UK FINANCE

UK Finance response to ICO's Draft Code of practice: direct marketing

Date: 4 March 2020

Sent to: directmarketingcode@ico.org.uk

UK Finance is the collective voice for the banking and finance industry.

Representing more than 250 firms across the industry, we act to enhance competitiveness, support customers and facilitate innovation.

Thank you for this opportunity to comment on the draft code of practice on direct marketing. Please find our comments below.

In part one of our response we outline our primary concern: that the draft code will make it difficult for our members to effectively reach customers with important communications, particularly those communications required by other regulators. This seems to create a regulatory conflict and risks negatively impacting customers. We strongly recommend discussing this issue with the Financial Conduct Authority and other sectoral regulators, and revising the code as suggested below.

Part two of our response sets out our comments in relation to other points in the code.

If you have any questions relating to this response, please contact [redacted]@ukfinance.org.uk

[redacted]

Part One: the scope of 'direct marketing purposes' and the risk of unintended consequences

1. The definition in the Code of 'direct marketing' is very wide and appears explicitly intended to catch activities intended to be in the public interest. We note that the discussion of public sector marketing, though not directly applicable to our members, includes notification by a regulator of a new complaints tool and the sending of personally addressed post promoting a health and safety campaign as examples of marketing.
2. There is a risk that this will significantly affect firms' ability (and the ability of government entities) to promote public good / public policy goals, such as raising awareness of fraud risks and how consumers can protect themselves, and campaigns to build public financial understanding. We are concerned that this would not be in the public interest. Greater flexibility is required to recognise the important role served by communications intended to achieve public good objectives, such as:
    a. Raising public awareness of important risks such as financial fraud
    b. Promoting actions required under a legal or regulatory obligation

c. Service or product communications sent primarily (though not necessarily *solely*, as in the draft code) for the benefit of the customer, in order to meet regulatory obligations to treat customers fairly
d. Raising awareness of tools available to help consumers manage their finances better, such as free credit rating checks, product comparison tools, explanations of interest rates and educational material, for example about how ISAs work
e. Promoting effective data protection, such as offering free security software

3. In particular, we note the following specific challenges with the scope of the draft Code.
4. Pages 20-21 – Regulatory communications
    a. We are concerned that the guidance on messages required for regulatory purposes will have unintended consequences that will negatively impact customers and create a conflict of regulatory requirements.
    b. We recognise the ICO's concern that firms might seek to push the bounds of 'regulatory communications'. However, the current guidance is unnecessarily restrictive in stating that such communications are outside of PECR only if the message is:
        - *"in a neutral tone, without any encouragement or promotion;*
        - *is given solely for the benefit of the individual; and*
        - *is against your interests and your only motivation is to comply with a regulatory requirement (eg the regulator is requiring you to tell people that they should consider using your competitors' services)."*
    c. This guidance is considerably stricter than what our members had understood to be the ICO view in prior discussions and communications required under FCA rules would not necessarily meet these tests. For example, BCOBS 4.1.2 6A requires firms to notify customers when a fixed-term savings account is nearing the end of its term. This notification must explain the consequences of the expiry and what the firm will do with the funds if no instructions are received. Crucially, the firm must also *advise the customer of the options available* and how to exercise these. In order to be helpful to customers, this needs to include what other savings products are available from the firm and how to move the funds when needed. Often, if the customer takes no action the funds will default into an account with a lower interest rate than other products that could be available.
    d. Other examples include:
        i. Communications to advise of mortgage rate change, with the customer defaulting onto a higher rate than other products that might be available if no action is taken.
        ii. Communications to customers on a long-term variable rate to advise them that a more competitive deal is available
        iii. Communications sent to 'mortgage prisoners' to inform them that competitive products are on the market.
    e. This is problematic given the ICO's guidance, as:
        i. Notifying the customer of other products available would likely be 'promotion'.
        ii. Although the message is certainly for the benefit of the individual, depending on what will happen to the funds at the end of the product's term, the firm could well *also* benefit, for example from the customer placing the funds into another product.
    f. There are similar requirements on firms to advise customers of important decisions and issues relating to other investment products, retirement planning, etc. Depending on the situation, complying with FCA expectations could require promotion of other products from the same firm but could also include promotion of products of *competitor* firms (for which soft opt-in would be unavailable, as it only extends to the

firm's own products). Firms will often need to include a clear 'call to action' in order to meet FCA expectations that customers will understand that they need to act in order to benefit from the best possible rate.

