Individual Reference Services Group

FINAL — DECEMBER 15, 1997

INDUSTRY PRINCIPLES — COMMENTARY

BACKGROUND:

The Individual Reference Services Group (IRSG) is composed of leading companies of the individual reference services industry. In recognition of the heightened interest in issues related to their services, the IRSG has developed self-regulatory principles. The focus of these principles is non-public information; that is, information about an individual that is of a private nature and not generally available to the public nor obtained from a public record. Signatories to these principles include individual reference services, as well as those companies that supply information to such services.

Individual reference services provide information that identifies or locates individuals, These services provide important societal benefits, For example, information obtained from these services helps locate witnesses to crimes and parents who are delinquent in their child support payments, and assists in important governmental and business functions such as fraud prevention and detection. The principles do not apply to functions other than identifying or locating individuals or verifying individual identities, For instance, database services of newspaper archives, or of prior business records relating to an individual, and database services used primarily for risk assessment, lie outside the scope of the principles.

Increased market demand, a highly mobile society, as well as rapid advances in technology, have spurred increased reliance upon and availability of information obtained through services provided by companies in the individual reference services industry,

This increased reliance upon and availability of information has heightened consumer interest regarding privacy and identity fraud concerns, as well as services provided by companies within the individual reference services industry. It is notable that there is no evidence these services are used for unlawful purposes. Nor has any organization or study, including the Federal Reserve Board in its specially commissioned 1997 report to Congress, been able to point to a single case of identity fraud that resulted from the misuse of an individual reference service.

Members of the individual reference services industry recognize the importance of minimizing risks associated with their services, and are strongly committed to taking a leadership role on these issues. The IRSG also realizes that self-regulation of this industry is the most effective and efficient way to minimize these risks. It is with this background that the IRSG has adopted these principles.

SUMMARY OF PRINCIPLES:

IRSG members commit to educating their users and the public about the services they offer and the privacy issues that are associated with these services. An educational initiative will allow users and the public to understand the capabilities of these services, and enable users to utilize the information obtained from these services responsibly.

The principles mandate that companies in the individual reference services industry acquire individually identifiable information only from sources known as reputable in the government and private sectors. They also adopt the Direct Marketing Association's long-standing prohibition on the use for non-marketing purposes of personally identifiable information obtained from marketing transactions. This refers primarily to customer lists and other material that reflects transactions undertaken by an individual. Here, with a few exceptions, the principles prohibit services from knowingly purchasing or selling individually identifiable information that is collected for marketing purposes and from knowingly retaining such marketing information for inclusion in their individual reference services. This would include information obtained from customer lists, warranty card responses, and the like, While marketing data generally may not be used as an individual reference resource, individual reference services may be used for direct marketing purposes, such as verifying the addresses of individuals for delivery purposes,

The core of the IRSG's self-regulatory effort is the self-imposed restriction on use and dissemination of non-public information about individuals in their personal (not business) capacity In addition, IRSG members who supply non-public information to other individual reference services will provide such information only to companies that adopt or comply with the principles. The principles define the measures that IRSG members will take to protect against the misuse of this type of information, The restrictions on the use of non-public information are based on three possible types of distribution that the services provide.

For *selective and limited distribution* of non-public information, the companies commit to state what uses of their information are appropriate and to provide such products only to qualified subscribers. Such subscribers are required to state their appropriate purpose for using such information and agree to limit the use and redissemination of such information to those stated purposes. The subscribers' qualifications and intended uses will be reviewed before the non-public information is made available, with the extent and nature of the review determined by the nature of the non-public information being requested,

For *commercial and professional distribution* of non-public information, the companies commit to limiting distribution to established professional and commercial users who will use the information only for appropriate purposes within the normal course and scope of their business or profession. Certain categories of non-public information, such as financial or medical records, will be excluded from this type of distribution. Records that reveal an individual's mother's maiden name identified as such also will not be distributed. Social security numbers and date of birth information will be distributed only if truncated in an appropriate manner. For example, recognizing the importance of preventing the reconstruction of original information otherwise

protected by these principles, the industry has adopted the consistent practice of masking the last four or more digits of social security numbers. These exclusions are intended solely for non-public information, and will not apply to public or publicly available information that may contain social security numbers or similar data.

In order to protect against abuse in both *selective and limited distribution* and *commercial and professional distribution,* individual reference services will maintain certain records, including the identity of subscribers and the terms and conditions agreed to by them, for three years after termination of each subscriber's relationship with the individual reference service, In addition, the companies will take steps to remedy abuses, if any, that they may learn about.

