



# Mobile Marketing Best Practice Guidelines

Direct Marketing Association (UK) Ltd

August 2005



# Contents

1.0 Introduction.....	3
1.1 What is Mobile Marketing? .....	3
1.2 Warnings About Misuse .....	4
2.0 Collecting and Managing Data .....	5
2.1 Collecting Data .....	5
2.1.1. Soft Opt-in Exclusion.....	5
2.1.2 Data Protection Notices.....	5
2.1.3 Privacy Policy .....	6
2.2 Data Hygiene.....	6
2.3 Marketing to children .....	7
2.4 House Files.....	7
2.4.1 Existing Personal Data .....	7
2.4.2 New Personal Data .....	8
2.5 Obtaining Positive Consent (notify at point of obtaining details that information will be used by third parties, Opt-in, Soft Opt-in) .....	8
2.5.1 Opt-Out Consent .....	8
2.5.2 Opt-In Consent .....	9
2.6 Renting Lists.....	9
2.7 Deciding on the Target Group .....	9
3.0 Mobile Campaigns.....	10
3.1 What are the first/key things that need to be thought about when setting up a mobile campaign? .....	10
3.2 Frequency of campaigns.....	10
3.3 When the best times to communicate are.....	10
3.4 Core Elements of a campaign .....	11
3.5 Those campaigns where we need to pay particular attention.....	12
3.7 Competitions, Draws and promotions .....	13
3.8 Distance Selling Regulations.....	14
3.8.1 Definition of Distance Selling.....	14
3.8.2 Information to be provided to consumers prior to entering a distance contract .....	14
3.8.3 Additional and written information to be provided to consumers following commencement of a distance contract .....	15
3.9 Bluetooth Campaigns .....	16
3.9.1 What is Bluetooth marketing? .....	16
3.9.2 Do I need consent from people before using Bluetooth marketing? .....	16
3.9.3 Surely if someone has their Bluetooth device “on”, I can assume that they have consented? .....	16
3.9.4 How can a consumer clearly and distinctly be given the opportunity to object to being contacted? .....	16
3.9.5 How can I use Bluetooth marketing in compliance with the consent requirements of the DMA Code of Practice? .....	16
3.9.6 How does Bluetooth marketing compare to marketing via Infrared? .....	17
4.0 Standard Metrics for Measurement & Reporting.....	18
4.1 Limitations on Reporting (What to expect) .....	18
5.0 Additional Points.....	19
5.1 Are there any special requirements if I am using premium rate numbers? .....	19
5.2 Location based mobile marketing.....	20
5.3 Special requirements regarding the use of adult content.....	25
6.0 Complaints and Dispute Resolution .....	26
6.1 Direct Marketing Authority & Code monitoring & Enforcement Procedures .....	26
7.0 Additional Requirements to be considered .....	27
7.1 The Stewart Report .....	27
Appendix A .....	28



## 1.0 Introduction

This best practice document has been produced to give practitioners an understanding of how mobile marketing applications can be used in an effective and non-invasive manner.

This document outlines the guidelines that should be adhered to, in order to develop responsive campaigns whilst recognising the rights of the consumer. Obligations provided by legislation that need to be complied with are also highlighted.

The DMA's goal in developing these guidelines is to:

- Encourage the use of Mobile Marketing as an effective marketing channel that can be used independently or in conjunction with other marketing channels.
- Outline specific examples of the use of Mobile Marketing and describe how campaigns should be structured.
- Provide practical advice about how to use the medium as well as legislative issues and applicable codes of practice that users of this medium need to be aware of.

### 1.1 What is Mobile Marketing?

Mobile Marketing refers to the process of marketing campaigns delivered via the mobile medium. Mobile has a number of unique benefits for marketers – it is 'always on, always with you and messages are always read'. UK penetration of mobile has now reached over 90% of the population hence the reach is exceptional. Moreover, mobile's virtues in dynamically tracking response and its immediacy in responding to events are key in making the medium ideal for direct marketers.

Mobile campaigns encompass acquisition, retention, customer service or CRM applications. The medium itself encompasses text messages (SMS), picture/audio messages (MMS) and the mobile internet (WAP). Campaigns can support responses as varied as requests for information, sales promotion, retail footfall generation and direct revenue generating sales.

Increasingly, mobile campaigns are being integrated with other media in the marketing mix – most notably on-line and e-mail. For instance a consumer may register their details on a website and then receive subsequent messages via mobile. The best examples of this integration are applications that are time specific (e.g. sport alerts or banking alerts) and therefore are required by the user wherever they are at whatever time.

In creating campaigns, a number of critical areas distinct to this medium must be addressed by marketers. These include the collection of permission from the consumer, the means of charging the consumer, areas of particular sensitivity (such as age and product type) and technical compatibility.

There is a wealth of legislative and Best Practice requirements of which marketers must be aware but this is all focused on making – and keeping – the medium attractive to the consumer. With the requisite care in planning and deployment, results to mobile campaigns.



## ***1.2 Warnings About Misuse***

Mobile's outstanding virtue is that it is the most personal of direct media. This however brings with it significant obligations on the marketer to respect user's privacy and to operate with the utmost focus on transparency as regards user's permission to communicate and any cost implications of participation in campaigns. These requirements are entrenched in legislative requirements through a number of bodies including the Information Commissioner (data protection and privacy issues) and ICSTIS (premium rate services and charging). Sanctions for compliance failure include fines and public censure.



## 2.0 Collecting and Managing Data

### 2.1 Collecting Data

When collecting personal data, which includes a mobile number, Data Users should:

- Comply with all requirements of the Data Protection Act 1998
- Only ask for the information that is reasonably necessary for the purpose of which the data is being used
- Have a clear Notice providing all requisite data protection notices and a link to, or full details of, a suitable Privacy Policy at the point of collection
- Gain the data subject's Consent to send Unsolicited Commercial Mobile Messages (for example with the use of an Opt-In check box) unless the Soft Opt In exception applies (detailed below)
- Comply fully with the requirements of the Data Protection Notices & Privacy Policy as outlined in (2.1.2)

#### 2.1.1 Soft Opt-in Exclusion

Individual subscribers must always have provided their express consent to receive mobile marketing communications, subject to the limited exception known as "Soft Opt-in" which applies only where:

- i) the mobile marketer has previously obtained the contact details of the recipient in the course of the sale or negotiations for the sale of a product or service to that particular recipient;
- ii) the mobile marketing communication to be sent relates to the marketer's **similar** goods and services only;
- iii) the mobile marketer has given the recipient a simple means, without charge, at the time of initial collection of the data to refuse (or opt out of) the use of his contact details for direct marketing purposes; and
- iv) included in each subsequent message to the recipient is included a right to opt out of future direct marketing sent by the medium of mobile.

These are the only circumstances where the Soft Opt-in exception can be relied upon. In all other circumstances, consent to use of data for mobile marketing must be obtained to comply with the obligations within data protection legislation.

#### 2.1.2 Data Protection Notices

When collecting a mobile number, the information (data protection notices) needs to be prominently displayed at the point of data collection – this can be expressed in the message or on a site (web or WAP).

Adequate information needs to be provided relating to:

- The identity of the Data User
- How the mobile number will be used
- The identity of any Third Parties who will gain the information disclosed
- What other data may be held about the individual
- Whether the data will be transferred to any other countries.