g. As such, in practice the Code's requirements are likely to make it difficult for firms in financial services to satisfy their obligations under the FCA Handbook while also staying within the ICO's expectations. *It is not reasonable to expect firms to manage this kind of regulatory conflict*.

h. Many firms have large cohorts of customers for which they do not have direct marketing consent or the required 'soft opt-in'. This is especially true of long-term products such as mortgages which typically last for 25 or more years. These customers can nonetheless belong to groups that the FCA is particularly keen to see firms contact proactively with better product options. Not receiving these communications is *likely to be detrimental to customers' interests*. Indeed, these messages are intended by the FCA to form a part of firms meeting their obligation to 'pay due regard to the interests of… customers and treat them fairly' (FCA Handbook, PRIN 2.1.1, Principle 6).

i. It would be an unfortunate situation if customers that have not opted into marketing become less informed about how to make important financial decisions than those customers that have opted into marketing. This is unlikely to have been the expectation of customers that have opted out of marketing.

j. We strongly recommend that:

i. The ICO should **discuss this issue with the FCA** (and likely also other sectoral regulators) to ensure that there is a coherent regulatory framework.

ii. The Code is amended to **make clear that when firms issue communications for the purposes of complying with the rules and guidance of other regulatory authorities, these are not considered 'direct marketing'** and are therefore outside of the PECR consent rules. This could be constrained by requiring that the communication not go beyond what is necessary to meet the regulatory requirement.

5. See also our comments below on service messaging.
6. Pages 19-20 – Service messaging
   a. The draft Code contains the following: "*If a message is actively promoting or encouraging an individual to make use of a particular service, special offer, or upgrade for example, then it is likely to be direct marketing. However if the message has a neutral tone and simply informs the individual for example of a benefit on their account then these are more likely to be viewed as a service message.*"
   b. In practice, however, firms will in some situations need to advise customers of changes to the nature of the services they receive which will need to encourage them to make use of alternative services. This can arise for example when there is a regulatory change that firms need to respond to.
   c. For example, in financial services we recognise that *generally speaking* it would constitute direct marketing to send emails to customers encouraging them to make use of mobile banking apps. However, industry is in the process of implementing new 'strong customer authentication' rules, which require multi factor authentication for some types of payments. As a consequence, firms need to contact customers to encourage them to either disclose their current mobile phone number or else download an online banking app. Customers who fail to do so risk finding themselves unable to make some types of payments.
   d. More broadly, it is in customers' interests to be aware of the different ways that they can access services, particularly when new means of access are introduced. It would

be unfortunate if only those customers for which the firm has a marketing preference are aware of new means of payment (eg: cheque imaging). Vulnerable customers are likely to be particularly impacted.

e. We would also like to highlight that our members' consumer research suggests that customers have a more nuanced view of communications from their providers than a simply split between 'servicing' and 'marketing'. Such messages include reminders of foreign exchange rates, reminders of how to renew a product that is coming to the end of its term (or obtain a similar one) and reminders of the customer's debit card PIN if they haven't used it for a long time. Where these messages are tailored to the customer and are in their interests, we understand from member research that they are well-received by customers and are viewed as servicing. If the final Code takes too hard a line on servicing messages, consumers could miss out on this kind of valuable information.

f. The Code should be amended to clarify that, even if there is encouragement to use a particular service, a message does not constitute direct marketing if it has a suitably neutral tone and:

  i. is necessary to make customers aware of how services can be accessed and how their rights can be exercised,

  ii. is necessary to make customers aware that a product is reaching the end of its term and to explain how to obtain a replacement product, or

  iii. is necessary to make customers aware of relevant legal or regulatory change.

g. Additional guidance should also be added to help firms navigate the requirement for a 'neutral tone' when providing servicing messages.

h. This could be helpfully supported by an example of a firm sending messages that inform customers of a benefit, but which do not constitute 'direct marketing'.

i. See also comments below on page 35.

