GENERAL GUIDANCE NOTE

Due diligence; risk assessment, and control on clients

Who should read this?

All Network operators and providers involved in the provision of premium rate services ('PRS') to consumers. It is important that senior management have considered matters addressed by the guidance with a view to establishing the right framework and effective processes (including supervision) for due diligence, risk assessment and control (DDRAC).

What is the purpose of the Guidance?

Under the Phone-paid Services Authority's Code of Practice, all Network operators and providers must carry out due diligence and risk assessment on any parties they contract with that form part of a value-chain delivering premium rate services to consumers. Due diligence and risk assessment and control represent separate and distinct processes that take place prior to the commencement, and throughout the duration, of a commercial agreement respectively. This General Guidance Note is designed to clarify the Phone-paid Services Authority' expectations as to how these processes should be performed in practice.

What are the key points?

The Phone-paid Services Authority believes that due diligence and risk assessment and control processes are central to good business practice. These processes are particularly important in the premium rate services market, where services are delivered to consumers through partnerships between Network operators and providers, which can, on occasion, include many different parties.

The Phone-paid Services Authority' expectation is that each party in a PRS value-chain will carry out due diligence prior to contracting with another party to provide a PRS. This should include an understanding of that party's history of compliance with the Phone-paid Services Authority's Code of Practice, including any breaches of the Code of Practice. Once contracted, we expect there to be ongoing risk assessment and control mechanisms in place, appropriate to the roles of the parties involved, which ensure that the Phone-paid Services Authority's Code of Practice is complied with.

The procedures set out in this General Guidance Note are designed to assist Network operators and providers in developing due diligence and risk assessment and control processes that are fit for purpose, recognising that any systems implemented must be proportionate and relevant to their business operation.

1. Desired outcomes – what we believe good DDRAC involves

1.1 The PRS industry value chain forms a connection from the providers of products and services to the consumers – customers of one of a range of telecommunications network operators, both in the fixed line and mobile space. Such connections enable the purchase of products and services quickly and easily when chosen by consumers; however, they also equip companies and individuals with the opportunity to, among other things, apply unwanted charges to people's phone bills. DDRAC is essential to establish the key commercial connections and to prevent or limit the abuse of PRS numbers and shortcodes.

1.2 The Code requires both carefully managed due diligence to be undertaken prior to contracting with other parties in the PRS value chain[1], and compliance with the obligations related to risk assessment and control mechanisms which are found at paragraph 3.1.3(a) and (b):

"*All network operators, Level 1 and Level 2 providers must . . . assess the potential risks posed by any party with which they contract in respect of:*

a. the provision of premium rate services, and
b. the promotion, marketing and content of the premium rate services which they provide or facilitate,

and take and maintain reasonable steps to control those risks."

1.3 DDRAC enables all parties in the value chain to be confident that the connections that are established are for good positive business and industry-wide growth. Such processes are built on the following four cornerstones:

- **Know your client** – all businesses have risks, and these can vary significantly dependent on the nature of the company and the services being operated. It is important to know your client so you can properly identify the risks involved and assess how to manage them. This is not to limit or prevent commercial relationships forming, but to ensure they are properly managed whether an issue ultimately arises or not.
- **Properly identify the risks** – this goes beyond listing risks, or simply identifying larger more obvious risks that may affect any commercial dealings. It involves proper consideration of the range and types of risks associated with particular clients and the services they provide, taking into account all the circumstances. This allows for effective management of the commercial relationship and careful preparation for handling of any problems that may arise.
- **Actions taken to control any risks** – once risks are identified, industry members must make a proper assessment of the issues that would arise if incidents occur. , and take proportionate steps to minimise the likelihood of such issues resulting in consumer harm. Steps taken need not involve significant resources in advance. Good

[1] See paragraph 3.3.1 of the Code, which states: "*All network operators and Level 1 providers must perform thorough due diligence on any party with whom they contract in connection with the provision of premium rate services and must retain all relevant documentation during that process for a period that is reasonable in the circumstances.*"

process planning and/or staff training may have a positive impact on a company's ability to respond effectively when incidents do occur. Even matters that are perceived to be unlikely or appear minor can pose long term difficulties if businesses are under prepared to respond to matters that do arise.