### **2.1.3 Privacy Policy**

Given the nature of these Guidelines, the disclosures suggested above naturally focus on transparency at the point of data collection as to the likely future uses of mobile phone numbers. There will doubtless be other data protection-related notices that the Data User will wish to make as a matter of law and best practice.

Since it may be inconvenient to provide this more extensive data protection notice at the point of data collection, general data protection Best Practice allows these other notices to be made elsewhere, by way of a clear and easy to understand "Privacy Policy".

This is on condition that if the mobile phone numbers and other personal data are being captured on-line, the Privacy Policy will be accessible in one click by way of a prominently flagged link above the submit button (as opposed to a "Privacy Policy" link in amongst various other general links to Terms and Conditions etc, or in a sidebar or only visible after scrolling to the very bottom of a web page). It should also be clearly accessible via a link from every email delivered.

If the data is being collected off-line, the Privacy Policy should be set out, as a matter of Best Practice, in full and attached to the material (such as an application form) used to collect the data.

Data Users will need to take care to ensure that their Privacy Policy is tailored to their particular needs, the expectations of their prospects and customers and consistent with their notification with the Information Commissioner's Office. The Privacy Policy should also set out the complete policy of the Data User with regard to personal data, and should therefore include, in a manner that is completely consistent with the data protection notice given at the point of collection, the policy as regards mobile phone number use. Please refer to section 20.17 of the DMA Code of Practice for further information.

Data Users will need to take guidance on the terms of their own particular privacy policy.

## **2.2 Data Hygiene**

Good list hygiene practices ensuring the quality of customer and prospect data are critical to developing consumer trust and help in facilitating message delivery.

Data Users should develop a policy that outlines the procedures which will be used to address: "Reply Handling", the "Processing of Un-Subscriptions", "Non Delivered", and "Number Validation". The goals of the policy should be to:

- Reduce incorrect, incomplete or outdated mobile numbers to a minimum
- Process "Mobile Unsubscribe Requests" (as soon as they are received)
- Suppress, not delete the individual's details

*Consumers have the option of objecting to unsolicited telephone communications through registering on the Telephone Preference List run by the Direct Marketing Association. As far as mobile marketing is concerned, consumers similarly are able to register their mobile telephone numbers on the Telephone Preference List. This means that marketers cannot make live marketing voice calls to such mobile numbers but will not necessarily be prevented from sending SMS messages. If a consumer has given their prior permission to mobile marketing messages, there is no need to regularly screen the Telephone Preference List.*



The Networks have defined a 'Universal Stop' policy to which all mobile marketers must adhere. It operates as follows:

<b>Short Code Service</b>	<b>Command</b>	<b>Resulting Action</b>
For single service short codes	STOP	All services will be ceased
New services on shared codes	STOP	This will stop the last service used by the subscriber as below
For existing multiple services on a single short code	STOP	The service last used by the subscriber will be ceased
	A further STOP instruction	This will stop subsequent services on the short code
	STOP ALL	This will stop all services on the short code

*This is designed to be simple to operate and to communicate.*

## **2.3 Marketing to children**

**SECTION PENDING APPROVAL FROM THE DMA BOARD.**

## **2.4 House Files**

### **2.4.1 Existing Personal Data**

Data Users should segment their base according to:

- Customers and prospects who have provided consent to receive mobile marketing, and who have not since unsubscribed
- Existing customers with whom the Data User sends marketing materials to on the basis of the Soft Opt In exception (as such individuals may only receive mobile messages marketing the 'similar products or services')
- Prospects or customers who do not fall into either of the above segments.

Going forward, the Data User may continue to send marketing mobile messages on the condition that:

- The recipient is given the opportunity to unsubscribe, each time an unsolicited mobile marketing message is sent
- Where the Soft Opt In is used, the content is, in terms of the products it is promoting, relating to similar goods and services to those in relation to which the recipient's data was first collected.



#### **2.4.2 New Personal Data**

When collecting new personal data for House Files, reference should be made to 'Collecting Data' (section 2.1) earlier in these guidelines

### **2.5 Obtaining Positive Consent**

**(Notify at point of obtaining details that information will be used by third parties, Opt-in, Soft Opt-in)**

#### **2.5.1 Opt-Out Consent**

This is where customers have been advised – at the point of personal contact details collection (including mobile phone number) – that mobile (or electronic) marketing messages will be sent to them unless they object. Remember a mechanism for objecting at that point of data collection must be given. Simply sending a marketing message containing an opt-out mechanism as the first point of objection does not comply with legal requirements.

An individual has the right at any time by written notice to a data controller to ask it to cease, or not to begin, processing their personal information for the purposes of direct marketing. Data protection legislation states that this right relates to marketing "*by whatever means*", so would cover all forms of mobile marketing just as it does mail, fax, telephone and email marketing. As far as mobile communications are concerned, the Information Commissioner permits the use of short codes as a valid address provided to consumers for marketing communication opt-out/unsubscribe requests. It is best practice to enable consumers to object to future direct marketing with the minimum effort and cost possible. If short codes are to be used for this purpose then it must be ensured that:

- i) The identity of the sender is clearly identified within the message;
- ii) The use of any such short code does not incur a premium rate charge for the consumer; and
- iii) The short code is valid at the time the SMS is sent.

The Information Commissioner has recommended that if a short code is to be used, consumers are informed of this short code in the body of the marketing message, for example:

*"[Company name] - 2STOPMSGSTXT'STOP'TO (add applicable 5 digit short code)".*

*Where it is clear that a recipient of a message wants to unsubscribe from further messages - even if they have not strictly followed the unsubscribe instructions provided correctly (such as if they text "unsubscribe" instead of "STOP") - it is best practice to unsubscribe them nonetheless.*

*It is also possible to give consumers the option of opting-out of communications relating to a particular service rather than marketing messages in general. The opt-out message could therefore refer to a particular service identifier also (such as a particular word or number). That way you are not prevented from continuing to send messages on other services that they do still wish to receive.*

In the event that customers are signed up to long-term promotions or seasonal services (such as those associated with sporting seasons) as well as providing them with the option to opt-out each time a communication is sent, it is best practice to also contact them at the start of each season to remind them what they have subscribed for, that the promotion/service is about to restart and an opt-out mechanism is given.



### **2.5.2 Opt-In Consent**

*This is where the mobile marketer gives customers the opportunity to actively choose to receive marketing messages from them. For this type of consent to be valid, not only must customers positively indicate that they wish to receive marketing messages, BUT if appropriate the notice that the mobile marketer provides must clearly explain that those marketing messages may contain information about other companies' products and services.*

## **2.6 Renting Lists**

### Host Mailings

The Data Supplier will send or instigate the sending out through their normal outsourcing arrangements, mobile marketing to their own mobile base, promoting the Data User's products and services.

The Data Supplier must have obtained positive consent from individuals to send host mailings, marketing types of products or services of the marketer.

The Data Supplier's mobile database is not passed to the Data User other than for the purposes of de-duplication.

The Data Supplier's name must appear in the message.

The Data Supplier manages the un-sub process as described under 'Data Hygiene' (section 2.2).

Questions that the Data User should ask the Data Supplier before entering into an agreement include:

- How and when the list was built
- Data Protection Notices and Privacy Policies present at the point of data collection
- Unsubscribe & Suppression Process
- Legal compliance in relation to collection of data

## **2.7 Deciding on the Target Group**

Targeting is a pre-requisite of any marketing activity. It is essential that the right message goes to the right audience at the right time.