Part 2: Further detail-focused comments

7. We note that the code, while very useful, is long. A summary document might be helpful to marketing teams that are new to the data protection topic area.
8. Different types of 'marketing purposes':
   a. Building on comments made above in relation to page 14, it is not always clear in the guidance what the phrase 'direct marketing' is intended to cover. We identify three types of processing that could potentially be in scope in different places:
      i. Sending direct marketing communications to individuals (potentially subject to PECR, depending on a range of factors).
      ii. Profiling an individual in order to better target marketing at them.
      iii. The use of an individual's personal data in analysis to understand the firm's customer base in order to make overarching observations and better design marketing strategy, without ever actually creating a profile of the individual or feeding into the sending of marketing material to that individual.
   b. It would be helpful for the guidance to recognise that processing in **category iii. above is not for 'direct marketing purposes'**, or at a minimum to acknowledge that such background processing would generally be of **much lower risk** to individuals. This is relevant to the section on 'look-alike audiences' on pages 91-92.

c. More broadly, it would be **helpful for the terminology used in the guidance to be more precise**, for example by referring to 'sending direct marketing' or to 'all processing for direct marketing purposes', as appropriate.

9. Page 14 – The discussion of the definition of 'direct marketing purposes' is somewhat unclear. It arguably could be taken to suggest that all processing of personal data for direct marketing purposes is subject to PECR rules. Given that PECR Regulation 22 only applies to the 'transmission of communications', we presume that this is not the ICO's intended meaning. Although page 8 outlines the scope of PECR as opposed to GDPR, **it would be helpful for the discussion on page 14 to mention PECR's scope again for clarity**.
10. Page 17 – solicited versus unsolicited marketing: It would be **useful for the Code to explore this further**. For example, where communications are sent to customers as a part of a service (such as newsletters sent as a part of a packaged bank account) be considered 'solicited'?
11. Page 18 – Scope of 'market research': **We suggest clarifying** that audience research for the purposes of improving marketing campaigns generally should be treated as research and not for marketing purposes. This is as opposed to research intended to help implement a specific marketing campaign.
12. Page 23 – campaigning and promotional activities:
    a. This section states that 'fundraising, campaigning and promotional activities' are also subject to PECR rules. However, the discussion relates solely to charities and not-for-profits. Page 78 takes a similar approach.
    b. In contrast, some of our members (ie: for-profit businesses) may wish to run fund raising drives or other charitable efforts as a part of meeting their corporate social responsibility obligations. This could include firms' staff sending emails or other electronic messages to clients and client employees in order to raise awareness of the campaign. Although sent to *corporate email addresses*, arguably such communications are using corporate details for personal use.
    c. **It would be helpful for the Code to clarify** whether a *for-profit* firm trying to raise awareness of a good cause would be considered within the scope of 'direct marketing' and whether the 'soft opt-in' option would be available.
    d. It would also be useful to describe in more detail what is meant by 'aims and ideals'. Specifically, socially responsible investment products, though related to certain ideals, **should nonetheless be treated as products** and therefore have the potential to be marketed under the 'soft opt-in'.
    e. Some members also include in their marketing material a description of their brand and its values. If this kind of content is considered to be marketing 'aims and ideals', it would arguably make the soft opt-in unavailable for these communications. The **code should make clear** that a description of brand and company values in a marketing communication can still benefit from the soft opt-in.
13. Page 31 – the 'good practice recommendation' suggests that firms should seek to rely on consent for all direct marketing:
    a. Given the context on page 31, we presume that this is intended to be a reference to the sending of direct marketing, as opposed to all processing for direct marketing purposes.
    b. More importantly, this recommendation is out step with the overarching ICO guidance on bases for processing, which states that **there is no hierarchy of bases and that firms should choose the most appropriate one**. Furthermore, consumers are accustomed to the idea that they may receive direct marketing from firms with which they have a relationship. Provided an option to unsubscribe / opt out is consistently provided (where relevant), it is hard to see that moving to consent would be in

consumers' interests. Indeed, they are likely to be confused by a sudden attempt to acquire consent.