- **Responding to incidents** – even where a business makes significant effort to comply with regulations and legal requirements, they may not be immune to problems arising. Providers ought to be prepared to respond calmly and proactively to incidents, working closely with the regulator and other parties in the value chain to identify, mitigate and correct any fallout, providing support to consumers. Breaches ought to be identified and acknowledged quickly when they arise so that they can be remedied and services are therefore delivered to a high standard to consumers.

1.4 This guidance sets out further information about each of these areas to equip industry members to build and maintain strong commercial arrangements. It will help businesses meet their obligations to conduct due diligence, risk assessment and control under Part 3 of the Code, and ensure consumer confidence in premium rate services.

2. Know your client – due diligence

2.1 The start of any new venture or commercial relationship is an exciting and important period. In relation to premium rate services, these commercial arrangements often build a connection between providers of products and services with the consumers that are searching for them, establishing a quick and easy method of payment for such services. This connection is vital for revenue creation and service / industry development. The connection also establishes the opportunity for businesses to add false or unwanted charges onto a consumer's fixed line or mobile phone bills, or lead to payments being made based on misinformation or misleading promotions. So building the right connections and managing those relationships is important.

2.2 The opportunity to strengthen growth and development of services is also a chance to limit the damaging impact of non-compliant services coming into the market – by getting to know your client businesses, you can establish better long-term connections and can identify risks to consumers more easily.

2.3 The level and standard of due diligence should be consistently applied to all new clients before any binding legal contract or commercial arrangement is entered into. The Phone-paid Services Authority's Code of Practice requires that effective due diligence processes are in place. It does not prescribe the process, or the information to be gathered, so the examples set out below are to illustrate the kinds of information gathering and other actions both Network operators and providers could take, before a binding commercial agreement is formed:

- Contact details for a client's place of business;
- Copies of each client's current entry (and first entry, if different) in the Companies House register;
- Names and addresses of any relevant people with influence over the business, such as owners and directors;
- Names and addresses of all individuals who receive any share from the revenue generated by the client;

- Undertakings from the client that no other party is operating in the capacity of a shadow director under the Companies Act, if appropriate;
- The names and details of any parent or ultimate holding company which the client is a part of, if appropriate;
- Confirmation from the Phone-paid Services Authority that the provider is registered with the Phone-paid Services Authority (where registration is required);
- To make clients aware of the Phone-paid Services Authority and requiring adherence to the Phone-paid Services Authority's Code of Practice

2.4 Any process needs to be implemented with the aim of getting to know your client, and if the usual methods of gaining an insight into the business leave room for doubt or a lack of clarity, businesses ought to consider what more is necessary to build a proper awareness of the client, the service and its associated risks.

3. Properly identify the risks – risk assessment

3.1 The Code places the obligation of risk assessment and control on all parties across the value chain, Network operators, Level 1 providers and Level 2 providers. Risk assessment and control is the business process that puts in place systems to assess and manage the level of risk that a particular client and/or their service(s) may pose in terms of non-compliance with the Code and/or the law, or causing consumer harm in general. Unlike due diligence, the Phone-paid Services Authority considers that the extent of any risk assessment and control needs to be proportionate to where the contracting party sits in the value-chain.

3.2 The essence of undertaking an ongoing robust analysis of risk is to enable providers to ensure they are considering fully the regulatory risks posed by a contracting party throughout the lifetime of a contractual arrangement. Where a commercial judgment has been taken, and an assessment of 'risk' made, our expectation is that reasonable steps and/or 'controls' should be implemented to help pre-empt, where possible, the likelihood of consumer harm.

Network operators obligations

3.3 We would expect Network operators to have in place risk assessment processes in relation to Level 1 providers with whom they contract. This might include a process for keeping under review the extent to which the Level 1 provider is associated with significant breaches by a number of its Level 2 clients, and a system to detect unusual patterns of use in relation to the services being offered across their network.