The first stage of a mobile marketing campaign is to decide on what target group should be receiving the campaign, ensuring that the creative is suitable for the recipients. This is particularly important given the personal nature of the mobile.

Targeting can be facilitated using previous purchase history, profiling techniques and, most importantly, permission levels.

Certain types of promotion must be handled with particular care including the means of targeting – see 3.5.



## **3.0 Mobile Campaigns**

### ***3.1 What are the first/key things that need to be thought about when setting up a mobile campaign?***

- Ensure that the target market has given permission to communicate with them **specifically** via this medium
- Be clear about the data being used (preferably make sure that it has been collected in-house or that the exact collection methods are known)
- Ensure that the medium is appropriate to that specific offer/target group (what is trying to be achieved – e.g. SP v CRM – how will mobile support it?)
- Ensure that the message is appropriate for the medium (can it be communicated by text or via images)
- If the message includes any cost to the target market, ensure that it be justified and it is clear in the communication (remember that the consumer pays to send in a message and can be charged to receive any acknowledgement – or ‘bounce back’ – message, so make clear that they understand the full cost to them)
- If you are supplying any downloadable content as part of your campaigns (such as ring tones or wallpapers), ensure that the target market understands that such downloads are reliant on the compatibility of their handset and also how it will be charged
- Ensure that the mobile marketer will be clearly identified to the recipient
- Ensure that the message includes the ability for the recipient to opt out from further messages
- Set objectives and expectations (what response are you measuring? Are your expectations realistic? Etc.).

### ***3.2 Frequency of campaigns***

- This should be set by the target market or at least be agreed to be based on a clear and unequivocal statement of intent for use by the mobile marketer or the data collector.

### ***3.3 When the best times to communicate are***

- Generally avoid sending messages that the recipient will receive between the hours of 2200 and 0700. The obvious exceptions here are services that are time sensitive and for which the recipient has specifically opted in.



### **3.4 Core Elements of a campaign**

- Permission collection – only send messages to those who have consented to receive them otherwise data protection legislation is breached.
- Message Wording - The capacity to state information where mobile phones are used is limited compared to the internet and other forms of media but marketers are still required to provide information about significant conditions in a mobile promotion together with any other relevant factors likely to affect a consumer's decision to respond to a promotion by mobile (such as associated cost implications). Where SMS is concerned, as space is limited to 160 characters, the general use of abbreviations within the marketing message is permitted and it is also possible in some circumstances to refer to a website where consumers can obtain additional applicable conditions and information.

*Information about the marketing you intend to do can be given before you send a marketing message or even before you collect the mobile number in question (such as in an advert, or on a website where the intended recipient signs up for the service). Assuming the recipient has clearly consented to the receipt of mobile marketing messages (see section 2.1), it is best practice for each marketing message to:*

- i) be clearly identifiable as a mobile marketing communication;
- ii) clearly state the identity of the sender of the communication (for example beginning the mobile message with the words "From [company name]);
- iii) provide a valid unsubscribe option so that recipients can unsubscribe from marketing communications as they wish;
- iv) include a clear identification of any promotional offers together with an explanation of any applicable conditions; and
- v) include a means of accessing any additional information, terms and conditions, and any applicable privacy policy in the event that the communication is being used to collect personal details.

So far as point 5 above is concerned, due to the limitations in space associated with mobile communications, a reference to an associated website can be made and it should then be ensured that the website provides all relevant information associated with the mobile communication. By having a website referred to within a marketing message will not excuse marketers from providing the information required by points 1 to 4 above in the text of the marketing message.

*The marketing message could therefore look like the following:*

*From Cheapflights – be a winner with cheap flights to Turkey for footie final. Visit [www.cheapflights.com](http://www.cheapflights.com). Reply "STOP" to opt out of further messages."*



### 3.5 Those campaigns where we need to pay particular attention

- Marketing to children (see 2.3)
- Adult content (see 5.3)
- Gambling (see 'Betting & Gaming' section of the CAP Code and [http://www.cap.org.uk/cap/news\\_events/news/2005/Gambling+on+legality.htm](http://www.cap.org.uk/cap/news_events/news/2005/Gambling+on+legality.htm))
- Alcohol (see 'Alcoholic Drinks' section of the CAP Code and [http://www.cap.org.uk/cap/news\\_events/news/2005/New+Alcohol+Advertising+Rules+Launch+ed.htm](http://www.cap.org.uk/cap/news_events/news/2005/New+Alcohol+Advertising+Rules+Launch+ed.htm))
- Sales Promotion - The European Parliament Directive 98/27/EC concerning sales promotion in the 'Internal Market' is in its final draft. Were it to pass into law it would have potentially disastrous consequences for premium rate sales promotions. The legislation has been under 'consultation' for four years including the removal of some of the most damaging aspects from the mobile industry's viewpoint – only for these same points to be reintroduced. The latest draft (17.10.04) has been reviewed by the DTI in a Regulatory Impact Assessment designed to identify the implications for UK businesses.

One of the key objectives is to harmonise law so that pan European campaigns are easier to operate from a single set of obligations across multiple territories. Whilst this is laudable, it is fairly obvious that this approach also means that combined requirements will need to accommodate the toughest individual terms (i.e. the highest common denominator).

There are 3 possible big impacts:

- i) A requirement not to charge any associated costs, other than non-premium rates of postage or telecommunications, for participation in a promotional contest or game. This in effect prohibits premium rate entry for sales promotion campaigns
- ii) A requirement not to allow a person under the age of 16 to participate in a contest or game without prior consent of that person's legal guardian
- iii) A requirement to include extended information about the promotion (e.g. actual value of prize) at the time of the initial communication. It is feared that this may render commercial radio advertising as impractical for a number of advertisers wishing to use sales promotion mechanics.

The scope however is importantly limited in that it *excludes*:

- Promotional contests and games in which participation is exclusively subject to a prior obligation to purchase a promoted good or service;
- Promotional contests and games offering a cash prize or a total prize package that exceeds EUR 100,000 (c. £68,000) per separate good or service per year in value;
- Promotional contests and games in the editorial content of a media or where a media is the promoter.

The Regulation contains an implementation deadline of **1 July 2006** however this date has no legal status until the Regulation is itself adopted. Such adoption is reliant upon further discussion at which point the relevant UK bodies (including the DMA) will lobby against the damaging implications.



- Financial Services (see Appendix A)
- Subscription Services (ongoing billing) – in addition to the data collection, data usage and opt-out processes, ICSTIS requires action in one key additional area – that of reminders. These actions are split according to the value of the service as follows:

***Where the service is charged less than or equal to 50p inc VAT***

At least once a month the cost per message (inc VAT) must be advised. This may be at the end of a service message, **for example**: “Latest score England 15 France 3. Each text costs 50p”.

***Where the service is charged at more than 50p inc VAT***

At least once a month the following information must be sent to subscribers;

- Name of service
- That the service is subscription based
- What the billing period is (e.g. week, month)
- How much the user pays per billing period
- Service operator details including UK telephone number

These points must be included in the first message which the consumer receives and must appear before any promotional content.

