

Complaint

IN THE MATTER OF

DIRECTORS DESK LLCCONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF
SEC. 5(A) OF THE FEDERAL TRADE COMMISSION ACT

Docket No. C-4281; File No. 092 3140
Filed, January 12, 2010 — Decision, January 12, 2010

This consent order addresses Directors Desk LLC's alleged false or misleading representations made to consumers concerning its participation in the Safe Harbor privacy framework agreed upon by the U.S. and the European Union. The Commission's complaint alleges that Directors Desk falsely represented that it was a current participant in the Safe Harbor when, in fact, from February 2008 until August 2009, Directors Desk was not a current participant in the Safe Harbor. The Commission's complaint alleges that in February 2007, Directors Desk submitted to Commerce a self-certification, which it did not renew in February 2008. Commerce then updated its status to "not current" on the Commerce public website. Directors Desk remained in "not current" status until it submitted a self-certification to Commerce in August 2009. The order prohibits Directors Desk from making representations about its membership in any privacy, security, or any other compliance program sponsored by the government or any other third party. It contains provisions designed to prevent Directors Desk from engaging in the future in practices similar to those alleged in the complaint, as well as reporting and compliance provisions.

Participants

For the *Commission*: *Molly Crawford and Katie Ratté.*

For the *Respondents*: *Chris Wolf, Esq., Hogan & Hartson .*

COMPLAINT

The Federal Trade Commission, having reason to believe that Directors Desk LLC ("respondent") has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

Complaint

1. Respondent Directors Desk LLC (“Directors Desk”) is a Delaware limited liability company with its principal office or place of business at 1 Liberty Plaza, New York, New York 10006.

2. Respondent is in the business of providing a secure online application that allows members of corporate boards of directors to access board meeting materials, board minutes, and other related documents through a website (www.directorsdesk.com).

3. The acts and practices of respondent as alleged in this complaint have been in or affecting commerce, as “commerce” is defined in Section 4 of the Federal Trade Commission Act.

4. Respondent has set forth on its website, www.directorsdesk.com, privacy policies and statements about its practices, including statements related to its participation in the Safe Harbor privacy framework agreed upon by the U.S. and the European Union (“U.S.-EU Safe Harbor Framework” or “Safe Harbor”).

U.S.-EU SAFE HARBOR FRAMEWORK

5. The U.S.-EU Safe Harbor Framework provides a method for U.S. companies to transfer personal data outside of Europe that is consistent with the requirements of the European Union Directive on Data Protection (“Directive”). Enacted in 1995, the Directive sets forth European Union (“EU”) requirements for privacy and the protection of personal data. Among other things, it requires EU Member States to implement legislation that prohibits the transfer of personal data outside the EU, with exceptions, unless the European Commission (“EC”) has made a determination that the recipient jurisdiction’s laws ensure the protection of such personal data. See Directive 95/46/EC of the European Parliament and of the Council (Oct. 24, 1995), available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>. This determination is commonly referred to as meeting the EU’s

Complaint

“adequacy” standard.

6. To satisfy the EU adequacy standard for certain commercial transfers, the U.S. Department of Commerce (“Commerce”) and the EC negotiated the U.S.-EU Safe Harbor Framework, which went into effect in 2000. The Safe Harbor allows U.S. companies to transfer personal data lawfully from the EU. To join the Safe Harbor, a company must self-certify to Commerce that it complies with seven principles and related requirements that have been deemed to meet the EU’s adequacy standard.

7. Companies under the jurisdiction of the U.S. Federal Trade Commission (“FTC”), as well as the U.S. Department of Transportation, are eligible to join the Safe Harbor. A company under the FTC’s jurisdiction that self-certifies to the Safe Harbor principles but fails to implement them may be subject to an enforcement action based on the FTC’s deception authority under Section 5 of the Federal Trade Commission Act.

8. Commerce maintains a public website, www.export.gov/safeharbor, where it posts the names of companies that have self-certified to the Safe Harbor. The listing of companies indicates whether their self-certification is “current” or “not current.” Companies are required to re-certify every year in order to retain their status as “current” members of the Safe Harbor framework. According to the Safe Harbor website, “Organizations should notify the Department of Commerce if their representation to the Department is no longer valid. Failure to do so could constitute a misrepresentation.” See Safe Harbor List, available at <http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list>.