c. We recognise that it might be simpler from a systems perspective to do all marketing on the basis of the consent. It is helpful for ICO to highlight this *potential efficiency gain* but it should not be phrased as an apparently superior compliance approach.

14. Page 32 – This example could be confusing (particularly for any consumers reading the Code), as it combines a number of different interacting components of the PECR rules. The example seems to imply that in this situation no firm would be able to send marketing; in the context of a charity this is true but the example does not make clear that for other types of firm another basis beyond 'consent' could be available. Firms in a comparable situation would often be able to rely on the 'soft opt in' and 'legitimate interests'. **We suggest avoiding confusion by adding a sentence in parentheses** at the end of the example, such as "(Although businesses in a similar situation might be able to rely on legitimate interests and the 'soft opt-in' for marketing of products and services – see page XYZ)"
15. Page 33 – Granular consent options:
    a. We question whether providing granular consent options in the way ICO suggests would improve customer understanding, or whether it would create customer confusion / risk information overload. Specifically, needing to offer consent for each sub-type of marketing-related processing. It might be helpful to have **an example of a suitably proportionate level of granularity**. An alternative approach might be to give a broader consent for marketing purposes (or similar term) and to direct the data subject to the relevant section of the privacy notice if they want to get into the detail. Indeed, a 'channel agnostic' approach would be consistent with the general technology-neutral nature of the GDPR and would be easier for customers to understand.
    b. It would also be **helpful for bullet 3 to acknowledge that legitimate interests** could also be a basis for processing for profiling.
16. Page 33 – the Code warns against 'unduly' incentivising consent. It is not at all clear what would cross this line. It would be **helpful for ICO to provide additional guidance** on what factors are likely to tip this balance one way or the other.
    a. As an example, given that market research can be 'for marketing purposes' (see also comments above on page 18), there is a risk that firms will feel unable to offer reasonable incentives (eg: donations to a charity of the choice of the individual) to participate in research.
    b. It could be **helpful to make the example less specific**; it could refer to more generic situations such as using discounts to incentivise individuals to sign up to email marketing, for example.
17. Page 35 – on legitimate interests:
    a. Given the apparent view that many types of communications that are for the purposes of complying with FCA regulation would amount to 'direct marketing', it is **important for this part of the Code to recognise that firms can have a strong legitimate interest in complying with regulatory rules and guidance** from sectoral authorities. See also comments above on pages 20-21.
18. Page 36 – on legitimate interests:
    a. The Code states that 'invisible processing' would be unlikely to pass the 'balancing test' for legitimate interests. It would be **useful for the Code to recognise explicitly** that where such processing has only a low impact on data subjects, legitimate interests could still potentially be available. For example, see comments below in relation to page 48.

b. The example on this page **should make clear** that the theatre's approach is likely to be compliant.
c. The Code states: "[it is difficult to pass the legitimate interests balancing test if] collecting and combining vast amounts of personal data from various different sources to create personality profiles on individuals to use for direct marketing purposes." **It would be helpful for the Code to clarify** that legitimate interests *can* be relied on for such processing, provided the firm takes care to deliver suitably prominent and specific privacy notice information, along with appropriate safeguards such as opt-outs.