This may be a free to receive message or the first of any billing messages. **Example** of good practice wording:

“Ringtone club: ur subscription is renewed and u have been charged £4.50 for Aug. U now have 12 credits go 2 [www.ringtoneclub.com](http://www.ringtoneclub.com) Customer services 0206 555 4444”s

### **3.7 Competitions, Draws and promotions**

*Any form of advertising or promotion in the UK must comply with British Code of Advertising and Sales Promotions (known as the CAP Code).*

*The Advertising Standards Authority has confirmed that the CAP Code also applies to SMS marketing communications. It applies where messages are sent to individuals in their private capacity either via their personal mobile phone number or their business mobile phone number. Due to the application of the CAP Code to mobile communications, any mobile message relating to a promotion of any description must provide certain information to the recipient within the promotional material. This is also the case with email and print promotions. Such details include the closing date of any competitions, eligibility restrictions, prize descriptions etc.*

*The Committee of Advertising Practice (CAP) issued guidelines in May 2004 to assist mobile marketers to interpret the application of the CAP Code to mobile phones.*

Also see Prize Promotions & The Law section of the CAP Code at <http://www.cap.org.uk/cap>.



## **3.8 Distance Selling Regulations**

### **3.8.1 Definition of Distance Selling**

Distance selling is the offering of goods or services to a consumer with a view to concluding a contract for those goods or services without the buyer and seller meeting face to face. Any offer for the purchase of goods and services that are available via mobile would therefore be considered to be made at a distance and fall under the provisions of the Consumer Protection (Distance Selling) Regulations 2000. The Distance Selling Regulations include a list of possible means of distance communication that would be caught within their scope and this includes videophones, so to conclude a contract by way of mobile video conferencing would also fall within the scope of this legislation. Some types of distance contracts such as those relating to sales of interest in land and financial services are exceptions to the rule and are not covered by the Distance Selling Regulations so legal advice is advisable when mobile is being considered as a tool to enter contracts.

Section 3.8 does not provide members with a comprehensive overview of the provisions of the Distance Selling Regulations, only an insight into the main provisions. Independent legal advice should therefore be sought when the ability to enter distance contracts is being considered.

### **3.8.2 Information to be provided to consumers prior to entering a distance contract**

**Prior** to the commencement of a distance contract, the supplier of the goods/services concerned must provide the consumer with the following information:

- i) the identity of the supplier and their address where payment is required;
- ii) a description of the main characteristics of the goods/services;
- iii) information relating to applicable prices (including all taxes);
- iv) delivery costs where applicable and the estimated time for fulfilment of an order;
- v) applicable arrangements for payment and delivery;
- vi) the existence of the consumer's right to cancellation (see below);
- vii) any applicable cost of using mobile to complete the transaction (such as if a premium rate telephone service is concerned);
- viii) details of any limitations on the offer such as geographic restrictions, period of availability of the offer or any other conditions that affects its validity; and
- ix) the minimum duration of the contract being entered into where appropriate.

If it is the intent of the supplier to substitute goods or services of an equivalent quality or price in the event that demand exceeds supply, consumers should be made aware of this fact and they should also be aware that the supplier will meet the cost of returning such substitute goods in the event that the consumer exercises their right to cancel the contract (see below).

When providing the consumer with this information it must be delivered in clear, plain language. Due to the space restrictions associated with mobile messages, this is again another example of where some basic information such as the identity of the supplier should be given in the initial SMS or WAP message and then the consumer should be given clear directions to an appropriate website where all applicable terms and conditions and information can be given. As the above information must be provided to the consumer **before** the transaction is commenced, it is important that consumers are given clear instructions as to how to obtain all relevant information on the website before they are able to enter into the transaction. The DMA Code of Practice also provides additional information on how consumers should be given applicable information.



### **3.8.3 Additional and written information to be provided to consumers following commencement of a distance contract**

In addition to the information which must be given to consumers detailed in section 3.8.2, prior to the conclusion of the contract or at least no later than the time of delivery (where goods are concerned) or in good time and in any event before the service has been fully performed (where services are concerned), the following information must also be provided:

- i) confirmation of the information listed in section 3.8.2;
- ii) information about the consumer's right to cancel the contract and details relating to the conditions and procedures to be followed to exercise this right (such as who is responsible for the return of cancelled goods and the cost of returning or collecting them);
- iii) the geographical address of the supplier;
- iv) information regarding any after-sales service and guarantees; and
- v) the conditions for exercising any contractual right to cancel a contract of unspecified duration or duration exceeding one year.

The Distance Selling Regulations dictate that this information must be provided in writing or in another durable medium that is available and accessible to the consumer (such as using email nowadays).

#### ii. Consumers' right to cancel distance contracts

Consumers have the right under the Distance Selling Regulations to issue a notice of cancellation with a defined cancellation period to cancel the distance contract. The cancellation period applicable begins on the day the distance contract is concluded and ends either:

- i) in the case of goods – on the expiry of 7 working days beginning the day after the day on which the goods are delivered; or
- ii) in the case of services – on the expiry of 7 working days beginning with the day after the day on which the contract was concluded.

The above cancellation periods apply where the supplier has complied with the information requirements detailed in section 3.8.2 above. Where these requirements have not been complied with within the correct timescales but the information is supplied to consumers within 3 months following the day after the date the contract is concluded where services are concerned or the day on which the consumer receives the goods in question, the cancellation period then expires 7 working days from the day after the date the consumer received the necessary information. In the event that the supplier does not comply with the information requirements detailed in section 3.8.2 at all then the consumer has the option to terminate the distance contract up until 3 months and 7 working days beginning with the day after the date the consumer receives the goods or the contract for services is concluded.

Unless the parties to a distance contract agree otherwise, a consumer may not exercise this cancellation right where the contract concerns matters including (i) services already commenced before the end of the cancellation period; (ii) goods/services where price is dependent on financial market fluctuations; (iii) goods supplied to the consumer's specifications; and (iv) gaming and lottery services etc.

If a consumer does opt to cancel a contract, the supplier must reimburse any sum already paid by the consumer within 30 days from the cancellation notice and any related credit agreements will also be terminated.



## **3.9 Bluetooth Campaigns**

### **3.9.1 What is Bluetooth marketing?**

[Bluetooth](#) mobile technology offers marketers a unique opportunity to reach people in a location specific area with rich content but without the cost and complexity of the mobile networks' SMS and MMS technology. With Bluetooth anyone with a Bluetooth enabled mobile device can instantly receive rich content including coupons, single track song downloads, short video clips, even links to WAP micro-sites.

### **3.9.2 Do I need consent from people before using Bluetooth marketing?**

Bluetooth technology does not broadcast to all devices, but instead actively listens for devices as they come into range and formulates a message specific to that unique device. This is akin to using a mobile phone number to communicate with the handset. Therefore the same standards should apply as any other form of mobile marketing such as SMS marketing. This means that you need consent from the intended recipient before sending a Bluetooth marketing message to their handset. See previous FAQs on consent.