VIOLATIONS OF SECTION 5 OF THE FTC ACT

9. In February 2007, respondent submitted to Commerce a self-certification to the Safe Harbor. That self-certification stated

Complaint

that its privacy policy has been effective since June 2004. (Exhibit A, Safe Harbor Certification).

10. In February 2008, respondent did not renew its self-certification to the Safe Harbor, and Commerce updated respondent's status to "not current" on its public website. Until August 2009, respondent did not renew its self-certification to the Safe Harbor and was in "not current" status on Commerce's website. (Exhibit B, Declaration of Damon C. Greer).

11. Respondent has disseminated or caused to be disseminated privacy policies and statements on the www.directorsdesk.com website, including, but not limited to, the following statements:

Directors Desk is a participant in the Safe Harbor program developed by the U.S. Department of Commerce and the European Union. We have certified that we adhere to the Safe Harbor Privacy Principles agreed upon by the U.S. and the E.U. For more information about the Safe Harbor and to view our certification, visit the U.S. Department of Commerce's Safe Harbor web site.

Exhibit C, December 2008 Privacy Policy.

12. Through the means described in Paragraph 11, respondent represented, expressly or by implication, that it is a current participant in the Safe Harbor.

13. In truth and in fact, from February 2008 to August 2009, respondent was not a current participant in the Safe Harbor. Therefore, the representations set forth in Paragraph 11 were, and are, false or misleading.

14. The acts and practices of respondents as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal

Complaint

Trade Commission Act.

THEREFORE, the Federal Trade Commission this twelfth day of January, 2010, has issued this complaint against respondent.

By the Commission.

Complaint

EXHIBIT A

Page 1 of 2

Organization Information:

Directors Desk, LLC
2510 N. Pines Road, Suite 207
Spokane, Washington 99206
Phone: 509-931-1099
Fax: 509-267-5465
<http://www.directorsdesk.com>

Contact Information:

Contact Office: Directors Desk Spokane
Contact Name: Bret Beresford-Wood, President
Phone: 866-895-3375 x511 Fax: 509-267-5465 Email: bwood@directorsdesk.com

Corporate Officer Information:

Corporate Officer: Bret Beresford-Wood, President
Phone: 866-895-3375 x511 Fax: 509-267-5465 Email: bwood@directorsdesk.com

Safe Harbor Information:

Signed up to safe harbor 02/15/2007 04:36:53 PM

Next certification 02/15/2008

EU/EEA Countries From Which Personal Information Is Received: France, Belgium, Germany, United Kingdom, Italy

Industry Sector: Computer Services - (CSV) Computer Software - (CSF) Information Services - (INF)

Personal Information Received From the EU: Directors Desk hosts and maintains a secure online application for corporate boards of directors. Certain directors residing in the European Union sit on corporate boards using our services. Such directors are able to access the full set of Directors Desk features to access information including board meeting materials, meeting minutes, documents, and other related materials. They can also communicate with officers and other directors of the corporation using tools within the online application, such as secure email.

Information collected from EU board members ("users") includes personal contact information that is stored in our system and made accessible to officers and fellow directors of the company client in question. This information may include: full name; work information including company name, address, phone and fax; home information including home address, phone, fax, mobile phone; biographical information including other boards on which the individual sits and related professional history; and personal contact information such as email address, wireless text messaging address, and fax number(s). All such personal information is stored online for the purposes of conducting board work for the company in question. As stated in our privacy policy, Directors Desk does not communicate directly with any of its clients' end-users, be these residents of the EU or otherwise, and we take strong measures to safeguard each user's personal information at all times.

Privacy Policy Effective: 6/10/2004

Location: <http://www.directorsdesk.com/privacy.asp>

Regulated by: Federal Trade Commission

Privacy Programs:

Verification: In-House

Dispute Resolution: In the event that any dispute arising out of or related to this policy is not settled by the parties, the parties will attempt in good faith to resolve such dispute by non-binding mediation in accordance with the American Arbitration Association Commercial Mediation Rules.

