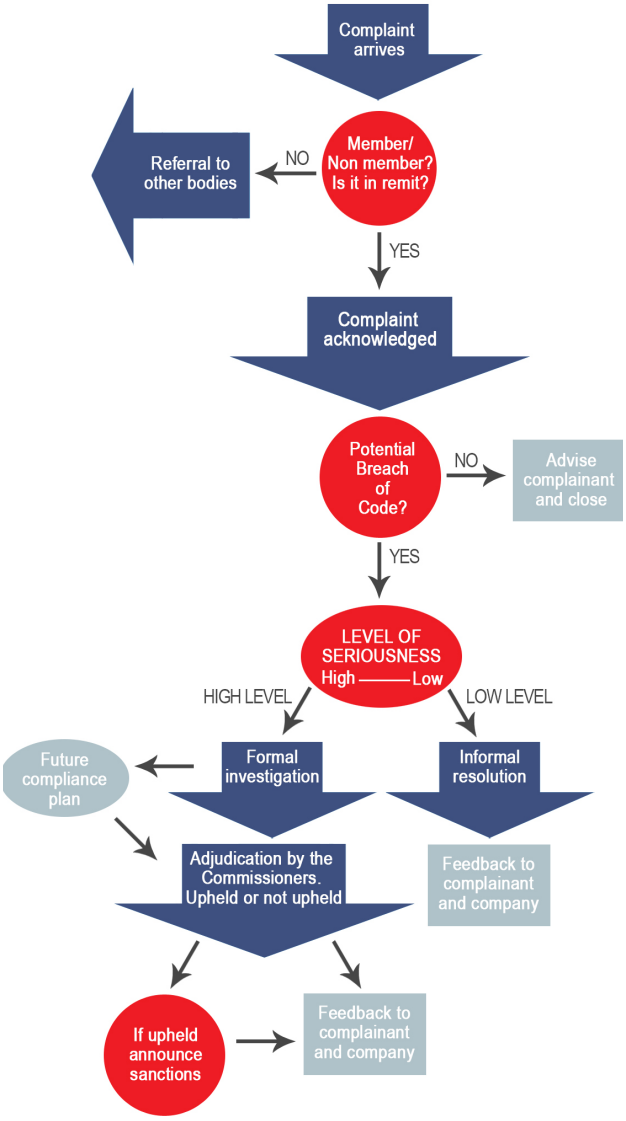
Nature of Complaints (DMA members only)
1st July 2014 – 30th June 2015



Monthly Complaints
1st July 2014 – 30th June 2015



The Complaint Process



The DMA Code Principles

Put your customer first
Value your customer, understand their needs and offer relevant products and services

Respect privacy
Act in accordance with your customer's expectations

Be honest and fair
Be honest, fair and transparent throughout your business

Be diligent with data
Treat your customer's personal data with the utmost care and respect

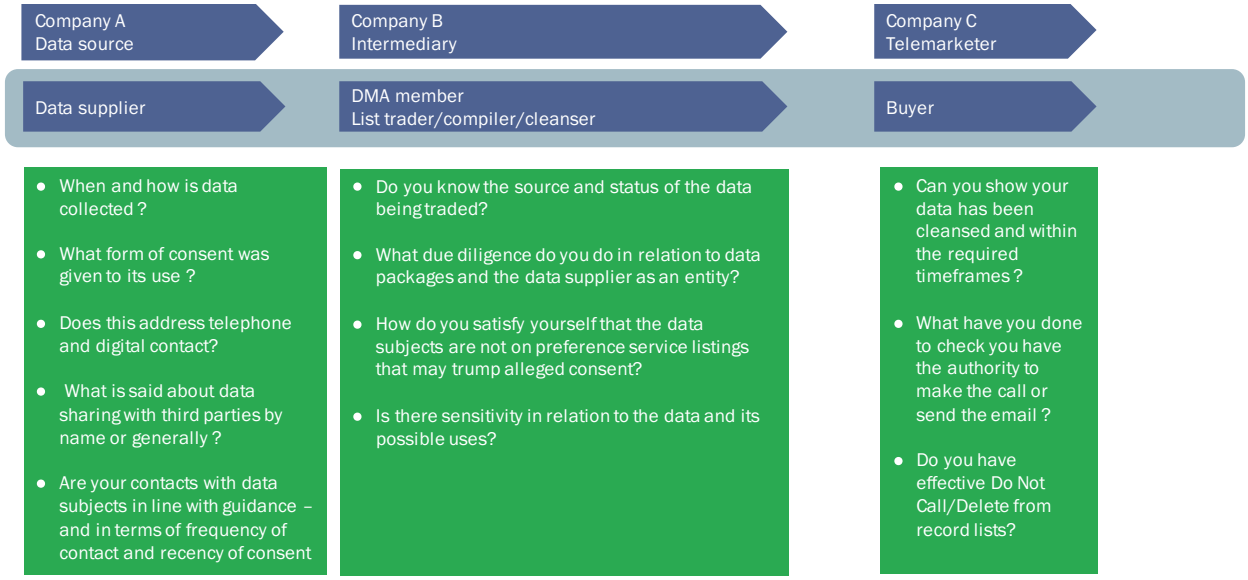
Take responsibility
Act responsibly at all times and honour your accountability

