



January 16, 2007

The Honorable Alberto R. Gonzales
Attorney General of the United States

The Honorable Deborah Platt Majoras
Chair, Federal Trade Commission

Subject: Identity Theft Task Force Request for Comments

On behalf of the Workforce Privacy Network, we appreciate the opportunity to submit comments to the Federal Identity Theft Task Force (the "Task Force").

The Workforce Privacy Network¹ is a part of the International Association for Human Resource Information Management (IHRIM). With some 2,400 members in 22 chapters representing employers in all 50 states, IHRIM² is the leading professional association for practitioners, vendors and consultants who work with HR systems and data. Given time constraints our comments reflect the views of the Workforce Privacy Network rather than those of IHRIM as a whole. Nonetheless, we believe they represent the employer perspective on identity theft, and identify both critical causes of identity theft that have not received sufficient federal attention and critical areas of preventive action not yet contemplated by the Task Force.

The Task Force has an historic opportunity to address an issue that has a major impact on commerce and the lives of American consumers. Although Americans fear and feel the effects of identity theft primarily as consumers, the exposure and misappropriation of their information linked to identity theft frequently occurs not in the context of their consumer relationships, but within the context of employment. Some studies have found, for example, that between 50% and 70% of cases of identity theft can be traced back to employees who mishandled or misused records.³

In recent years, the information security field has turned a great deal of its attention away from "securing the perimeter" toward addressing "internal threats." These threats include employees and contractors who fail to heed organizational policies,

¹ See www.hr-privacy-security.org.

² See www.ihrim.org.

³ See, e.g., *2004 Data Security Tracking Study*, Ponemon Institute (2004); J.M. Collins and S.K. Hoffman, "Identity Theft: Predator Profiles, Based on 1,037 Actual Cases," Manuscript (2003), Michigan State University; Collins, Judith, *Preventing Identify Theft In Your Business; How To Protect Your Business, Customers and Employees*, Wiley (Hoboken, NJ, 2005).

are careless, fall prey to social engineering, fail to adequately protect personal information in their possession, etc., along with a small number who engage in outright criminal activities.

The importance of focusing attention on the employment context is evident in another significant way as well. Employees are frequently exposed to identify theft, not as consumers, but as employees. Over the last few years tens of millions of employees have received notices from their employers that their personal information has been lost, stolen or inappropriately accessed. In other words, not only are employees directly or indirectly implicated in causing identity theft; employees are also all too commonly those personally jeopardized by data breaches.

However, the documents that we have reviewed from the Task Force to date focus primarily on maintaining the security and preventing the misuse of “consumer” data, only mentioning employee data tangentially or in the limited context of what government agencies can do to prevent identify theft arising out of human resources practices.

We understand, of course, that the Federal Trade Commission often protects employees and their data through laws explicitly regulating consumers in contexts such as the Fair Credit Reporting Act and under its general consumer protection authority under Section 5 of the Federal Trade Commission Act. We suggest however, that the area of employee data warrants some special focus in analyzing the causes of identity theft, and therefore its remedies. We note moreover, that the standard forms for reporting identity theft used by the Federal Trade Commission request no information on the employment of the complainant, raising questions about whether employment-related causes of identity theft can be properly identified and investigated by the Commission and others. Even so, employment relationships were identified by the complainants themselves as the third most prevalent basis for identity theft according to the most recently published FTC identity theft complaint data.⁴

Privacy and information security regulation and standards have often treated employment relationships as an afterthought, rendering the benefits of such standards in the employment context suboptimal and their interpretation more difficult. Given the importance of protecting personal information in the employment context to preventing identity theft, that context deserves special attention by the Task Force.

One of the ways of achieving this would be through the creation of an advisory committee on the protection of personal information in employment (on which we would be pleased to serve). We also note the absence on the Task Force of the Secretary of Labor, and respectfully suggest that her inclusion would reflect recognition of the importance of education and standards for employers in the area of identity theft.

⁴ *Consumer Fraud and Identity Theft Complaint Data*, Federal Trade Commission, January-December 2005 (Federal Trade Commission, January 2006).

Finally, we recommend that employers, employment-related professional organizations and other parties interested in workplace privacy should be encouraged to provide input as to the nature of any new guidelines, standards, laws or regulations. The goals of the Task Force will not be well-served if information in the employment context were subject to standards developed solely with consumers in mind. Like organizations engaged in consumer relationships, however, multi-state employers and their employees would benefit from clear national standards rationally related to addressing the particular identity theft risks they face. Therefore we are confident that addressing our recommendations will benefit the work of the Task Force in crafting creative, practical and politically feasible ways of addressing identity theft.

Respectfully Submitted,

Anne Clifford, Chair
On behalf of the Board of Directors,
Workforce Privacy Network
IHRIM
P.O. Box 1086
Burlington, MA 01803
anne.clifford@fmr.com
www.hr-privacy-security.org