

Complaint

IN THE MATTER OF

HTC AMERICA INC.CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF
SECTION 5(A) OF THE FEDERAL TRADE COMMISSION ACT

Docket No. C-4406; File No. 122 3049
Complaint, June 25, 2013 – Decision, June 25, 2013

The consent order addresses allegations that HTC America failed to take reasonable steps to secure the software it developed for its smartphones and tablet computers, in violation of Section 5(a) of the FTC Act. According to the complaint, HTC America failed to provide its engineering staff with adequate security training, failed to review or test the software on its mobile devices for potential security vulnerabilities, failed to follow well-known and commonly accepted secure coding practices, and failed to establish a process for receiving and addressing vulnerability reports from third parties. As a result of HTC America's failure to implement reasonable security measures, malware was permitted to be placed on millions of consumers' devices without their permission. This malware could be used to record and transmit information entered into or stored on the device, including, for example, financial account numbers and related access codes, geolocation information, or medical information such as text messages received from healthcare providers and calendar entries concerning doctor's appointments. The complaint further alleges that the user manuals for HTC America's Android-based devices contained deceptive representations. The consent order requires HTC America to develop and release software patches to repair the vulnerabilities in its devices. The consent order further requires HTC America to establish a comprehensive security program designed to address security risks during the development of its devices and to undergo independent security assessments every other year for the next 20 years.

Participants

For the *Commission*: *Nithan Sannappa* and *Jonathan Zimmerman*.

For the *Respondent*: *Susan Lu Lyon, Cooley LLP*.

COMPLAINT

The Federal Trade Commission, having reason to believe that HTC America, Inc. ("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 HTC America Inc. (“HTC”) is a Washington corporation with its principal office or place of business at 13920 SE Eastgate Way, Suite #400, Bellevue, WA 98005.

2. 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.

3. Respondent is a mobile device manufacturer that develops and manufactures smartphones and tablet computers using Google Inc.’s (“Google”) Android operating system and Microsoft Corporation’s (“Microsoft”) Windows Mobile and Windows Phone mobile operating systems.

ANDROID’S PERMISSION-BASED SECURITY MODEL

4. Google’s Android operating system protects certain sensitive information (e.g., location information or the contents of text messages) and sensitive device functionality (e.g., the ability to record audio through the device’s microphone or the ability to take photos with the device’s camera) through a permission-based security model. In order to access sensitive information or sensitive device functionality, a third-party application must declare the fact that it will access such information or functionality.

5. Before a user installs a third-party application, the Android operating system provides notice to the user regarding what sensitive information or sensitive device functionality the application has declared it requires. The user must accept these “permissions” in order to complete installation of the third-party application.

**HTC’S FAILURE TO EMPLOY REASONABLE
SECURITY IN THE CUSTOMIZATION OF ITS MOBILE
DEVICES**

6. HTC has customized its Android-based mobile devices by adding and/or modifying various pre-installed applications and components in order to differentiate its products from those of competitors also manufacturing Android-based mobile devices.

Complaint

HTC has also customized both its Android and Windows Mobile devices in order to comply with the requirements of certain network operators, such as Sprint Nextel Corporation (“Sprint”) and AT&T Mobility LLC (“AT&T”). Since the customized applications and components are pre-installed on the device, consumers do not choose to install the customized applications and components, and the device user interface does not provide consumers with an option to uninstall or remove the customized applications and components from the device.

7. Until at least November 2011, respondent engaged in a number of practices that, taken together, failed to employ reasonable and appropriate security in the design and customization of the software on its mobile devices. Among other things, respondent: (a) failed to implement an adequate program to assess the security of products it shipped to consumers; (b) failed to implement adequate privacy and security guidance or training for its engineering staff; (c) failed to conduct assessments, audits, reviews, or tests to identify potential security vulnerabilities in its mobile devices; (d) failed to follow well-known and commonly-accepted secure programming practices, including secure practices that were expressly described in the operating system’s guides for manufacturers and developers, which would have ensured that applications only had access to users’ information with their consent; and (e) failed to implement a process for receiving and addressing security vulnerability reports from third-party researchers, academics or other members of the public, thereby delaying its opportunity to correct discovered vulnerabilities or respond to reported incidents.

8. As a result of its failures described in Paragraph 7, HTC introduced numerous security vulnerabilities in the process of customizing its mobile devices. Once in place, HTC failed to detect and mitigate these vulnerabilities, which, if exploited, provide third-party applications with unauthorized access to sensitive information and sensitive device functionality. The following examples in paragraphs 9 to 15 serve to illustrate the consequences of HTC’s failure to employ reasonable and appropriate security in the design and customization of the software on its mobile devices.