3.4 Network operators should also satisfy themselves that their Level 1 clients have in place effective systems for due diligence and risk assessment and control, so as to protect their own end-users from harm.

3.5 Where the risk profile of certain services or market sectors is known to be high, for example live adult entertainment or clients specialising in certain number ranges (such as 070, or a high rated voice service numbers), we would expect Network operators and providers to be particularly vigilant and ensure that appropriate (and where necessary additional) controls are

in place. This level of vigilance would also be expected where the service type has an extensive history of breaches, whether by the potential client or not.

3.6 We would also expect there to be consideration given to the length of time a provider had been active in the UK PRS market, particularly as this relates to knowledge of their responsibilities under the Phone-paid Services Authority's Code of Practice and how to operate their services in a way that pre-empts and prevents consumer harm. We would expect providers who are new to the market to be alerted to the requirement to register with the Phone-paid Services Authority. This can be achieved within the standard terms and conditions of any contract referring to these obligations.

3.7 All providers, wherever they sit in the value-chain, bear a responsibility, where they discover instances of Code breaches and/or consumer harm, to report it to the Phone-paid Services Authority at the earliest available opportunity and take appropriate action to ensure cessation of the breaches or harm. This ought to involve providing information and support to affected consumers. As well as helping the Phone-paid Services Authority to assist in protecting consumers, this will assist in resolving issues quickly. Should the harm involved mean that an investigation is necessary, the co-operation shown by Network operators and providers in mitigating harm to consumers will be a significant factor when weighing evidence.

Considering risks posed by Level 1 providers and other intermediaries in the value chain

3.8 Where a business is building connections with a business other than a Level 2 provider, the following steps may be useful when assessing risks:

- Obtaining information about a client's history of compliance with the Phone-paid Services Authority's Code of Practice, specifically any previous rulings made by the Phone-paid Services Authority, especially in respect of previous due diligence or risk assessment and control failings, and monitoring any patterns of breaches by their clients;
- Checking whether any of the directors or other associated individuals have been involved, or connected, with other companies that have had previous rulings made against them by other regulators (e.g. Advertising Standards Authority; Gambling Commission; Financial Services Authority; Information Commissioner's Office; Ofcom, including whether a client is on Ofcom's 'Number Refusal List' or 'Under Assessment List'; etc.). Should such rulings exist, then the practices that led to them being investigated should be considered as risks that might reoccur;
- Inspecting the processes Level 1 providers have in place to assess the parties they contract with to comply with their own due diligence and risk assessment and control responsibilities;
- Taking action to ensure that the client quickly addresses any issues which are identified (including monitoring to verify that corrective action has in fact been taken). Obviously, what 'action' the Network operator and/or Level 1 then decide to enforce will be determined by, and be made proportionate to, the contractual relationship in place. Therefore, it is important that the contracting party is subject to sufficient contractual control and understands the requirements placed upon them to ensure they continue to assess their own clients operating further down the value-chain.

3.9 The exact level and detail that a Network operator or Level 1 provider might wish to obtain and consider at any particular point may change as circumstances in the market change, or, if there has been a significant structural reorganisation altering the composition of the Level 1 provider concerned (e.g. the acquisition and/or merger with another company, creation of a holding company structure, change of a director(s)). This could potentially impact upon alter the commercial relationship that may have previously been entered into. The key point to stress is that the risk assessment process is something that should be reviewed and responded to, where the circumstances make it reasonable to do so.