19. Pages 41-42 - the length of valid consent:
    a. The draft code states: "Depending on the circumstances it is likely to be harder to rely on consent as a genuine indication of wishes as time passes." It would be helpful for the code to acknowledge that if the firm includes a suitable 'opt out' consistently, it is reasonable to assume that the individual is content to receive direct marketing. The individual remains in complete control, being able to opt out at any time. If the firm has to send messages seeking renewed consent, this risks simply increasing the volume of marketing-related messages that consumers receive. **It should be clarified that firms can continue to send direct marketing in reliance on consent, provided the individual receives the required opt out option with each communication.**
    b. In the context of consents which have not yet been acted on by the firm, it would be helpful for the Code to **give examples on page 41** of considerations which suggest consent would remain valid for a longer period (like it does on page 42 in a different context). These include seasonal products, products that are renewed annually (eg: some insurance products) and other products with a long redemption curve. This should also be clarified in the 'best practice' example on page 42; consent from a third party to market seasonal products, etc, ought to be valid for longer than six months.
20. Page 42 – the **Code should clarify** that data no longer needed for marketing does not need to be erased if it is also necessary for another legitimate purpose.
21. Page 47 – bullet 3 states that controllers should include their 'retention periods' for marketing data. This should be **amended to reflect that Article 13(2)(a),** which allows firms to give the criteria used to determine the retention period.
22. Pages 48-49 – transparency when data is collected from other sources
    a. Some of our members use publicly available data in order to identify individuals that could be eligible for certain products, particularly products available only to high net worth individuals, in order to target marketing.
        i. Where the firm ultimately determines that an individual is not eligible for a product, it would be disproportionate to expect the firm to then have to contact the individual and advise that their public information had been assessed and that they had been determined to be ineligible for product XYZ. This would be more likely to confuse the individual than to advance her interests.
        ii. **The guidance should clarify** that in this circumstance, sending such a communication would be disproportionate and therefore not required under Article 14(5)(b).
    b. The **guidance should also clarify that it may be possible** to rely on the disproportionate effort exemption where data controllers collect personal data from various sources to build profiles, but this new processing actually has a minor effect on individuals. This could arise for example where a data controller has a direct relationship with a data subject and has already suitably explained its profiling activities. The firm might, during the course of that relationship, later obtain new

personal data from 3rd party sources for the purposes of developing its profile of the individual (or the same personal data but from a new 3rd party source). Provided the new processing has no materially greater impact on the individual and a suitable explanation of the profiling was given in the initial privacy notice, it seems disproportionate for data controller to proactively notify individuals about the new data source. This would need to be carefully assessed and documented in each instance.

c. The guidance on this page also suggests that the exact sources of data must be provided. This **should be amended to align with Recital 61**, which allows for 'general information' to be provided.

23. Pages 50-51 – explaining the use of personal data for marketing purposes:
    a. The Code here states that firms should avoid using terms such as 'marketing insights', 'marketing purposes' or 'marketing services', as they are not specific enough. It is not clear, however, what level of information ICO actually expects firms to provide or the categories of activity that might need specific mention in privacy notices. We note that there is a difficult balance to be maintained here; consumers might benefit more from receiving more succinct information than a detailed explanation which risks causing the reader to disengage or causing confusion. This balancing act **should be acknowledged in the Code, with guidance provided** on how best to ensure the appropriate level of granularity.
    b. The example is of a low-quality communication; it would be helpful to also **give an example of good practice**.
24. Page 52 – use of publicly available data: This section of the guidance highlights the importance of providing notice but does not refer to the Article 14 exemptions, which may apply. This section **should be amended to cross refer** to the discussion of the exemptions on pages 48-49.
25. Page 54 – obtaining contact details of existing customers' friends and family:
    a. In some instances, existing customers pass on the details of friends or family on their own initiative. This seems to pose little practical risk to data subjects. **We recommend clarifying in the Code** that in this situation a firm can contact the friend / family member of the customer, provided the customer has made clear that the contact has been made on the request of the data subject.
26. Page 56 – Profiling and data enrichment: The 'at a glance' box contains two typos: 'there are addition rules' and 'on the using their'.
27. Pages 57-59 on profiling:
    a. As a general point, we note that this section focuses on the negatives of targeted marketing and does not recognise the positives for consumers. In particular, targeted marketing – made possible through profiling – can help consumers see less, but more relevant marketing, rather than large amounts of marketing of no interest. It would be helpful for the tone of the **guidance to acknowledge** this positive contribution of profiling.
    b. This section states that 'wealth profiling' requires a DPIA. However, this is not in line with the more detailed section on page 28 or with the ICO's more detailed overarching guidance on DPIAs, which only treat this kind of processing as *potentially* requiring a DPIA. **Pages 57-59 should be aligned** with page 28 and the more general guidance.
    c. The Code states that 'intrusive profiling' for direct marketing purposes is unlikely to be able to rely on legitimate interests. Although the Code refers to various factors that imply a profiling could be 'higher risk' (eg: large scale, use of special category data) it is not clear what is meant by 'intrusive profiling'. Given that the Code suggests such processing would require consent, **guidance as to the meaning of this term is**