Personal Data Covered: Online and offline

Human Resource Data Covered: No

Complaint

EXHIBIT A (continued)

Page 2 of 2

 Do you agree to cooperate and comply with the European Data Protection Authorities? Select
Appropriate Response

Certification Status: Not Current

Compliance Status:

[Safe Harbor Overview](#) | [Safe Harbor Documents](#) | [Workbook](#) | [Safe Harbor List](#)
[Information Required for Certification](#) | [Certification Form](#)

FEDERAL TRADE COMMISSION DECISIONS
VOLUME 149

Complaint

EXHIBIT B

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of

DIRECTORS DESK, LLC,
a limited liability company.

)
)
)
)
)
)
)

DOCKET NO.

DECLARATION OF DAMON C. GREER

I, Damon C. Greer, based upon my personal knowledge concerning matters to which I am competent to testify, hereby declare as follows:

1. I am the Associate Director for Electronic Commerce in the Office of Technology and Electronic Commerce at the U.S. Department of Commerce ("Commerce"), and I am the lead administrator of the U.S.-E.U. Safe Harbor Framework.
2. Commerce is not a party to the captioned matter.
3. Commerce is responsible for developing and overseeing the U.S.-EU Safe Harbor Framework ("Safe Harbor"), a voluntary program that provides U.S. companies with a method for receiving personal data lawfully from the European Union. To join the Safe Harbor, a company must self-certify to Commerce that it complies with a set of principles that have been deemed to meet the EU's adequacy standard.
4. As Associate Director, I am responsible for maintaining an accurate list of those companies that self-certify to Commerce that they comply with the Safe Harbor principles. As part of my responsibilities, I oversee a public website, www.export.gov/safeharbor, where I post the names of companies that have self-certified. The listing of companies indicates, among other things, whether their self-certification is "current" or "not current." Companies are required to re-certify every year on the anniversary of the date they first self-certified in order to retain their status as "current" members of the Safe Harbor framework.
5. In February 2007, Directors Desk LLC ("Directors Desk") submitted a self-certification to Commerce. Directors Desk's next self-certification was due in February 2008.
6. Directors Desk did not submit a self-certification by the February 2008 deadline, and as a result I updated Directors Desk's status to "not current" on Commerce's public website.

Complaint

EXHIBIT B (continued)

To date, I have not received any documents or information from Directors Desk to renew its self-certification. Directors Desk is still in "not current" status on the Commerce website.

I declare under penalty of perjury under the Laws of the United States of America that the foregoing is true and correct. Executed this 7th day of June, 2009, in Washington, D.C.

A handwritten signature in black ink, appearing to read "Damon C. Greer", is written over a horizontal line.

Damon C. Greer
Associate Director for Electronic Commerce
Office of Technology and Electronic Commerce
U.S. Department of Commerce

Complaint

EXHIBIT C

DIRECTORS DESK PRIVACY POLICY

<http://www.directorsdesk.com/company/privacy.asp>

Directors Desk
A HARBARO OMA COMPANY

Our Solution • Advantage • Security • Company

CONTACT US

Privacy Policy
Effective Date: 6/10/2004 - Latest Revision: 2/15/2007 12:02:40 PM

Directors Desk, LLC ("Directors Desk") is dedicated to establishing a trusting relationship with its clients and client end-users ("users"), based on respect for personal identity and information, by promoting the use of fair information practices. This privacy statement covers all Web properties ("online applications") owned and maintained by Directors Desk, including but not limited to <http://www.directorsdesk.com> and <https://secure.directorsdesk.com>.

Because Directors Desk wants to demonstrate its commitment to our users' privacy, we are disclosing:

1. What personally identifiable information Directors Desk collects
2. How Directors Desk uses the information
3. With whom Directors Desk may share user information
4. What choices are available to users regarding collection, use and distribution of the information
5. What types of security procedures are in place to protect the loss, misuse or alteration of information under Directors Desk control
6. How users can correct any inaccuracies in the information

Information Collection and Use

Information Collection
Directors Desk is the sole owner of aggregated system information its web properties, and the clients of Directors Desk are the sole owners of personal user information belonging to their board and committee members entered into their specific Directors Desk account(s). The Directors Desk online applications collect information from users at several different points:

Account Management Screens
In order to use Directors Desk services at any level, a user must first be set up in the Directors Desk online application. This is done by Directors Desk account representatives, administrative users ("Corporate Secretaries") of the client company, or the users themselves. During account setup the following user information fields are required:

- First and last name
- Personal User Name (can be set by the user)

It is highly recommended, but not required, that user accounts also contain a valid email address, in order for the application to be able to send information updates ("Announcements") to the user, in order to keep them abreast of new information related to their board management responsibilities.

