SLAUGHTER AND MAY/

MAY 2022

CONSENTS, RECORDS AND DISGUISES: LESSONS FROM ICO DIRECT MARKETING ENFORCEMENT ACTIONS

A version of this briefing first appeared in the Privacy Laws & Business UK Report, Issue 121 (May 2022)

The past year has seen a continued trend of enforcement action by the Information Commissioner's Office (**ICO**) for breaches of the direct marketing rules contained in the Privacy and Electronic Communications (EC Directive) Regulations 2003 (**"PECR"**). Whilst a number of these actions are directed at persistent unscrupulous spammers and scammers, the ICO has also fined many well-known businesses, often evidencing a strict interpretation of the rules. The ICO continues to emphasise that it expects organisations to learn from others' mistakes when conducting marketing campaigns, and so this briefing discusses some key aspects of recent ICO fines and the learnings and pitfalls organisations can draw from them. Further information on the fines referred to is set out below in this briefing.

Soft opt-in and the ability to opt-out

Check that customers checking out on your website as guests are given the option to opt-out of marketing

The Royal Mail guest check out process did not provide an option for customers to opt-out of marketing, and, as a result, the ICO was clear that they could not rely on the 'soft opt-in' exemption in respect of these customers. It is important to therefore ensure that each customer journey through your website has the necessary opt-out wording at the appropriate point.

Check that those placing orders over the phone have the ability to opt-out

The ICO found that Papa John's could not rely on the soft opt-in exemption in relation to customers that had placed an order over the telephone, as those customers were not given the opportunity to opt-out at the time their details were collected. The ability of customers to access the Papa John's app or website to amend their marketing preferences was not considered sufficient by the ICO on the basis that any information about marketing choices should be provided to individuals directly rather than them having to seek it out for themselves. Organisations wishing to send electronic marketing to telephone customers therefore need to incorporate an appropriate opt-out mechanism into the customer journey.

This could be, for instance, by adding to an existing pre-recorded message a statement that the customer's data will be used for marketing and that if the customer wishes to opt-out, they should inform the call handler who will shortly be taking the call.

Ensure that there is no time gap between collecting the customer data and providing the ability to opt-out

In the case of We Buy Any Car (WBAC), the customer submitted their data on the website to receive a quote which was sent by email within seconds. The opt-out wording was included in the email, rather than on the website. Despite the gap between the personal data being provided and the opt-out wording being received being so short, the ICO concluded that the ability to opt-out of marketing was not provided at the time of collecting the information. WBAC was therefore not allowed to rely on the soft opt-in.

Soft opt-in and privacy notices

Check that all your customers are told where to find your privacy notice

Both Royal Mail and Papa John's were found to have failed to make their privacy notice available. Royal Mail hadn't provided one to customers checking out as guests and Papa John's was on its website but not drawn to the attention of telephone customers.

Minimising the impact of human error

Test systems for vulnerability to human error and consider what steps to take to minimise the risk and impact of such error

The ICO appears to be making limited allowances for human error. In the case of Royal Mail, a manual error in selecting marketing lists for a campaign led to just under 100,000 opted-out customers receiving 'reminder' marketing emails. The ICO considered that Royal Mail should have been aware of the risks of storing consenting and non-consenting email addresses in the same system and hadn't taken reasonable steps to prevent the issue. Similarly, the ICO considered that Reed Online Ltd (ROL) knew or ought to have known of the risk of a contravention occurring in part because it had a high

proportion of opted-out individuals on its database, and it considered ROL's processes and checks to be inadequate.

Although it is difficult to completely fool-proof systems against human error, it is worth considering what checks you have in place. Post-breach, ROL identified certain actions which would prevent similar future incidents occurring, such as processes for reviewing and signing-off when campaigns are switched to 'scheduled', a quality assurance process to identify errors, re-considering any scheduled emails outside of core working hours and looking into options around email recall capabilities. The ICO's view was that these should have been in place from the outset, especially for large campaigns.

Marketing vs service messages

Establish clear and firm lines internally as to what constitutes 'marketing' as opposed to 'service' messages

Genuine service messages are not marketing and are therefore not covered by the PECR consent requirements, with the ICO concluding that the emails in the case of Virgin, the Conservative Party and AMEX were on the wrong side of the line.

In the case of AMEX, its internal guidance distinguished between operational, service and marketing emails. Operational emails were defined as any "purely factual/operational communication with no content promoting products or services to recipient[s] including information promoting services and/or benefits associated with American Express product[s] held by recipient[s] - e.g. account alerts".

Service emails were defined as any "communication including information promoting services and/or benefits associated with American Express product[s] held by recipient[s] - e.g. benefit awareness/ reinforcement".

In contrast, marketing emails were defined as any "communication promoting products and services not held by recipient[s]". In accordance with this guidance, Amex had classified the emails in question as service emails.

The ICO disagreed with this classification, pointing out that AMEX's definition of service emails recognised that they contained marketing content. The ICO also considered that none of the emails in question were neutrally worded and purely administrative in nature. Instead, each email sought to encourage the customer to make purchases on their AMEX card and, in the case of the AMEX app emails, also to make use of that product.

This demonstrates the importance of providing appropriate internal guidance and considering each campaign on a case-by-case basis as necessary - the enforcement notice sets out the wording of a number of emails and is a helpful reference point for this.

Data retention and direct marketing

Ensure your data retention policies appropriately factor in direct marketing records

During the ICO's investigation of Sports Direct, it became apparent that Sports Direct was struggling to present relevant evidence of its actions and rationale for sending direct marketing material to customers it had not contacted for some time. Many of the relevant employees had left Sports Direct, and most of the relevant files and communications created during their employment had been deleted in accordance with their retention procedures for when employees depart. This highlights the importance of ensuring that standardised data deletion processes do not hinder proper record keeping.

