Ministry of Justice

# Claims Management Regulation
# Special Bulletin: Direct Marketing
May 2014

**Tackling non-compliance relating to direct marketing is a key priority for the Claims Management Regulator ("CMR").**

We have recently increased our compliance resource and we are undertaking more risk based marketing audits to identify, stop and prevent bad practice.

The CMR also works closely with the Information Commissioner's Office ("ICO") and the Office of Communications ("Ofcom"), who remain the primary regulators in this area. This involves sharing intelligence to target, investigate and take firm enforcement action against claims management companies ("CMCs") engaged in non-compliant direct marketing.

This bulletin has been published to coincide with the recent enforcement activity by the ICO on direct marketing involving CMCs. It highlights common issues recently identified with some CMCs who direct market, and contains guidance on compliance with the conditions of authorisation.

## In this issue...



## Live marketing calls

If you make live telesales calls, regulation 21 of The Privacy and Electronic Communication (EC Directive) Regulations 2003 ("PECR") requires you to screen your data against the Telephone Preference Service ("TPS") register, unless the consumer has notified you that, for the time being, they do not object to receiving calls.

Some businesses are failing to screen data against the TPS register, or alternatively, are failing to screen the data as frequently as required. In addition, some businesses claim that TPS registered consumers have notified them that they do not object to its calls, but are unable to produce evidence of this when asked by us, or when challenged by the consumer. This is leading to complaints to individual businesses, as well as the CMR and other regulators.

Data should be screened against the TPS register before use and at least every 28 days thereafter. Overriding consent is only valid if it is given to the particular caller. The CMR continues to receive data from Ofcom, in order to enable close monitoring of businesses that make live telesales calls. Where there are persistent and/or a high number of complaints from consumers who, despite being registered with the TPS are still receiving telesales calls, enforcement action will be taken.

## Emails, texts or automated calls

Before marketing by email or text, or by automated 'voice broadcast' calls, businesses must ensure that the subscriber has given their prior consent, in accordance with regulations 22 and 19 of PECR.

In relation to texts or emails, there is an exception to this known as a 'soft opt-in'. This only applies in the specific circumstances specified in regulation 22 (3) of

PECR, and in our experience businesses are rarely able to provide sufficient records to satisfy this.

Consent must be knowingly given, clear and specific, and cannot be inferred. In order to demonstrate that they have acted compliantly, business should keep appropriate records of what the consumer has consented to, and details of how and when this consent was obtained.

It is best practice for businesses undertaking such marketing to obtain consent directly. However, businesses seeking to rely on prior consent obtained by third parties should have appropriate due diligence mechanisms in place to monitor the sources of the referrals and should retain appropriate records of the checks they have in place.

Businesses found to have transmitted, or instigated the transmission of emails, texts or voice broadcast calls that are unable to demonstrate that prior consent was obtained, will be deemed to be in breach of PECR and consequently General Rule 5 of the Conduct of Authorised Persons Rules 2013 (2) ("CAPR").

## Data suppliers

Many businesses are relying on assurances from third parties, contractually or otherwise, that personal data has been obtained fairly and lawfully, that data has been screened against the TPS register and/or that consumers have consented to receiving communications.

Businesses that transmit or instigate the transmission of calls, texts or emails in contravention of PECR and the Data Protection Act 1998 ("DPA"), will be in breach of General Rule 5 of the CAPR. In addition, businesses will also be in breach of Client Specific Rule 4, which requires compliance with the Direct Marketing Association's ("DMA") Code. This means that if you advertise, send advertising on behalf third parties, or outsource advertising to third parties, you should ensure that PECR, the DPA and the DMA's Code are complied with.

If you intend on buying or renting lists from third parties, you must undertake robust checks to satisfy that you are compliant with the PECR and DPA. To assist you in ensuring that you do not breach the requirements, the ICO have published detailed guidance on what may amount to reasonable due diligence in such circumstances. We would expect such due diligence checks to be documented.

If, when undertaking your due diligence checks, a third party is unable to provide records to demonstrate that it is reliable, you should not use them as you are therefore unable to satisfy yourself that you are going to be compliant. Businesses that do so could breach the CAPRs and put their authorisation at risk.

## Unauthorised introducers

Businesses should be ensuring that they are not accepting referrals from third parties who require authorisation. Regulated claims management services includes (but is not limited to) advertising for or otherwise seeking out persons who may have a cause of action, and referring details of a claim, claimant, cause of action or potential claimant to another person. This could include data brokers as well as lead generators and data suppliers that introduce work to you.