User Roster Screens
It is common and recommended practice for a certain level of personal contact information to be placed into the user account, in order to make such information the client company's Roster. The Roster screens are used by board members and other client users to contact fellow board and committee members. To protect users' privacy rights, all fields that are stored in the application for the user are viewable in the user's view of the Roster, and the user is able to add/delete/remove information in each field. Further protecting the user, the application provides each user with a set of personalized "privacy settings" allowing him or her to make choices about how such information is used within their client company Roster. For instance, the user can choose to keep their home or cell phone information private from all users except the Corporate Secretary users.

Use of Information by Directors Desk
Except where Directors Desk account representatives are specifically asked to provide data entry services on the client's behalf, Directors Desk acts as a passive conduit for the entry and distribution of all users' email communications and personal information, and therefore will not monitor, edit, or disclose the contents of a user's information unless Directors Desk in good faith believes that such action is necessary to conform to the edicts of the law or comply with legal process served on Directors Desk. Subject to the legal exceptions listed in the Privacy Policy, Directors Desk will never disclose to any third parties any of the personal information uploaded to our online applications by our users.

Profiling Activities
We store information that we collect through cookies, log files and third-party audit trails to create a profile of our users. A profile is stored information that we keep on individual users that details their viewing preferences. Consequently, collected information is tied to the user's personally identifiable information to improve the content of the site for the user. This profile is used only for the purpose of tailoring a user's visit to our online applications, and never to direct marketing promotions or other communications not

Complaint

EXHIBIT C (continued)

DIRECTORS DESK LLC PRIVACY POLICY

<http://www.directorsdesk.com/company/privacy.asp>

directly related to their use of the system. We do not share personally identifiable elements of your profile with other third parties. If shared at all, your profile is shared in aggregate form only, rendering personally identifiable information impossible.

Cookies

A cookie is a piece of data stored on the user's computer tied to information about the user. Usage of a cookie is in no way linked to any personally identifiable information while on our site. We use both session ID cookies and persistent cookies. For the session ID cookie, once users close the browser, the cookie simply terminates. A persistent cookie is a small text file stored on the user's hard drive for an extended period of time. Persistent cookies can be removed by following Internet browser help file directions.

By setting a cookie on our site, users would not have to enter their User Name more than once, thereby saving time while on our site. If users reject the cookie, they may still use our site. The only drawback to this is that the user will be required to re-enter the User Name upon each new site visit. Persistent cookies enable us to track and target the interests of our users to enhance the experience on our site. See the "Profile" section, above.

Due to the secure nature of the application, we allow no business partners to use cookies on our site.

Log Files

Like most online applications, our servers use log files to analyze trends, administer the site, track user's movement in the aggregate, and gather broad demographic information for aggregate use. IP addresses, etc. are not linked to personally identifiable information.

Communications from the Site**Informational Updates**

We do not send users communications, but rather provide our clients with tools allowing them to send communications to other users related to the board work and related processes empowered by Directors Desk. Certain new users will receive a welcoming email issued by their Corporate Secretaries to activate their new account. Established users will occasionally receive emails, cell phone text messages, and faxes (collectively, "Announcements") containing information about new board information that is available for their viewing, new messages they have received from client staff or other board members, or action items such as votes and surveys that need to be completed by the user. All such Announcements are issued exclusively by the designated and Client Company authorized Corporate Secretaries, unless the user has elected to receive proactive notifications of certain new information as it becomes available within their accounts. In which case automated emails are sent out by the system. In all cases, however, the user can modify any email, wireless, and fax addresses at which they receive communications simply by logging into their accounts, or choose to opt out of receiving Announcements entirely. Users thus retain full control over the extent to which they receive information updates at all times.

Service Announcements

On rare occasions it is necessary to send out a strictly service related announcement. For instance, if our service is temporarily suspended for maintenance we might send users an email. Users may opt-out of these communications. However, these communications are never promotional in nature.