When changing IT systems or IT providers, ensure this does not impact direct marketing preference records

The ICO found that the Conservative Party had failed in twelve cases to ensure that records of customers who had unsubscribed from marketing emails were properly transferred when it changed email provider. In the ROL decision, the error occurred as part of the migration to a new system, highlighting the importance of additional controls and checks during major changes.

Third party consent

If a third party is collecting consent on your behalf, check whether your organisation is appropriately identified along with a description of the type of marketing you will send

When fining SAGA (and also Leave.eu in February 2019), the ICO emphasised, by reference to its direct marketing guidance, that consent to marketing obtained by a third party on a marketer's behalf will not generally be adequate by itself. However, it may be compliant where the third party consent is sufficiently clear and specific. In the SAGA decision, a seemingly exhaustive list of categories of organisations who the customer 'consents' to receive marketing messages from was not specific enough to satisfy this requirement. A generic description as to "similar organisations", "partners" and "selected third parties" would not be compliant either, or precisely named 'categories' of third parties (although naming a specific type of organisation may be sufficient for valid consent more generally).

Key recent fines

Company	Date	Fine
Reed Online	April 2022	£40,000
Royal Mail	March 2022	£20,000
Virgin Media	December 2021	£50,000
WBAC	September 2021	£200,000
Sports Direct	September 2021	£70,000
SAGA Services Ltd	September 2021	£150,000
SAGA Personal Finance	September 2021	£75,000
Papa John's	June 2021	£10,000
Conservative Party	June 2021	£10,000
AMEX	May 2021	£90,000
Leave.EU Group Limited	February 2019	£45,000

Mitigating factors

Notification to the ICO

There is no mandatory breach notification regime under PECR. However, Royal Mail voluntarily self-reported its PECR breach and this was recognised by the ICO as a mitigating factor. That said, unless one believes that the ICO will receive direct complaints from customers which it will act upon, it seems unlikely that organisations will consider the benefit of self-reporting to outweigh the potential downsides in most cases.

Suspension of marketing activities following a complaint

The ICO acknowledged that Papa John's decision to suspend marketing to individuals placing orders over the telephone was a mitigating factor (and similarly for Amex when it stopped marketing opted-out clients during the ICO investigation). Whether suspension will be a practical approach for organisations will likely depend on a number of factors, including the number of complaints received, the importance of a particular campaign to the organisation and their attitude to risk. However, organisations should at least consider reviewing their marketing model or practices following the receipt of complaints, something the ICO had noted Amex had failed to do (after receiving 22 complaints). This was considered to be an aggravating factor.

Co-operation with the regulator

In the Conservative Party decision, the ICO comments that although the Party did engage with the investigation and was not obstructive, its extensive delays in responding to requests for information and clarification meant that its conduct was not a mitigating factor (although it wasn't an aggravating factor either). This suggests that engaging with the ICO and responding promptly to questions is likely to be viewed as a mitigating factor. The other fines referred to in this briefing do not explicitly mention co-operation as a mitigating factor. However, there are clearly advantages to co-operating with the ICO, including PR benefits if the organisation is seen as pro-active, effective and responsible.

Internal investigations or audits

The ICO has accepted as a mitigating factor the steps a company has taken, or commits to take to investigate and audit their PECR compliance. Organisations should therefore consider what steps they can take in this regard to demonstrate their intentions to remedy any issues and to be PECR compliant.

Comment

Overall, the recent ICO fines show that the ICO is willing to take action in relation to direct marketing beyond the areas one would typically consider as most likely to cause distress or harm. Examples are nuisance calls and marketing relating to sensitive information, where, for example, the ICO expects explicit consent for marketing to pregnant women. The ICO's approach to taking enforcement action, coupled with it generally appearing to favour a strict interpretation of the law, leaves organisations little room for error.

Unhelpfully for organisations grappling with PECR compliance, the ICO guidance in this area is somewhat in limbo – although the ICO has existing guidance on direct marketing on its website, it had published updated draft guidance in January 2020. The consultation on that guidance closed in March 2020 and the final version is yet to be issued. Perhaps now that the handover to the new Information Commissioner, John Edwards, has completed, we may see a final code later this year which should assist organisations in understanding the ICO's approach in this area.

Whilst the level of fines imposed have not been significant for most of the organisations involved, management time and external costs in dealing with an ICO investigation and the potential reputational damage from the existence of enforcement action need to be factored in. Ultimately the question of PECR compliance is therefore one of risk - marketing, data privacy and legal teams will need to determine what is appropriate for your organisation based on your customer base, appetite for risk and the sector in which you operate. And if the government's proposals for data protection reform adopted , this risk profile is likely to change again, with PECR attracting GDPR-level fines and the ICO potentially gaining equivalent investigatory powers as under the GDPR, for example the power to issue assessment notices in order to access premises and documentation.

CONTACT

REBECCA COUSIN
PARTNER
T: 02070903049
E: Rebecca.Cousin@slaughterandmay.com

ALEX BUCHANAN
TRAINEE SOLICITOR
T: 02070904045
E: Alex.Buchanan@Slaughterandmay.com

CINDY KNOTT
PSL COUNSEL AND HEAD OF DATA PRIVACY KNOWLEDGE
T: 02070905168
E: Cindy.Knott@slaughterandmay.com

London
T +44 (0)20 7600 1200
F +44 (0)20 7090 5000

Brussels
T +32 (0)2 737 94 00
F +32 (0)2 737 94 01

Hong Kong
T +852 2521 0551
F +852 2845 2125

Beijing
T +86 10 5965 0600
F +86 10 5965 0650