### **3.9.3 Surely if someone has their Bluetooth device “on”, I can assume that they have consented?**

Unfortunately, manufacturers of equipment that include Bluetooth set up their equipment in different ways. This means that the person that you intend to communicate with may have simply bought a device that has Bluetooth active and set to “discoverable” – they may however not be aware of this. You therefore cannot infer consent from the fact that a Bluetooth is in that mode. You must obtain consent to the use of Bluetooth marketing. See FAQ below: *How can I use Bluetooth marketing in compliance with the Privacy & Electronic Communications Regulations 2003?*

### **3.9.4 How can a consumer clearly and distinctly be given the opportunity to object to being contacted?**

It is difficult for people to express an opt-out request to a Bluetooth marketing system. They may not know what content to send and or where to send the content to express an opt-out request. There is no concept of “Reply” to Bluetooth because Bluetooth is not a message solution. Thus there is no option to “Reply with the word STOP” as you would find in SMS marketing. See FAQ below: *How can I use Bluetooth marketing in compliance with the Privacy & Electronic Communications Regulations 2003?*

### **3.9.5 How can I use Bluetooth marketing in compliance with the consent requirements of the DMA Code of Practice?**

One such solution may be to promote the availability of Bluetooth content on traditional media (poster or other OOH media) and invite people to “pair” with the marketing campaign. When someone wants to opt-out, they can delete the pairing. As long as a person’s device is paired to the marketing campaign, the device is eligible to receive marketing messages. The first message to the device could explain that in order to opt-out of future marketing messages, they need only to delete the pairing.

A further potentially compliant implementation for Bluetooth marketing involves a 3<sup>rd</sup> party downloaded application. Based upon an application that is downloaded to the mobile device a consumer can activate the application and then send and receive content via Bluetooth. Samples of this type of application were recently presented by Viacom and Kameleon and Jellingspot. The application may be either Symbian or Java or Windows ME based.



### **3.9.6 How does *Bluetooth marketing compare to marketing via Infrared?***

Infrared marketing offers many of the same benefits of Bluetooth marketing in that it offers consumer content in a location specific construct. Consent for infrared marketing is implied in that a person must actively direct their infrared enabled device towards the marketing system's infrared transmitter to receive the content. Casual "walk near" contact is highly unlikely to occur. The connection is only valid for as long as the device is directed at the transmitter and thus opt-out is as simple as walking away.



## 4.0 Standard Metrics for Measurement & Reporting

### 4.1 Limitations on Reporting (*What to expect*)

One of the key benefits of mobile marketing - much like e-mail and the Internet - is the ability to view the campaign actions in a very short time scale. The benefit to the practitioner from this speed of reporting is that the effectiveness of a campaign can be viewed immediately, allowing decisions on subsequent campaign content and targeting to be made in an accurate and timely fashion.

Reports themselves can be produced in a number of ways, via an on-line reporting tool, through bespoke reporting applications or as a simple excel spreadsheet.

Delivery Metrics:

- SMS – Number of messages sent, number delivered, number bounced, number of stop messages and number of replies – where promotion of downloads is promoted via SMS, metrics can show the number of pieces of content purchased and value
- MMS – Number of messages sent, number delivered, number bounced, number or replies, number of stop messages number of opens and click throughs – purchase tracking
- WAP Push – number sent, number delivered, number bounced, number opened, number of click throughs – purchase tracking

For MMS and WAP Push

Open rate

The number of opened messages can be ascertained by using an image (gif) look up when the message has been opened.

Click through rates

Where URL links are available within the message or WAP push, the number of people clicking onto each link can be measured.

Purchase tracking

This can take place in all 3 applications in different ways.

SMS - When using an SMS message to promote the sale of a piece of content, e.g. a ring tone, the number of people downloading the ring tone and the total value of the sales can be measured.

MMS and WAP – As there is the ability to browse from an MMS and a WAP push, the reporting available can track the number of purchases made on a WAP site. This is the same as web based reporting.

The reporting available will depend on the supplier used and the nature of the messages. Not all suppliers will be able to report on all the aspects mentioned above.



## 5.0 Additional Points

### 5.1 Are there any special requirements if I am using premium rate numbers?

*The use of premium rate numbers and services is subject to the regulatory regime of the Independent Committee for the Supervision of Telephone Information Services [ICSTIS] which regulates such services in their entirety – their content, promotion and overall operation, alongside existing legislation and other codes such as the advertising CAP Code. Premium rate services offer some form of content, product or service that is charged to the user's telephone bill or is deducted from prepaid credit on prepay mobile phones. In the mobile world, such services include mobile phone ringtones, logo downloads, or subscription services such as a daily joke that is sent to the subscriber's handset. Such services are usually advertised on 090 codes, and in the mobile world may also use short access codes as a response mechanism that causes a premium rate charge to be applied to the user's bill or prepay credit.*

*ICSTIS regulatory requirements are set out in their code of practice that can be found on their website<sup>1</sup>. The code is set out in separate sections dealing with:*

- administrative provisions for service providers wishing to use a premium rate number or offer a premium rate service, including the requirement to obtain prior permission from ICSTIS where the intended service is one that attracts specific obligations.
- General provisions for service providers including specific requirements on providing information about the costs involved in using or subscribing to the service, as well as the promotion of such services and their costs.
- live services such as chatlines, services offering counselling, sexual entertainment services etc.
- sensitive services such as those aimed at children<sup>2</sup>, or specifically adult services such as sexual entertainment, betting, virtual chat and dating services.

*In allowing their network to be used for premium rate services, network operators are required (as a condition of their operating licence) to secure the service providers agreement to comply with the ICSTIS Code of Practice and this is therefore likely to be an obligation within any contract with network operators that content providers and marketers may have.*

*The CAP Code guidance relevant to mobile marketing also makes it clear that the ICSTIS Code of Practice must be complied with and that it is equally applicable to mobile messages that are both **sent and received** by the mobile marketer. It must therefore be ensured that:*

- i) *consumers opting-out of future direct marketing must not be charged for this right at a premium rate; and*
- ii) *consumers whose only method of entering a prize draw is via a mobile facility must not be charged at a premium rate.*

*If a phone number is therefore to be given for recipients of mobile communications to opt-out of further communications, it should be ensured it is a standard rate number, or even better, a free phone number.*

<sup>1</sup> <http://www.icstis.org.uk/>

<sup>2</sup> For the purposes of the ICSTIS code, a child is any person under the age of 16.



*ICSTIS investigations may arise in one of two ways – either as a result of complaints received or as a result of action initiated by ICSTIS Secretariat. Following investigation the ICSTIS Secretariat will prepare an investigation report for the Adjudications Panel. Sanctions range from requiring the service provider to remedy the breach to levying a fine or requiring the service provider to pay compensation to the affected individuals. In exceptional circumstances and where the ICSTIS Secretariat determines that a breach is serious and an urgent remedy is required, an emergency procedure may be used, which may result in ICSTIS requiring the network operator to withhold payment and/or block access to the relevant service or numbers. Further information on the lawful and appropriate use of premium rate numbers or services should be obtained from ICSTIS who can be contacted via their website.*

## **5.2 Location based mobile marketing**

This section outlines the EU Working Party 29 Opinion on the use of Location Based Services (LBS) along with the existing rules and Best Practice on the subject. It is worth noting that LBS may or may not always constitute direct marketing. LBS may be enhanced with marketing that takes advantage of location information, but LBS is not *inherently* direct marketing.