Customer Service

We communicate with users on a regular basis to render technical assistance as part of our 24-Hour Help Desk activities. We reply via email or phone, in accordance with the user's wishes, and all such activities are initiated by the user.

Spam and Junk Email

Directors Desk has a zero tolerance policy for abuse. While we cannot be responsible for communications users receive from other users such as fellow board members and Corporate Secretaries on their client company accounts, it is our intention to use all legally available means to prevent distribution and receipt of unsolicited commercial communications through the service. We ask that any users who are annoyed by receipt of such junk email, please report such activity to abuse@directorsdesk.com.

Sharing**Legal Disclosure**

Though we make every effort to preserve user privacy, we may need to disclose personal information when required by law wherein we have a good-faith belief that such action is necessary to comply with a current judicial proceeding, a court order, legal process served on our online application, or in order to investigate, prevent, or take action regarding illegal activity.

Aggregated Information (non-personally identifiable)

We will always attempt to use aggregated demographic information in any case where user information must be shared, such that no personally identifiable information is disclosed to outside parties. In the event that personally identifiable information must be used, we will first notify clients in accordance with the Subpoena Policy outlined below. Any actions taken there under by our client to protect its users' personal information will be respected subject to limitations imposed by the law.

Business Transitions

In the event Directors Desk goes through a business transition, such as a merger, being acquired by another company, or selling a portion of its assets, users' personal information will, in most instances, be part of the assets transferred. Users will be notified prior to a change of ownership or control of their personal information. If as a result of the business transition, the users' personally identifiable information will be used in a manner different from that stated at the time of collection they will be given a choice not to have their information used in this different manner, as described in the notification of changes section, below.

Links

Directors Desk's online applications may contain links to other sites. As with all site content, these links are not placed in the system by Directors Desk but rather by the Corporate Secretaries of the client company, or other users authorized to post content.

Please be aware that Directors Desk is not responsible for the privacy practices of such other sites. We encourage our users to be aware when they leave our sites and to read the privacy statements of each and every Web site that collects personally identifiable information. This privacy statement applies solely to information collected by Directors Desk's online applications. Information that is collected on these sites does not fall within the auspices of this policy.

DIRECTORS DESK LLC

Complaint

EXHIBIT C (continued)

www.directorsdesk.com

<http://www.directorsdesk.com/company/privacy.asp>**Security**

Directors Desk takes every precaution to protect its users' information. Security falls into several categories and user information is protected both online and off-line.

Secure Products & Tools

On all screens of the Directors Desk application, information is encrypted and is protected during transit from the client's PC to our servers with the best encryption software in the industry - SSL. While browsing the application, the lock icon on the bottom of Web browsers such as Microsoft Internet Explorer becomes locked, as opposed to un-locked, or open, when users are just 'surfing', in order to easily identify to the user that their data is being transmitted securely. To fully protect our users, it is not possible to access the application without using an SSL connection.

Data Encryption

Documents uploaded to the system, as well as database entries containing personal information, are stored in accordance with each client company's data encryption policy. At a minimum, this includes storing all sensitive personal information (such as user passwords, social security numbers, date of birth, etc.) in a fully encrypted format. In many cases, the encryption technologies used will preclude Directors Desk from being able to decrypt the data.

Unauthorized Access

Directors Desk has taken extreme measures to protect user information against unauthorized access. These measures include but are not limited to: a) storing all data in hosting facilities that are SAS-70 Level II Certified; b) storing user information in secure offline repositories not accessible to routine "hacking" attempts; c) engineering sophisticated application security technologies specifically designed to detect and protect against unauthorized data access; d) treating all user information stored in web applications as highly confidential during storage, transmission, and backup.

Protection Against Loss

Directors Desk provides, as part of its service, full data mirroring and nightly tape backups to protect user information from being inadvertently lost or destroyed.

Protection Against Data Corruption and Alteration

Directors Desk uses state-of-the-art technologies, techniques and processes to maintain data integrity at all times. This includes use of an enterprise-level relational database system (RDBMS) that has been tested extensively both in-house and by industry at-large.

Offline Security

In addition to protecting user information stored in electronic systems, we also employ security measures to protect user information offline. All of our users' information, not just the sensitive information mentioned above, is restricted in our offices. Only employees who need the information to perform a specific job (for example, our customer service representatives) are granted access to personally identifiable information.