For *general distribution* of non-public information, the companies will not knowingly provide non-public information products that contain an individual's social security number, mother's maiden name identified as such, non-published telephone directory information obtained from a phone company (as defined by Newton's Telecommunications Dictionary), date of birth information, credit history, financial history, medical records, or similar information. The services also will not provide products in which information is retrievable by input of a social security number. The individual reference service will take reasonable steps to protect against the misuse of non-public information provided in this type of distribution.

In addition to limiting access to non-public information, the principles require individual reference services to provide security to avoid unauthorized access to their materials, The security provided will include both technical and managerial controls to protect information. Periodic reviews of security also will be made to ensure the proper protection of information.

In the spirit of openness, the principles require individual reference services to have an information practices policy statement available to the public upon request. These statements will describe the types of information included, the types of sources from which that information is obtained, the nature of how the information is collected, the type of entities to whom the information may be disclosed, and the type of uses to which the information may be put. This openness will enable individuals to understand the reference service's use of the information it possesses.

Individual reference services will also inform individuals, upon request, of the choices, if any, available to limit access or use of information about them contained in the products and services that the companies create, maintain, or provide access to. The ability of an individual to limit access to his or her information should not serve as an impediment to law enforcement use of the databases. However, individual reference services will provide individuals with an opportunity to limit the public's access or use of non-public information about them that is distributed to the general public under principle V.C.

The principles also require an individual reference service to provide information about the nature of public record and publicly available information that it makes available in its products and services and the sources of such information. Subject to limited legal and security exceptions,

the companies will make available to individuals, upon request and under reasonable conditions, non-public information contained in products or services that specifically identifies them and that is distributed as part of an individual reference service to users.

The FTC disagrees with the IRSG's approach to responding to requests by individuals for public record information about themselves contained in a company's databases, Where the requested information is publicly available or a matter of public record, the principles allow the individual reference service to provide guidance on how the requester can obtain the information directly from the source. The FTC proposes that companies furnish individuals with all public record and publicly available information about themselves contained in the companies' databases in order to address two accuracy-related issues: first, the possibility that errors might arise in the transmission of information from the source to the company's database; and second, the possibility that information about different individuals might be mistakenly linked in compilations about a single individual.

The signatories of these principles understand the public's interest in enabling individuals to verify that errors do not occur when public record and publicly available information is transmitted or compiled about them. However, technological advancements have eliminated the need for most companies to keystroke or otherwise manually input this type of information, thereby significantly reducing the possibility for error. This, the signatories believe, when coupled with quality assurance measures implemented by the industry, yields information that reliably reflects the data provided by the originating public record source,

Moreover, there is an enormous potential burden associated with retrieving and verifying relevant information from the large number of databases of public records. This contrasts with the modest burden associated with retrieving information about an individual from the far smaller number of databases of non-public information. It should also be noted that many of the potential harms that might befall an individual whose public record information is inaccurate are already addressed by existing laws, including the Fair Credit Reporting Act.

Nevertheless, the signatories have pledged to reexamine, in 18 months, the issue of responding to requests by individuals for public record information about themselves.

In addition, the experience of applying these principles and conducting the assurance reviews will shed further light on the accuracy issue to the extent to which any inaccuracies might be derived from transmission or compilation errors that may occur under the control of an individual reference service. Based upon this experience, the signatories over the next 18 months will collectively or individually carefully consider undertaking a study to assess the accuracy of information about individuals in their databases as a reflection of the information about such individuals provided by the originating public record source.

In connection with children, the individual reference services industry recognizes the heightened sensitivity necessary in dealing with the individually identifiable information about

children. For this reason, the principles strictly limit the availability of non-public information concerning anyone identified as being under the age of eighteen.

The signatories of these principles commit to having annual assurance reviews conducted of those services they offer that they identify as being subject to the principles. These reviews will - be conducted by qualified independent professional services such as accounting firms, law firms, or security consultants. These independent professional services will use criteria developed by assurance professionals and approved by the signers as a group, As experience and changing circumstances require changes in the principles or in the criteria used for assurance reviews, the approval of the signers as a group will be needed to adopt such changes,

Companies will have a reasonable opportunity, determined by the nature of the concern and circumstances that surround it, to respond to any concerns that are expressed in such assurance reviews. Because individual reference services that obtain non-public information from IRSG members will be required by contract to abide by the principles, they, too, will need to have assurance reviews conducted annually.

While a summary of each assurance report shall be made publicly available, the signatories of these principles are exploring additional means of enabling the public to identify individual reference services that are in compliance with these principles.

The IRSG members believe that these principles provide the most effective way to secure the benefits of these important information service resources while assuring effective protection of consumer privacy, IRSG members pledge to implement these principles fully by no later than December 31, 1998.