[1]"Data Collection Agent" is defined in the proposed order as any software program, including any application; created, licensed or distributed, directly or through a Third Party, by respondent; installed on consumers' computers, whether as a standalone product or as a feature of another product; and used to record, or transmit information about any activity occurring on that computer, unless: (a) the activity involves transmission of information related to the configuration of the software program or application itself; (b) the transmission is limited to information abo

0.0000 TD(lim)Tj19.e0.00 0.00 0.00 rgBT72TD(n a)Tj14.2800 0.0000Br1D(n a)Tj14.280000

Part II.A. of the proposed order requires Compete to provide corrective notice to consumers who had previously installed a Data Collection Agent. Compete must inform consumers about the categories of personal information collected and transmitted by the software, and how to uninstall it. Part II.B. requires the company to provide for two years phone and e-mail support to assist consumers who seek to disable or uninstall a Data Collection Agent.

Part III of the proposed order requires Compete to provide a copy of the order to third parties with whom it has now, or will have in the future, any agreement in connection with any Data Collection Agent made available by the third party.

Part IV of the proposed order prohibits the company from making any misrepresentations about the extent to which it maintains and protects the security, privacy, confidentiality, or integrity of any information collected from or about consumers.

Part V of the proposed order requires Compete to maintain a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of information (whether in paper or electronic format) about consumers. The security program must contain administrative, technical, and physical safeguards appropriate to Compete's size and complexity, the nature and scope of its activities, and the sensitivity of the information. Specifically, the proposed order requires Compete to:

• designate an employee or employees to coordinate and be accountable for the information security program;

• identify material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks;

• design and implement reasonable safeguards to control the risks identified through risk assessment, and regularly test or monitor the effectiveness of the safeguards' key controls, systems, and procedures;

• develop and use reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from Compete or obtain on behalf of Compete, and require service providers by contract to implement and maintain appropriate safeguards; and

• evaluate and adjust its information security programs in light of the results of testing and monitoring, any material changes to operations or business arrangements, or any other circumstances that it knows or has reason to know may have a material impact on its information security program.

Part VI of the proposed order requires Compete to obtain within 180 days after service of the order, and biennially thereafter for 20 years, an assessment and report from a qualified,