needed. This could perhaps include inferences that might be considered offensive or upsetting.

d. The Code seems to focus on the practice of using profiling to identify individuals the firm would like to market to. We suggest that the **Code should also specifically cover the use of profiling to identify individuals that should <u>not</u> be marketed to** and thus remove them from marketing lists. In the financial services sector in particular, firms screen marketing lists to identify individuals in financial difficulty, to whom credit products should not be marketed. Firms do this as a part of complying with their obligations to treat customers fairly. **A pragmatic approach is needed for this kind of profiling, which is intended to protect customers**.

28. Page 60 – matching and appending data:
    a. The Code states that buying additional contact details for existing customers is likely to be unfair unless the customer has given consent. **The Code should make clear** that there are other situations beyond marketing where this practice is more likely to be legitimate, such as when data matching is for fraud prevention purposes.
29. Pages 61-62 – tracing:
    a. This section takes a hard line against the use of tracing services. In the context of banking and financial services, the most likely reason that an individual has not updated his/her contact details is in our view, and contrary to the Code's view, that (s)he has simply forgotten to do so.
    b. We sympathise with the position in the Code insofar as marketing is the *only* reason that the individual's contact details are needed, for example in the context of a firm whose business is solely the distribution of advertising. However, in financial services firms have regulatory obligations to maintain up-to-date contact details with their customers as a part of maintaining an ongoing relationship with them and ensuring fair treatment. For example, firms sometimes need to provide communications to customers to protect their interests (for example where the customer is vulnerable, or an important product / service change is occurring – see comments above on regulatory communications and servicing messages).
    c. The Code should make clear that tracing services remain legitimate, when the firm has an important non-marketing purpose.
    d. **The Code should also make clear** that marketing can legitimately continue, where tracing has been needed for another important purpose. It would be confusing for customers who have decided not to object to / unsubscribe from marketing to have these communications cease, despite that the ongoing relationship and ongoing communications of other kinds.
    e. As an important related detail, we do not necessarily agree with the Code's statement that "tracing an individual for direct marketing purposes takes away control from people…". Individuals can choose to opt out of marketing at any time; this option should of course always be presented prominently.
30. Page 66 – direct marketing by post: **This section should discuss the potential basis for processing**, particularly noting that legitimate interests could be available.
31. Page 69 – there is a typo in the heading: 'Calls management calls' should presumably be 'Claims management calls'.
32. Page 74 – Direct marketing by email:
    a. The Code states that email addresses identify a unique user, distinguishing them from other users, and therefore amounting to personal data. This is not necessarily the case. Some email addresses are generic, such as 'queries@firmxyz.com', potentially accessed by multiple employees. **The Code should be amended to recognise** that it is not likely that such email addresses would constitute personal data.

b. The discussion of tracking pixels should **acknowledge that some examples of 'strictly necessary' tracking pixels exist**, such as those that simply serve to determine 'open rates' of emails.