Considering risks posed by Level 2 providers or other parties to which Part 2 Code responsibilities have been contracted out[2]

3.10 The importance of risk assessments being undertaken spreads across the value chain, however it becomes more impactful the closer you get to the operators of the services. The Phone-paid Services Authority would expect the risk assessment and control to be of a nature that ensures that the consumer outcomes that the Phone-paid Services Authority's Code of Practice requires are able to be met. Compliance with paragraph 3.1.3(a) and (b) of the Code is highly likely to include, but not be limited to, the following expectations:

- Assess key indicators as to whether a client is a potential high risk provider. Where the client has not previously operated PRS, or is otherwise unknown, they should be assessed as high risk in the first instance.
- Check the names of the client's directors and other associated individuals against previous the Phone-paid Services Authority decisions.
- Conduct a search using the Phone-paid Services Authority's registration database, or use alternative means to ascertain information about the client which is relevant to a risk assessment.
- Consider the service types being launched and any associated risks, using information from published adjudications and other industry information sources to identify trends and issues.
- Ascertain how a client will promote their service, and where warranted by the risk posed by the client and the service, seek examples of promotional material, assess them and issue any advice or direction to the client as a result.
- Take ongoing steps to control risk following the launch of the client's service, in line with the risk assessment already performed.

3.11 Providers are advised to keep processes under review, and if necessary modify or refine, their existing risk assessment and control procedures to ensure that they meet, at the least, the expectations bulleted above. A failure to do so is likely to breach the Code in the event of an investigation.

[2] Where a Level 2 provider has sought the expertise of a third party and contracted out regulated activities, they may still be responsible under the Code for compliance with Part 2 rules. In such cases, the Level 2 provider is highly recommended to undertake due diligence to get to know their agent, and put in place risk assessment and control processes to manage that relationship effectively.

3.12 In the case of affiliate marketers and other agency agreements, Level 2 providers should consider the following in addition to ongoing DDRAC considerations already set out in Guidance elsewhere. This is not an exhaustive check list but intended as a guide. We also recommend that providers keep an audit trail of any actions taken in order to record activities for further reference and review as appropriate:

- Companies checks;
- Reputational checks through Google, blogs, AV vendors, Level 1 providers etc.;
- How established the affiliate network is;
- Whether, according to any information that has been made available to the Level 2 provider or to industry more generally, the affiliate or any associated individual has been associated with any breach of the Code or any other related Codes of Practice or law – this, in particular, should be ongoing;
- Whether the affiliate network is aware of and committed to the UK legislative and regulatory landscape, i.e. the Code and other relevant codes and legislation including the Data Protection Act, PECR, the CAP Code and relevant consumer protection laws;
- How the affiliate network sources its traffic. For example, does it source its traffic from file-sharing websites (this will likely result in increased risk);
- If the affiliate network sub-contracts with other affiliate networks in doing so (which will amplify any risk) and how it sources and vets individual affiliates;
- Whether the affiliate network is willing and able to explain where and in what terms it plans to place your advertising;
- Using traffic monitoring using tools such as Alexa or SimilarWeb to understand and monitor how an affiliate generates traffic;
- The level and sophistication of the tracking technologies the affiliate uses;
- Whether the network in question has fraud detection systems and monitoring tools in place;
- Whether the affiliate network is prepared to run its service on a trial basis.

Questions to consider as part of affiliate Due Diligence Risk Assessment and Control

Pre-Contract Due Diligence	Post-contract Monitoring, Risk Assessment and Control	Response
• Who am I contracting with and what compliance record do they have? • Is any proposed contract in my best interests? • Does my affiliate understand my requirements and the requirements of the Code of Practice? • Does my affiliate network take compliance seriously? • Do the contractual payment terms and speed of payment potentially incentivise non-compliance?	• Is my monitoring systematic and does it give me a good understanding of how my customers are being drawn to my service? • Do I have the appropriate controls in place to ensure that any unusual activity is identified quickly? • Am I analysing all aspects of this relationship, including customer complaints? • Given the risks associated with affiliate marketing, can I demonstrate that my monitoring is sufficient, thus adequately mitigating those risks?	• If I do identify an issue, do I have a clear process in place to resolve it quickly? • Is this realistic and actionable? • Is my affiliate capable of identifying, or indeed willing to identify, and deal with rogue traffic sources?

4. Actions taken to control any risks

4.1 Having ascertained information about the company and considered all potential risks, it might follow that a Network operator or provider is in a position to develop a plan of action (made bespoke to a particular client) to sit alongside the contract, or an equivalent commercial arrangement that has been entered into. This could be made available upon request by the Phone-paid Services Authority and used as mitigation in the event of a formal investigation being raised. In this way, a company can ensure risks do not go ignored and processes by which to respond to incidents can be understood ready for implementation.