Businesses found to be accepting referrals from persons acting in contravention of the Compensation 2006 could be deemed to be aiding, abetting, counselling or procuring a criminal offence. You should therefore ensure you have appropriate mechanisms in place to ascertain whether your introducers require authorisation.

Checks should be made prior to accepting any referrals from third parties. In order for you to be satisfied that a business is authorised, there should be an exact match of the business name if using the authorised business search on our website, and such checks should be documented.

## Time limits

Some businesses have been able to demonstrate that they obtained consent to market to consumers, however such consent was obtained several months or years prior to the communication being made.

Many of the PECR regulations state that communications can be made if the consumer has notified that he consents for the time being to receive them. Consent will not remain valid indefinitely. In order to determine whether consent is still valid,

businesses should consider the wording used, the context in which it was given and the nature of the relationship between the business and the consumer.

When obtained by a third party rather that by your business, the ICO advises that generally, businesses should not rely on consent given more than six months ago. Further information from the ICO can be found here.

Businesses should ensure they have appropriate processes in place to establish when consent was obtained, and what information was provided to the person consenting.

## Suppression

In accordance with PECR, the consent that you hold allowing you to contact a consumer can be withdrawn at any time. In addition, consumers can request not to receive live telesales calls from your business.

In practical terms, this means that businesses should maintain a 'suppression list' of consumers who have opted out of receiving marketing, or have otherwise told you that they do not wish to be contacted. In most cases, consumers' details should be suppressed rather than deleted, so you know not to contact them. This involves you retaining just enough information to ensure their preferences are respected. A failure to suppress numbers would not only be a breach of PECR and General Rule 5 of the CAPR, but also a breach of the DPA if you subsequently use the consumers' details for marketing purposes.

In addition, some businesses are failing to provide a valid address in emails and texts to which consumers can request to opt out of such communications. This is a requirement of regulation 23 of PECR, and a failure to comply would again constitute a breach of General Rule 5 of the CAPR.

## Misleading marketing

A number of businesses are failing to provide accurate information about the services that they provide when telemarketing to consumers. Examples include stating that a financial review will be undertaken by the business, when simply providing services relating to mis-sold PPI, and claiming that a certain amount of compensation is available for the recipient of the message to claim.

When marketing to consumers, you must ensure that all information provided is clear, transparent, fair and not misleading in accordance with Client Specific Rule 1 (c) of the CAPR. Similarly you must ensure that you have sufficient training and monitoring processes in place for your telesales staff, in accordance with General Rule 4.

Some businesses are labelling communications as market research, when the purpose is to sell services, generate leads or collect data for marketing. This practice, known as "sugging", is prohibited by the DMA's Code, and therefore constitutes a breach of Client Specific Rule 4 as well as Client Specific Rule 1 (c). Businesses will also be breaching the DPA by processing the data, in contravention of General Rule 5. Similarly, if a business is sugging, and has called a number registered with the TPS, sent a text or email without consent, or instigated someone else to do so, it might also be in breach of PECR.

## Identification

A number of issues have been identified in relation to authorised businesses identifying themselves in marketing.

When making outbound calls, businesses must ensure that they provide a calling line identification number, to which return calls can be made. If not a geographic number, this must be a presentation number which satisfied Ofcom's Guide to the use of Presentation Numbers. Businesses failing to comply with these requirements will be contrary to the DMA's Code, and consequently in breach of Client Specific Rule 4 of the CAPR.

Some businesses are using trading styles that they are failing to notify us of either at all or within the 20 working days required by General Rule 16 of the CAPR.

Furthermore, a number of businesses are also failing to disclose their identity when marketing. Client Specific Rule 1 (a) of the CAPR requires advertisers to clearly identify themselves when soliciting business through advertising, marketing or other means. Businesses failing to do so in calls, texts or emails will also be in breach of General Rule 5, as many of the PECR provisions similarly require such identification.

## Further information

Businesses requiring further advice in relation to the compliance of their direct marketing practices should refer to our CMR Marketing and Advertising guidance or contact the:

- ICO
- DMA
- Ofcom, or our
- CMR Business Advice Team on **0333 200 1320** or email **business@claimsregulation.gov.uk.** Where necessary, the Business Advice Team may signpost you to an appropriate organisation.