33. B2B marketing: If the communication is addressed to a specific business employee but the content is directed to the business, does this amount to 'direct marketing'?
34. In-app messages:
    a. The Code states in several places that these are within scope of the PECR rules. As a point of law, we do not agree that this is necessarily correct, as such messages will not necessarily amount to 'electronic mail' under Regulation 2 of PECR. This is for two reasons:
        i. First, to be 'electronic mail' under Regulation 2, a message must be sent over a 'public electronic communications network'. Many apps do not exist for the purposes of making 'electronic communications services' available to members of the public, meaning they are not a 'public electronic communications network'.[1]
        ii. Second, these messages are often within the domain of the firm providing the app and are not "stored in the network or in the individual's terminal" and are therefore not 'electronic mail' under Regulation 2 of PECR.
    b. Whether or not a particular app's messages amount to 'electronic mail' will depend on the way the app functions and the type of message (pop-ups and banners within the app, pages displayed after logging into the app, etc).
    c. It might be appropriate for the Code to explore the complexity of the scope of PECR in this area and highlight to firms that they should consider taking advice on this matter.
    d. That said, the data processing for such marketing would need to either be based on consent or on legitimate interests, in which case a suitable 'opt out' tool would be required. This would provide a suitable safeguard to individuals.
    e. **The Code should be revised to make clear that providing marketing in-app can be but is not *necessarily* 'direct marketing' under PECR, and to provide guidance on appropriate safeguards.**
35. Page 80 – the Code states that 'some partnerships' are treated as individual subscribers. It would be **helpful to have more detail** on when this would apply.
36. Pages 82-83 –
    a. Contrary to the first paragraph of page 83, on our reading regulation 22 of PECR only requires the consent of the individual to be received by the sender, not the instigator. We note that the instigator cannot 'instigate' the sending of the marketing without consent, but the consent only needs to be provided to the sender. This is particularly relevant when a company / brand within a corporate group sends marketing about products of other group companies. Consistent with this view, we note that page 27 of the guidance, particularly the example, seems to say that it would be 'good practice' for the sender to screen against the instigator's suppression list, and that only the sender needs to have consent. **This should be clarified in the Code**.
    b. Discussion of 'refer a friend' schemes:
        a. We acknowledge the ICO's concerns about viral marketing and the risk that these could be seen as a way to avoid having to comply with GDPR and PECR requirements. Clearly, where a firm is instigating others to send pre-scripted

[1] Regulation 2 of PECR refers to section 151 of the Communications Act 2003, which defines a 'public electronic communications network' as "an electronic communications network provided wholly or mainly for the purpose of making electronic communications services available to members of the public"

messages to large numbers of recipients (eg: all of one's contacts), this poses a privacy risk to those individuals.

b. However, more conventional 'tell a friend' campaigns pose only a low risk of detriment to individuals and can provide clear benefits to consumers.
c. In some instances, a firm might invite its customers to tell their friends about the firm and its services. In some cases, the firm might offer an incentive to customers to do so. **Provided the firm does not provide text for customers to share, we understand that this does not amount to instigating direct marketing. This appears to be the case under the Code, but it would be helpful to make this clearer**.
d. Any processing of personal data would of course need a suitable basis for processing. Legitimate interests could, in our view, provide a suitable basis.
e. Additional guidance should be included in the final Code to **clarify the sorts of safeguards** which could be appropriately deployed to protect individuals' interests and ensure that firms do not employ a 'scatter gun' approach. These could include providing a single code being issued to the referring customer for any referral, to evidence the link between the referrer and the referee; this can further help ensure the details for applying would be issued on a case by case basis and not as part of a wide sharing of an application mechanism.

c. It would be **helpful for the Code** (and indeed the more general DPIA guidance) **to clarify** that references to 'new technologies' should be taken to refer to technologies that are new to the industry, rather than just new to the firm. Presumably a technology that is industry-standard does not pose the same level of risk, particularly when being provided by an experienced external supplier. More broadly, lack of understanding of a technology among data subjects can potentially be resolved through carefully designed transparency information and need not give rise to practical consumer risks.