4.2 The formulation of an action plan could be based on the following:

- To periodically test and/or monitor certain 'risks' that would normally be associated to a particular service category (e.g. for a subscription service, it may be prudent to test the clarity of promotions, whether reminder messages have been sent, with delivery confirmation noted, and that 'STOP' commands have been properly processed);
- The frequency of such testing should reflect the risk posed by both the client and the service type. For example, a client with no breach history, or where none of the directors are linked to other companies with breaches, and low- risk service types (such as football score updates), would require far less monitoring than a client with an extensive breach history that provides a high- risk category of service (e.g. a subscription-based lottery alerts system with a joining fee);
- 'Mystery shopper' testing could be used as, and when, appropriate;
- Internal mechanisms to enable 'whistle-blowing' by staff, where appropriate;

- Putting in place internal checks that correlate with unusual patterns of activity which may indicate consumer harm (e.g. spikes in traffic and/or consumer complaints made directly to the provider about one specific service);
- Having a procedure to alter and address instances of non-compliant behaviour;
- Monitoring of the client's service to ensure that any directions given by the Phone-paid Services Authority have been complied with;
- Producing a compliance file, comprising of a written record of the assessment, the subsequent action plan and evidence of any monitoring and/or testing required by the plan having taken place. This record does not necessarily need to be lengthy (although this will depend on the client and the actions taken under the plan), but should be made available to the Phone-paid Services Authority upon request.

4.3 Any assessment of risk should be an ongoing process and reconsidered in light of any new information. This might include updates to a client's breach history, a change in an individual client's approach to compliance or alterations to the company structure (e.g. the acquisition/amalgamation of another company, the creation of a holding company structure, appointment of new company directors, changes to the company name, etc.).

Assessment of any failure in relation to DDRAC

4.4 Where consumer harm has occurred, the assessment that will always be applied is to determine on a case-by-case basis whether the risk that harm might arise was reasonably identifiable and controllable. The Phone-paid Services Authority will seek to examine what actions were taken by the provider that contracted with the party which caused the consumer harm to ensure this risk was managed appropriately.

4.5 Where a Network operator or Level 1 or 2 provider is unable to provide evidence to the Phone-paid Services Authority that adequate due diligence was carried out, or that an adequate level of risk assessment and control took place, a Phone-paid Services Authority Tribunal is likely to classify this as a *serious* or *very serious* breach of the Phone-paid Services Authority's Code of Practice (dependent on the circumstances of the case).

4.6 Where such a breach is upheld, the Phone-paid Services Authority Tribunal may enforce a range of sanctions, including that a compliance audit to be undertaken by an independent third party to address those failings and to bring a Network operator's, or registered party's, compliance framework up to the required standard. For more information about investigations, and the role of sanctions, please refer to the 'Code 14 Supporting Procedures'.

5. Responding to incidents

5.1 Providers ought to be prepared to respond calmly and proactively to incidents, working closely with the regulator and other parties in the value chain to identify, mitigate and correct any fallout, providing support to consumers. Breaches ought to be identified and acknowledged quickly when they arise so that they can be remedied and services therefore delivered to a high standard to consumers.

5.2 In order to limit and address consumer harm, providers are encouraged to proactively alert the Phone-paid Services Authority to any issues regarding its own or third party services. Such

proactive cooperation will be considered by the Phone-paid Services Authority in relation to decisions regarding the most appropriate action to take (if any). Where enforcement action is deemed necessary such cooperation is likely to mitigate any sanctions imposed by a Tribunal, particularly where there has also been swift identification of issues arising supported by evidence of remedial action taken in keeping with established DDRAC procedures set up by the Network operator or provider. Where further dialogue is considered necessary, an effective DDRAC procedure may assist the Phone-paid Services Authority making it more likely breaches can be resolved using the Track 1 procedure, as defined at paragraph 4.3 of the Phone-paid Services Authority's Code of Practice.