Choice and Opt-Out Options

User information is never used for purposes that are not directly related to their board and committee activities. All use of personal information is subject to a full set of 'opt-out' options made available to the user. For instance, if the user does not wish to disclose his or her email address, they are able to remove that data from the system. If the user does not wish for other directors to see his or her home or work contact information, again they can remove those fields from the system. If a user's personally identifiable information changes (such as zip code, phone, email or postal address), or if a user no longer desires our service, we provide a way to correct, update or delete/inactivate users' personally identifiable information. This can be done at the Roster profile page of the Directors Desk service patronized by the user.

Notification of Changes

If we decide to change our privacy policy, we will post those changes in this privacy statement, and other places we deem appropriate, so our users are always aware of what information we collect, how we use it, and under what circumstances, if any, we disclose it. We will use information in accordance with the privacy policy under which the information was collected.

If, however, we are going to use users' personally identifiable information in a manner different from that stated at the time of collection we will notify users via email. Users will have a choice as to whether or not we use their information in this different manner. In addition, if we make any material changes in our privacy practices that do not affect user information already stored in our database, we will post a prominent notice on our Web site notifying users of the change. In some cases where we post a notice we will also email users, who have opted to receive communications from us, notifying them of the changes in our privacy practices.

Safe Harbor

Directors Desk is a participant in the Safe Harbor program developed by the U.S. Department of Commerce and the European Union. We have certified that we adhere to the Safe Harbor Privacy Principles agreed upon by the U.S. and the E.U. For more information about the Safe Harbor and to view our certification, visit the U.S. Department of Commerce's Safe Harbor web site. In the event that any dispute arising out of or related to this policy is not settled by the parties, the parties will attempt in good faith to resolve such dispute by non-binding mediation in accordance with the American Arbitration Association Commercial Mediation Rules. No litigation for the resolution of such dispute may be commenced until the parties try in good faith to settle the dispute by such mediation in accordance with such rules and either party has concluded in good faith that amicable resolution through continued mediation of the matter does not appear likely. The parties to this mediation shall share the costs of mediation equally. Any settlement reached by mediation shall be recorded in writing, signed by the parties, and shall be binding on them.

Civil Subpoena Policy

Directors Desk does not release personally identifying information about our customers except in limited instances related to law, security, or safety. To request customer information from Directors Desk in a civil case, you must serve Directors Desk with a valid subpoena, court order, or search warrant and agree to Directors Desk's terms of compensation below.

All civil subpoenas should be directed to:

Directors Desk, LLC
Subpoena Department
2510 N. Pines Road, Suite 207

Complaint

EXHIBIT C (continued)

DIRECTORS DESK PRIVACY POLICY

<http://www.directorsdesk.com/company/privacy.asp>

Spokane, WA 99206
Fax: 1-509-267-5465



Upon receipt of a valid subpoena, it is Directors Desk's policy to notify the client whose information is sought. In non-emergency circumstances, Directors Desk will generally not produce the subpoenaed subscriber's identity information until approximately two weeks after receipt of the subpoena, unless a formal objection is filed by the customer or we are legally required to do so.

Directors Desk charges \$50.00 per hour for research (plus additional fees if testimony or deposition is required), \$0.25 per page, and \$22.00 to respond via Federal Express. We will invoice the person or entity submitting the subpoena following receipt and the subpoena proponent must make payment within 15 days from the date of receipt of our invoice. Checks should be made out to Directors Desk, LLC.

It is Directors Desk's policy to release information sufficient to identify our customer only where the party seeking the information has filed a legal action that implicates our customer in some legally cognizable impropriety or wrongdoing or can show that the information requested is material to the issues involved in the underlying case. Directors Desk requests a copy of the complaint and all supporting documentation to indicate how the customer's account information is related to the pending litigation. Note that Directors Desk reserves the right to determine in its sole discretion the applicability of this policy to any particular request and, further, this policy does not create any enforceable legal rights, either for our customers or for requesting parties.

Enforcement and Sanctions

All employees and contractors of Directors Desk are required to sign a written acknowledgement that they have read and agree to abide by the terms of this Privacy Policy. Any infractions are subject to severe penalties, including termination and/or legal action.