37. Pages 87-88 – cookies: it would be **useful for the Code to discuss and compare** the responsibilities of the platform and the advertiser, eg: under regulation 6.
38. Page 90 – targeting via social media:
    a. The Code states that data processing to upload a contact list to a social media platform for 'audience matching' is likely to need to rely on consent, as it would be unlikely for the three-part legitimate interests test to be satisfied. It is not clear why the ICO thinks that this is the case. These tools do not *necessarily* depend on complex profiling; they simply allow a firm to market to individuals via a different medium, where they will already be expecting to receive targeted advertising. The actual disadvantage / risk to individuals seems low in such scenarios, particularly if suitable 'opt out' tools are provided and transparency information is carefully designed. We note, though, that as a platform adds more profiling or other complex processing, this will impact the legitimate interest assessment, with more safeguards required. **It would be useful for this to be acknowledged and discussed in the guidance** rather than just stating that 'consent will probably be required'.
    b. Similar comments apply in respect of subscription television services, app advertising and location-based direct marketing on pages 92, 95 and 96. As a detail point, we note in particular that page 95 is confusing, saying that in-app marketing probably needs to rely on consent even if no cookies are used. This is supported by a reference to the general online advertising guidance in the Code, but the most relevant section seems to be the top of page 89, which simply says that online advertising will need to rely on consent if cookies or special category data are involved. **Page 95 should be amended to follow the approach under page 89**, focused on requiring consent for cookies and special category data.

c. The Code states: “This type of targeted advertising on social media does not fall within the definition of electronic mail in PECR." However, it is not clear exactly what type of marketing is being referred to, as the preceding text is more about types of data and data sources. **This should be clarified**.
d. An example of a suitably constructed privacy notice would be useful in this section.

39. Page 96 – advertising IDs: we query whether it is necessary for each advertiser to know how the ID is used by other parties in situations where the advertiser will not be the data controller.
40. Pages 91-92 – look-alike audiences:
    a. These tools exist on platforms other than social media. Presumably the guidance is intended to also cover such other contexts but this is not clear from the guidance.
    b. The guidance states that where a business uploads a list of contacts to a social media platform, the two companies are likely to be ‘joint controllers’. This seems to go beyond the relevant ruling by the Court of Justice of the European Union. This ruling sets out that the firm sending data to the social media platform is only a joint controller for *those aspects of the processing for which it determines the purposes and means of processing, not all processing of the data*. **This should be clarified in the Code.**
    c. Further guidance in due course on this joint controller relationship could be helpful.
41. Page 111 states that screening out individuals from a list that do not qualify for a product does not count as ‘maintaining a suppression list’.
    a. **The guidance should clarify that this activity is still valid**, provided there is a suitable basis for processing, etc. At present the context and example about a lender screening out customers seem to suggest that this activity is not legitimate. We presume that this is not the ICO’s intention.
    b. As a detail point, we highlight that in financial services, firms have a regulatory obligation to screen recipients of marketing material. This is in order to ensure that the firm does not market credit products to individuals for whom they would not be appropriate, as a part of their ‘responsible lending’ obligations. (See also comments above in relation to profiling).
42. Online ads and new technology – though not directly applicable to our members, we note that the emphasis on consent for behavioural advertising and data broking could result in the adtech industry being made untenable. Changes to common practices are no doubt required but we query whether the strong line taken in the draft Code might be premature, with a staged process of raising standards more appropriate.
43. It would be useful for the Code to include a short note highlighting that the e-Privacy Regulation is coming and might necessitate changes to PECR.
44. A specific section on loyalty schemes would be useful, given these are widespread across industries.
45. Another useful example that ICO could include would be in relation to M&A, given that companies sometimes purchase other companies specifically to acquire their customer data. Points to explore could include where the legal controller changes / remains the same, and where the sector might change.

ENDS