Understanding the Data Journey

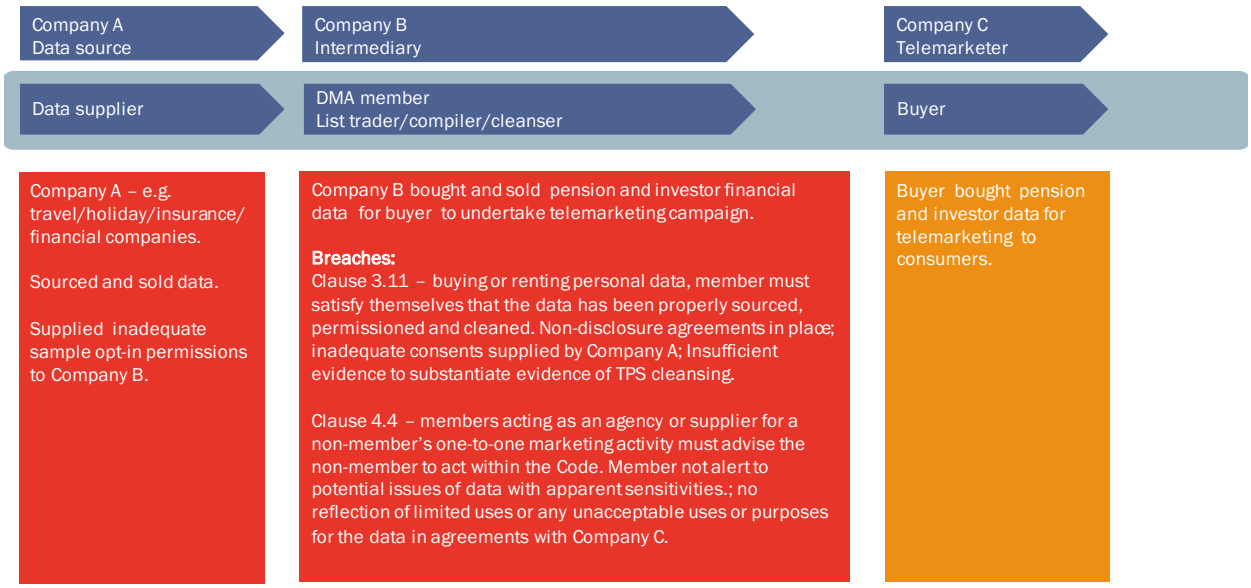
A data journey is the path travelled by a consumer's data throughout its use. Visualising the data journey allows us to see how data has moved from one step to another. We can signpost different clauses or possible breaches at each step to help identify problems.

There is a need to look beyond the behaviour of the single party against which a complaint has been made and instead understand the whole process. By understanding how someone's data is obtained and looking at how the data is added to, bundled and sold on, we can understand why and when we get calls, e-mails and other marketing messages from unexpected sources.

There are common steps in the journey of a consumer record throughout its use. Below is an example of what a data journey might look like and the types of questions we may ask at each step. We can then clearly identify different causes and possible breaches at each stage in the journey.



Here is an example of a data journey. Signposting possible breaches at each step helps to identify the relevant areas of concern.



Direct Marketing Commission
Registered Number: 6469055
Registered Office: 70 Margaret Street, London, W1W 8SS
Telephone: 020 7291 3350
Email: dm@dmcommission.com
Web: www.dmcommission.com