Decision and Order

DECISION AND ORDER

The Federal Trade Commission, having initiated an investigation of certain acts and practices of the Respondent named in the caption hereof, and the Respondent having been furnished thereafter with a copy of a draft of Complaint which the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued, would charge the Respondent with violation of the Federal Trade Commission Act; and

The Respondent and counsel for the Commission having thereafter executed an agreement containing a consent order, an admission by the Respondent of all the jurisdictional facts set forth in the aforesaid draft complaint, a statement that the signing of the agreement is for settlement purposes only and does not constitute an admission by the Respondent that the law has been violated as alleged in such complaint, or that any of the facts as alleged in such complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission's Rules; and

The Commission having thereafter considered the matter and having determined that it had reason to believe that the Respondent has violated the Federal Trade Commission Act, and that a complaint should issue stating its charges in that respect, and having thereupon accepted the executed consent agreement and placed such agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comments, and having duly considered the comment received from an interested person pursuant to Section 2.34 of its Rules, now in further conformity with the procedure prescribed in Section 2.34 of its Rules, 16 C.F.R. § 2.34, the Commission hereby issues its complaint, makes the following jurisdictional findings, and enters the following order:

1. Respondent Directors Desk LLC is a Delaware limited liability company with its principal office or place of

Decision and Order

business at 1 Liberty Plaza, New York, New York 10006.

2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the Respondent, and the proceeding is in the public interest.

ORDER**DEFINITIONS**

For purposes of this Order, the following definitions shall apply:

- A. Unless otherwise specified, “respondent” shall mean Directors Desk LLC and its subsidiaries, divisions, affiliates, successors and assigns.
- B. “Commerce” shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

I.

IT IS ORDERED that respondent and its officers, agents, representatives, and employees, directly or through any corporation, subsidiary, division, website, or other device, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication, the extent to which respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy, security, or any other compliance program sponsored by the government or any other third party.

Decision and Order

II.

IT IS FURTHER ORDERED that respondent shall maintain and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of, for a period of five (5) years from the date of preparation or dissemination, whichever is later, all documents relating to compliance with this order, including but not limited to:

- A. all advertisements, promotional materials, and any other statements containing any representations covered by this order, with all materials relied upon in disseminating the representation; and
- B. any documents, whether prepared by or on behalf of respondent, that call into question respondent's compliance with this order.

III.

IT IS FURTHER ORDERED that respondent shall deliver a copy of this order to all current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having responsibilities relating to the subject matter of this order, and shall secure from each such person a signed and dated statement acknowledging receipt of the order. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities.

IV.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation(s) that may affect compliance obligations arising under this order, including, but not limited to: a dissolution, assignment, sale, merger, or other action that would result in the

Decision and Order

emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. *Provided, however,* that, with respect to any proposed change in the corporation(s) about which respondent learns fewer than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Part shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

V.

IT IS FURTHER ORDERED that respondent shall, within sixty (60) days after service of this order, and at such other times as the Commission may require, file with the Commission a report, in writing, setting forth in detail the manner and form in which it has complied with this order.

VI.

This order will terminate on January 12, 2030, or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; *provided, however,* that the filing of such a complaint will not affect the duration of:

- A. any Part in this order that terminates in fewer than twenty (20) years;
- B. this order's application to any respondent that is not named as a defendant in such complaint; and

Decision and Order

- C. this order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order as to such respondent will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

Analysis to Aid Public Comment

**ANALYSIS OF PROPOSED CONSENT ORDERS
TO AID PUBLIC COMMENT**

The Federal Trade Commission (“FTC” or “Commission”) has accepted, subject to final approval, a consent agreement from Directors Desk LLC (“Directors Desk”).

The proposed consent order has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission will again review the agreement and the comments received, and will decide whether it should withdraw from the agreement and take appropriate action or make final the agreement’s proposed order.