We should start with some definitions. The use of location within mobile messages/transactions really covers three different areas:

- The Mobile Networks' definition of LBS – relates to the transfer of personal location data via their networks (as identified by the grid reference of the cell in which a subscriber's mobile phone was last located, to infer the subscriber's location and thereby provide a valued added service.)
- The legislative definition of LBS – relates to the transfer of location data by any means (inc GPS which is independent of mobile networks and more accurate)
- The marketers' definition of LBS – may well relate to the transfer of location data as provided by the consumer themselves (e.g. by providing a postcode within a mobile location service or by using non network proximity services such as Bluetooth, Infrared, RFID and WiFi,). It should be noted however that postcodes are not personal location data and that Bluetooth for instance also does not reveal the mobile number of the subscriber, therefore neither of these applications relate to 'personal data' in the legislative sense.

For the reasons, above is suggested that the more generic term Location Based Marketing be used to cover all of these applications. This will allow members to consider all of the implications of location based activity before looking at the specifics of their application.

NB: New technology is around the corner that will enable some mobile devices to be equipped with their own GPS (Global Positioning System) technology such that the device can report its location based on satellite positioning. This is to be borne in mind for the future as it obviously is another form of LBM with implications on 'personal data'.



### Service & User Types

In addition, discussion of LBM usually differentiates between Active/Passive and Target/Non-Target uses.

The two service types are:

- An Active (pull) service results in the location of the subscriber being revealed once, following an action on the part of the subscriber
- A Passive (push) service allows the service provider to track the subscriber on an on-going basis after an initial opt-in only. Sometimes a Passive service results in a Push message to the consumer; other times a third party is informed of the location.

The two user types are:

- A Target user usually *instigates* the action themselves (e.g. searching for a local service according to where the Target user is located)
- A Non-Target user's location is identified as a result of an action by someone else.

Therefore most, though not all, Non-Target services are Passive and most Target services are Active.

Governance: The DPA and PECR address LBM directly but not in great detail. In the UK a working group of nine leading LBS providers (LSP) has developed an Industry Code of Practice (but for Passive services only). An EU Working Party has recently attempted to address the issues not covered by the DPA and PECR and there is a great deal of overlap between their findings and the UK Code. More detail follows below.

#### **5.2.1 Existing legislation concerning LBM**

The UK's Privacy and Electronic Communications (EC Directive) Regulations 2003 (the "Regulations") define "location data" as being any data processed in an electronic communications network which indicates the geographical position of the terminal equipment of a user of a public electronic communications service. Data relating to the specific location of the terminal equipment concerned; the direction of the individual's travel and the time the location information was recorded is all considered to be location data. Generally, location data may only be processed where the user/subscriber of the public electronic communications network/service concerned cannot be identified from the data or the processing of the data is necessary for the provision of a value added service with the consent of that user/subscriber. Even when location data is processed in accordance with the Regulations for a value added service, the processing must be restricted to what is 'necessary' for those purposes and only the public communications provider concerned, a third party actually providing the value added service or a person authorised by either of these parties may process the location data.

Where location data also relates to individuals and either on its own or when put together with other data it can identify an individual, the provisions of data protection legislation also need to be complied with where location data is processed.



### 5.2.2 The EU Working Party

In November 2005, the EU's Working Party began looking at the primary issues affecting the use of personal data in, and resulting from, the use of LBM. There has been a significant rise in these services such as -

- i) 'Target' requested services such as find the nearest chemist to my current location or tell me when my friend is in the area
- ii) 'Non-Target' requested services such as locate my employee or child to their current position.

The distinction between Target and Non-Target is a subtle one because in both cases the service will only work with knowledge of the location of the subscriber him/herself.

The Working party isn't seeking to change or add to existing legislation governing LBM or data protection but to 'spell out how some of its provisions should be applied'.

The specific issues it highlights are:-

- i) National law – that the data controller is subject to the laws of the territory in which that controller is established and NOT where the user is resident or their data is generated (so a company operating via a site in India but tracking a UK consumer would be subject to Indian law). Moreover, any data transferred across borders would be subject to the requirements of data protection legislation (8<sup>th</sup> principle) governing such transfers and what is considered to be acceptable protection offered by the territory to which the data is transferred (for example Safe Harbour considerations applicable to the USA).
- ii) Informing Data Subjects – The current Regulations state that prior to obtaining the consent of an individual to process location data for the purpose of providing a value added service, the LBS provider must inform the individual concerned of a) the purpose of the data processing, b) the types of location data that will be processed, c) the duration of the processing and d) whether the data will be handled by a third party for the purpose of supplying the service concerned. Once the individual has provided their consent to the processing of their location data, they have the right to withdraw this consent at any time and they must be given the opportunity (via a simple and free means) to withdraw their consent in respect of any individual connection or transmission concerned. Data protection legislation and best practice must also be followed from a data protection perspective (such as the identification of the data controller concerned and notifying the individual of their data protection related rights and ability to opt-out of communications received).

The Working Party says that this information should be supplied by the Service Provider or by the Networks owning the user relationship where the Service Provider is not in direct contact with the individual. It is recommended this information is provided either in the T&C's (with ongoing access to this via a site for instance) or each time the service is used.

- iii) Obtaining consent for the processing of location data – the Working Party says that this cannot be collected by implication merely by service details being included in the T&C's. It must be explicitly given by the individual concerned so that consent is informed and freely given. It may be collected for a single or an ongoing service as long as it is in accordance with data protection legislation.



- iv) Entities required to obtain the data subject's consent – Depending on whether the service is supplied by the Network Operator or a third party, consent must be obtained by one or the other. The Working Party suggests that a trusted third Party might be set up to handle incoming requests for services which utilise location data which would then pass all service requests to the relevant end user Service Providers. The Service Providers which would deliver the service via the third party operator without identifying the individual requesting the service. It is just an idea. In any event, operators need to introduce measures to verify and authenticate requests for access to location data by third parties offering value added services.
- v) Ensuring Consent Is Valid – to ensure that an individual who has consented to a LBS is the same individual that the location data relates to, the Working Party states that consent must at least be confirmed by (a) sending a message to the user's terminal equipment after consent has been collected confirming the subscription to the service and (b) if necessary also requesting a confirmation of the subscription (i.e. double opt in) from the user.
- vi) Right to withdraw – the data subject has the right to withdraw from the processing of their location data at any time via simple and free means (such as Universal STOP). The Working Party believes that individuals should be kept informed of their right to withdraw, not only when they subscribe for a service but also when they use it.
- vii) Data Storage Time – data can be stored 'only for the duration necessary for the provision of a value added service'. Unless the data is needed for billing purposes, it should not be otherwise retained (so unless the service provider is a Network, that means it should be deleted once the service is provided although it's not clear whether this means the single transaction or a period of subscription)
- viii) Transmission of Personal Data to 3<sup>rd</sup> parties – data cannot be transferred to any party other than that which provides the service on behalf of the user or the Networks.

The Working Party also looked at a number of more specific issues around particular *service types*:

- ix) Location of children – there must be a balance between the right of the parent to monitor their children's whereabouts from a safety perspective and the right of children to avoid (in the words of The International Convention On The Rights Of Children) 'being subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence'. The most practical aspect of this is that the Service Provider must 'introduce appropriate procedures' to ensure that people claiming to be parents are actually so and that no one else can access such a service. They should also ensure, as far as possible, that the person being tracked via the phone is actually the phone owner
- x) Location of employees – data processing that enables an employer to locate a person directly (e.g. via handset) or indirectly (e.g. via vehicle), uses personal data and the employer must therefore comply with the provisions of data protection legislation. The Working Party is of the view that the processing of location data on employees must correspond to a specific need on the part of the employer. Employees should therefore give their express consent to the processing of such data as part of their employment and consent should also be addressed by 'all the relevant stakeholders'. The reason for tracking a person must be justified (e.g. tracking a package or resource planning); it might be considered 'excessive' if applied to people who organise their own travelling or where undertaken solely to monitor the person's work where another means might instead be used. In any event, no location data should be collected on employees outside of their working hours.



### **5.2.3 The UK Networks**

The UK Networks developed a Code of Practice back in September 2004. This distinguishes between Active services and Passive services.

The Code of Practice focuses on Passive services only, where the location data is supplied by the Networks (i.e. the cell location of the individual) without each check being initiated from the subscriber's handset.

The bullet points of the Code are:

- i) Only a parent or guardian can open an account used to locate a child under the age of 16 (so that the child can only participate in such a service with their parent or guardian's permission).
- ii) A parent or guardian must provide proof of ID and address when registering.
- iii) Child location services must be marketed responsibly and must not exploit parents' concerns or fears.
- iv) The Service provider must ensure that consent is actually submitted from the mobile device to be tracked – no service must be supplied if this is not verified. Once the service starts, Service providers must continue to verify this
- v) Services must not be used to undermine privacy or for any form of unauthorised surveillance. Services to corporate users (such as companies monitoring staff) must make clear this legal requirement on the employer.
- vi) Service Providers must send out a confirmation of the service to the subject. This should preferably be in the form of a SMS to the subject. Service Providers must similarly send to consumers using the service, random and periodic SMS alerts to remind them that other people can track their location. The code lays down a minimum recommended frequency for such reminders based either on elapsed time or on the number of location requests.
- vii) Services must be 'easy to use' and all such information must be available via phone help lines, web and WAP sites.
- viii) All services must be easily terminated via Universal STOP.
- ix) Locatees must always be able to easily identify those who are able to locate them. They must also be told the exact type of information made available when their handset is switched off.
- x) Where practical, consents, alerts, suspensions and terminations should all be handled via SMS.

At the time of issue, this agreement was signed by the 4 networks (not therefore Three), plus a number of 'aggregators' and several service suppliers and data contributors such as Ordnance Survey. This code is more explicit than the MMA Code and actually addresses some of the issues raised by the EU Working Party.

Service providers who provide a subscription services which involve the processing of data location should also be mindful of the UK mobile operators' code of practice relating to subscription services and their marketing materials. This code came into force during August 2005 and now forms part of the contract that service providers will enter with their chosen network operator.



### **5.3 Special requirements regarding the use of adult content**

*The UK based mobile network operators have created a joint code of practice for the self-regulation of new forms of content on mobile phones to address parental concerns about inappropriate or adult content being sent to children's handsets. A copy of the code of practice can be obtained from the website for the Independent Mobile Classification Body<sup>3</sup> [IMCB]. The key element to this code of practice is the appointment of an independent classification body responsible for providing a framework for classifying commercial content that is only suitable for customers aged 18 and over. The IMCB, which is a not-for-profit subsidiary of ICSTIS, is the body thus appointed.*

*The remit of IMCB is to provide a classification framework against which commercial content providers can self-classify their own content as 18 where appropriate. Such content will be placed behind Access Controls so that, when combined with age verification arrangements, it is only available to those identified as 18 or over.*

*The following services are covered by the IMCB classification framework:*

- Still pictures;
- Video and audiovisual materials; and
- Mobile games, including java-based games.

*The following fall outside the IMCB remit (but are governed by legislation as well as other applicable codes of practice):*

- Text, audio and voice-only services including those delivered as a premium rate service and therefore ICSTIS regulated (see above).
- Gambling services (because these are already age restricted by UK legislation).
- Moderated and unmoderated chat rooms (commercial unmoderated chat rooms will only be accessible by those aged 18 or over).
- Location based services (see 5.2).
- Content generated by subscribers, including web logs.
- Content accessed via the internet or WAP where the mobile operator is providing connectivity only.

*In general, content that falls within the following categories should be classified as 18 – any content encouraging unlawful underage activity such as underage drinking or gambling, frequent and repetitive use of strong foul language, actual or realistic depictions of sexual activity, nudity, graphic violence, illegal drug taking, horror, or activity that encourages imitation such as ear-claps, head-butts etc.*

*It is intended that mobile operators will implement access control mechanisms via which they will verify the age (ie 18 or over/under) and will block commercial content rated 18 or over from reaching the handsets of their users and subscribers aged under 18.*

---

<sup>3</sup> <http://www.imcb.org.uk/classificationframe/>



## **6.0 Complaints and Dispute Resolution**

### ***6.1 Direct Marketing Authority & Code monitoring & Enforcement Procedures***

DMA members must comply with the provisions of the DMA Direct Marketing Code of Practice. Non-members are strongly advised to comply with the Code as it is a useful summary of the legal and best practice requirements for direct marketers. Section 20 deals specifically with mobile marketing.

The DMA's Compliance Department monitors the activities of DMA members, through compliance visits, mystery shopping and annual questionnaires.

The DMA has established The Direct Marketing Authority to enforce the provisions of the Code, where compliance has not been achieved. The Authority operates and is funded independently of the DMA. The members of the Authority are an independent Chairperson, a minimum of three further independent members and a minimum of three industry members acting in their individual capacities. The Authority investigates all unresolved consumer complaints against DMA members whether received directly or through the DMA. If the Authority finds that a member is in breach of the Code it can impose a variety of sanctions ranging from an undertaking from the member that the breach will not be repeated to expulsion of the member from the DMA. Members have the right to appeal against a ruling by the Authority to the Appeals Commissioner.

Members must also comply with the provisions of The British Code of Advertising, Sales Promotion and Direct Marketing (CAP Code), which is enforced by the Advertising Standards Authority (ASA).

Mobile marketers must also comply with the Code of Practice and Guidelines issued by The Independent Committee for the Supervision of Standards of Telephone Information Services (ICSTIS).



## 7.0 Additional Requirements to be considered

### 7.1 *The Stewart Report*

Ongoing fears about the safety of mobile (around both handsets and masts) have been raised by the National Radiological Protection Board's (chaired by Sir William Stewart) report. This is an update of an earlier report published in 2000 and covers a large volume of research that has been undertaken in the intervening years. Whilst the focus has been the health effects of masts and infrastructure, concerns have also been raised about the use of handsets and the radioactivity created by them particularly on the brains of young children. The Stewart Committee's report found that 'there is no hard evidence at present that the health of the public in general is being affected adversely by the use of the mobile phone' – however the report recommended that 'particular attention be given as to how best to minimise exposure of potentially vulnerable sub groups such as children.....who may be sensitive to airwaves'. This has proven sufficient for a number of parents and parental groups to raise serious concerns. These Best Practice notes relate to **non-voice** applications however it is pertinent to note these concerns around voiced applications too.



## Appendix A

The Following applies to all members offering consumer financial products and services, including:

- a) investment opportunities, including the giving of investment advice, managing or arranging investments, buying, selling, subscribing for or underwriting investments, banking, life-based insurance and pure protection policies, collective investment schemes and funeral plan contracts
- b) mortgages and mortgage advice
- c) general insurance and insurance advice
- d) consumer loans.