This matter concerns alleged false or misleading representations that Directors Desk made to consumers concerning its participation in the Safe Harbor privacy framework (“Safe Harbor”) agreed upon by the U.S. and the European Union (“EU”). It is among the Commission’s first cases to challenge deceptive claims about the Safe Harbor. The Safe Harbor provides a mechanism for U.S. companies to transfer data outside the EU consistent with European law. To join the Safe Harbor, a company must self-certify to the U.S. Department of Commerce (“Commerce”) that it complies with seven principles and related requirements. Commerce maintains a public website, www.export.gov/safeharbor, where it posts the names of companies that have self-certified to the Safe Harbor. The listing of companies indicates whether their self-certification is “current” or “not current.” Companies are required to re-certify every year in order to retain their status as “current” members of the Safe Harbor framework.

Directors Desk provides an online application that allows members of corporate boards of directors to access board meeting materials, board minutes, and other related documents through a website (www.directorsdesk.com). According to the

Analysis to Aid Public Comment

Commission's complaint, Directors Desk set forth on its website privacy policies and statements about its practices, including statements that it is a current participant in the Safe Harbor.

The Commission's complaint alleges that Directors Desk falsely represented that it was a current participant in the Safe Harbor when, in fact, from February 2008 until August 2009, Directors Desk was not a current participant in the Safe Harbor. The Commission's complaint alleges that in February 2007, Directors Desk submitted to Commerce a self-certification, which it did not renew in February 2008. Commerce then updated its status to "not current" on the Commerce public website. Directors Desk remained in "not current" status until it submitted a self-certification to Commerce in August 2009.

The proposed order applies to Directors Desk's representations about its membership in any privacy, security, or any other compliance program sponsored by the government or any other third party. It contains provisions designed to prevent Directors Desk from engaging in the future in practices similar to those alleged in the complaint.

Part I of the proposed order prohibits Directors Desk from making misrepresentations about its membership in any privacy, security, or any other compliance program sponsored by the government or any other third party.

Parts II through VI of the proposed order are reporting and compliance provisions. Part II requires Directors Desk to retain documents relating to its compliance with the order for a five-year period. Part III requires dissemination of the order now and in the future to persons with responsibilities relating to the subject matter of the order. Part IV ensures notification to the FTC of changes in corporate status. Part V mandates that Directors Desk submit an initial compliance report to the FTC, and make available to the FTC subsequent reports. Part VI is a provision "sunsetting" the order after twenty (20) years, with certain exceptions.

Analysis to Aid Public Comment

The purpose of the analysis is to facilitate public comment on the proposed order. It is not intended to constitute an official interpretation of the agreement and proposed order or to modify in any way their terms.

Complaint

IN THE MATTER OF

PFIZER, INC.

AND

WYETHCONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF
SEC. 5(A) OF THE FEDERAL TRADE COMMISSION ACT AND SEC. 7
OF THE CLAYTON ACT*Docket No. C-4267; File No. 091 0053*
Filed, October 14, 2009 — Decision, January 25, 2010

This consent order addresses the acquisition by Pfizer Inc., of all of the issued and outstanding shares of Wyeth. Pfizer and Wyeth are two of only four major suppliers in the relevant cattle, companion animal, and equine health products markets. In the majority of these markets, the transaction would reduce the number of competitors from four to three and give Pfizer between 50 and 100 percent of the market and the acquisition would create a monopoly in the market for equine joint-injected steroids in the United States. The complaint alleges that the acquisition would cause significant competitive harm to consumers in the relevant U.S. markets for cattle, companion animal, and equine health products by eliminating actual, direct, and substantial competition between Pfizer and Wyeth. The Consent Agreement requires Pfizer to divest to Boehringer Ingelheim Vetmedica, Inc., Wyeth's U.S. animal health business in all areas of overlap, except for equine tapeworm parasiticides and equine herpesvirus vaccines. In the area of equine tapeworm parasiticides, the consent order requires Pfizer to return to Virbac S.A. Pfizer's exclusive distribution rights for these products; and in the area of equine herpesvirus vaccines, Pfizer is ordered to divest to BI Pfizer's equine herpesvirus products. The assets for each of the divestitures include all of the relevant intellectual property, customer lists, research and development information, and regulatory materials, as well as two of Wyeth's three U.S. manufacturing facilities.

Participants

For the *Commission*: Michael R. Barnett, Susan Huber, Lynda Lao, Gregory P Luib, David Von Nirschl, and Kari A. Wallace.

For the *Respondents*: Andrew J. Forman and Charles F. (Rick) Rule, Cadwalader, Wickersham & Taft LLP; Harry T.