### Definition of Distance Contract

For the purposes of the following document, a distance contract for financial services is any contract concluded between a supplier and a consumer under an organized distance sale or service provision scheme run by the supplier, who, for the purposes of that contract, makes exclusive use of one or more means of a distance communication up to and including the time at which the contract is concluded.

### Legislation

Members issuing commercial communications for financial products must comply with all relevant legislation, the most recent and applicable being the Financial Services and Markets Act 2000 and ensuing Orders, with particular reference to the Financial Services and Markets Act 2000 (Financial Promotion Order) 2001 as amended in 2001, 2002 and 2003. The Financial Services (Distance Marketing) Regulations 2004 implement the EU Distance Marketing of Consumer Financial Services Directive 2002 (DMD) and are designed to cover any "gap" services or products not governed by the Financial Services Authority (FSA). In addition, there are the FSA Rules implementing the DMD, which will amend sections of the FSA Handbook. These rules have also been incorporated into the FSA Mortgage Conduct of Business Rules (MCOB) and the Insurance Conduct of Business Rules (ICOB) as these products fall within the FSA's jurisdiction. Members issuing commercial communications for consumer credit products must also comply with the Consumer Credit Act 1974, The Consumer Credit (Advertisements) Regulations 2004, The Consumer Credit (Disclosure of Information) Regulations 2004, The Consumer Credit (Agreements) (Amendment) Regulations 2004 and The Consumer Credit (Early Settlement) Regulations 2004.

### FSA

Members issuing commercial communications for financial products regulated by the Financial Services Authority (FSA) must either be authorised to do so by the FSA, or be acting on behalf of organisations that are authorised to do so by the FSA. If members are acting on behalf of an authorised organisation, this fact must be clearly disclosed. All such communications must comply with the FSA's Handbook of Rules.



Contents of financial offers

Offers for financial products must clearly indicate the nature of the contract being offered and must be expressed in simple terms so that recipients are in no doubt as to the commitment they are entering into.

Information to be included

In good time before being bound by any distance contract or offer for financial services, the consumer must be provided with the following information in a clear and comprehensible manner:

<b>Description</b>	a description of the main characteristics of the financial product being offered
<b>Price</b>	the total price, including all related fees, charges and expenses and all taxes paid via the supplier or where the exact price cannot be indicated, the basis for the calculation of the price
<b>Limitations</b>	any limitations, penalties and the terms of withdrawal
<b>Rates of interest etc</b>	the basis used to calculate any rates of interest, forecasts or projections
<b>Warning notices - risks</b>	warning notices regarding the existence of special risks associated with features of the product and an indication that the value of the product may vary and, unless guaranteed, can go down as well as up
<b>Guarantees</b>	where the value of the product is guaranteed, details of the guarantee offered
<b>Warning notices - past and future performance</b>	warning notices that past performance or experience does not necessarily give a guide for the future (any examples used must not be unrepresentative)
<b>Taxes/extra costs</b>	where applicable, an indication that other taxes and/or costs may exist that are not imposed by or paid via the supplier
<b>Validity of offer</b>	any limitation of the period for which the information is valid
<b>Payment and performance</b>	arrangements for payment and performance
<b>Cost of communicating</b>	any specific additional cost for the consumer of using the means of distance communication to accept the offer in question
<b>Details of the supplier</b>	full details of the supplier, and any relevant representative, including:
<b>Identity</b>	their identity and main business



<b>Address</b>	the geographical address at which the supplier, and any relevant representative, is established and any other relevant address
<b>Registration number</b>	any registration number or equivalent relating to any trade or similar public register in which the supplier is entered and, where relevant, full details of any representative of the supplier in the consumer's country of residence and
<b>Other professionals involved</b>	details of any professional involved in the sale of the product including identity, geographical address and the capacity in which that person is acting
<b>Details of contract</b>	details of the contract including:
<b>Right of withdrawal</b>	the existence or absence, except in certain specified circumstances, of a right of withdrawal and where the right of withdrawal exists, its duration (as required by law) and the conditions relating to the right. Information must also be provided on the amount that a consumer may be required to pay where withdrawal from a service takes place after commencement. Information must also be provided, inter alia, on the address to which the withdrawal notice should be sent
<b>Duration of contract</b>	the minimum duration of the contract in the case of financial services to be performed permanently or recurrently
<b>Early termination of contract</b>	information on any conditions or penalties applying to early termination of the contract
<b>Applicable law</b>	an indication of which country's law will apply (within the EEA) to the particular distance contract and any contractual clause on law applicable to the distance contract and/or competent court
<b>Language to be used</b>	the language in which the contractual terms and conditions and prior information as detailed are to be supplied and the language used, with the consumer's agreement, to communicate for the duration of the contract
<b>Redress</b>	any information on redress mechanisms and methods of access to them the existence of any guarantee funds or compensation arrangements.

#### Consumer Credit Advertisements

All advertisements must use plain and intelligible language, be easily legible, and include the name of the advertiser.



### Content of consumer credit advertisements

If a credit advertisement displays an amount (in monetary Terms) relating to any of the following key linked indicators then all the following key indicators must be shown together as a whole, with equal prominence and a second category of financial details. The key indicators are:

- a)** the frequency, amount and number of payments
- b)** notification of other charges and fees associated with the credit such as annual fees and broking fees
- c)** the total amount payable
- d)** the typical APR.

The second category of financial details are:

- a)** the amount of credit - either the actual amount, or an indication of the range of credit available
- b)** the amount of deposit, if one is required
- c)** the cash price of the goods or services purchased (where appropriate) and
- d)** any advance payment if required.

The typical APR must be displayed in the same place as the other information and one and a half times the size of the other information. The postal address at which the advertiser may be contacted will also have to be shown, except for advertisements that appear in retail premises, that contain contact details for dealers or credit brokers, or are broadcast on radio or television.

### Advertisements for secured lending or hiring

Advertisements of this type must reveal that security is required and state the nature of that security. If the security for a loan takes the form of a mortgage or charge over the borrower's home then the appropriate statutory wealth warning must be shown with the required prominence.

### APR

Only one typical APR may be displayed in each advertisement. However a single piece of advertising copy may contain multiple advertisements. The typical APR must be accompanied by the words "typical", "variable" (where required) and denoted as "% APR".

The typical APR must be shown:

- a)** where any other interest rate or other APR is quoted
- b)** where any of the key financial information in the Content of consumer credit advertisements section is shown
- c)** where any part of an advertisement indicates that credit is available to those individuals who otherwise may find it difficult to obtain credit, for example "CCJs - no problem"
- d)** Where any favourable reference is made about the credit or nature of repayments or interest i.e. "low interest": "cheap loans" - etc
- e)** Where any incentive is offered.

The typical APR must represent the rate at or below which the advertiser reasonably expects to apply to at least 66% of agreements entered into after and as a result of the advertisement. A "from APR" may be quoted but this must be the lowest APR that the advertiser reasonably expects at least 10% of those being given credit on or after the date of the advertisement to receive. It will have to be



accompanied in the advertisement by a corresponding "to APR" representing the actual highest APR on offer. Both rates must have equal prominence. The 66% typical APR must be shown with greater prominence than the upper and lower figures.

Restrictions on certain expressions in credit advertisements

The following expressions are prohibited where they do not reflect the reality of the product on offer, "overdraft", "interest free", "no deposit", "loan guaranteed", "pre-approved", "gift", "present", "weekly equivalent".