Complaint

PERMISSION RE-DELEGATION

9. HTC undermined the Android operating system's permission-based security model in its devices by introducing numerous "permission re-delegation" vulnerabilities through its custom, pre-installed applications. Permission re-delegation occurs when one application that has permission to access sensitive information or sensitive device functionality provides another application that has not been given the same level of permission with access to that information or functionality. For example, under the Android operating system's security framework, a third-party application must receive the user's permission to access the device's microphone, since the ability to record audio is considered sensitive functionality. But in its devices, HTC pre-installed a custom voice recorder application that, if exploited, would provide any third-party application access to the device's microphone, even if the third-party application had not requested permission for that functionality.

10. HTC could have prevented this by including simple, well-documented software code - "permission check" code - in its voice recorder application to check that the third-party application had requested the necessary permission. Because HTC failed in numerous instances to include permission check code in its custom, pre-installed applications, any third-party application exploiting these vulnerabilities could command those HTC applications to access various sensitive information and sensitive device functionality on its behalf -- including enabling the device's microphone; accessing the user's GPS-based, cell-based, and WiFi-based location information; and sending text messages - all without requesting the user's permission.

11. Malware could exploit these vulnerabilities to, for example, surreptitiously record phone conversations or other sensitive audio, to surreptitiously track a user's physical location, and to perpetrate "toll fraud," the practice of sending text messages to premium numbers in order to charge fees to the user's phone bill. These vulnerabilities have been present on approximately 18.3 million HTC devices running Android v. 2.1.x, 2.2.x, 2.3.x, and 3.0.x.

Complaint

APPLICATION INSTALLATION VULNERABILITY

12. Relatedly, HTC pre-installed a custom application on its Android-based devices that could download and install applications outside of the normal Android installation process. Again, HTC failed to include appropriate permission check code to protect this pre-installed application from exploitation. As a result, any third-party application exploiting the vulnerability could command this pre-installed application to download and install any additional applications from any server onto the device without the user's knowledge or consent. Because this would occur outside the normal installation process, the user would not be presented with a permission screen that explained what sensitive information or sensitive device functionality the additional application being installed would be able to access. In effect, this vulnerability undermines all protections provided by Android's permission-based security model. This vulnerability has been present on approximately 18.3 million HTC devices running Android v. 2.1.x, 2.2.x, 2.3.x, 3.0.x and certain devices that were upgraded to Android v. 4.0.x.

INSECURE COMMUNICATIONS MECHANISMS

13. HTC failed to use readily-available and documented secure communications mechanisms in implementing logging applications on its devices, placing sensitive information at risk. Logging applications collect information that can be used, for example, to diagnose device or network problems. Because of the sensitivity of the information, as described below, communications with logging applications should be secure to ensure that only designated applications can access the information. Secure communications mechanisms -- such as the Android inter-process communication mechanisms expressly described in the Android developer guides, or secure UNIX sockets -- could have been used to ensure that only HTC-designated applications could access the sensitive information collected by the logging application. Instead of using one of these well-known, secure alternatives, HTC implemented communication mechanisms (e.g., INET sockets) that could not be restricted in a similar manner. Moreover, HTC failed to implement other, additional security measures (e.g., data

Complaint

encryption) that could have secured these communications mechanisms. Because the communications mechanisms were insecure, any third-party application that could connect to the internet could communicate with the logging applications on HTC devices and access a variety of sensitive information and sensitive device functionality, as described below.

- a. HTC Loggers. Beginning in May 2010, HTC installed its customer support and trouble-shooting tool HTC Loggers on approximately 12.5 million Android-based mobile devices. Because HTC Loggers could collect sensitive information from various device logs, it was supposed to have been accessible only to HTC and certain network operators, and only after the user had consented to its use by manually entering a special code into the mobile device. Moreover, the Android permission-based security model normally requires a third-party application to obtain the user's consent before accessing the device logs. Because HTC used an insecure communications mechanism, however, both of these intended protections were undermined, and any third-party application on the user's device that could connect to the internet could exploit the vulnerability to communicate with HTC Loggers without authorization and command it to collect and transmit information from the device logs. This information could include, but was not limited to, contents of text messages; last known location and a limited history of GPS and network locations; a user's personal phone number, phone numbers of contacts, and phone numbers of those who send text messages to the user; dialed digits; web browsing and media viewing history; International Mobile Equipment Identity ("IMEI") or Mobile Equipment Identifier ("MEID"); and registered accounts such as Gmail and Microsoft Exchange account user names.
- b. Carrier IQ. Beginning in 2009, HTC embedded Carrier IQ diagnostics software on approximately 10.3 million Android-based mobile devices and 330,000 Windows Mobile-based mobile devices at the direction of network operators Sprint and AT&T, who used

Complaint

Carrier IQ to collect a variety of information, described in subparagraph (i) below, from user devices to analyze network and device problems. In order to embed the Carrier IQ software on its mobile devices, HTC developed a “CIQ Interface” that would pass the necessary information to the Carrier IQ software. The information collected by the Carrier IQ software was supposed to have been accessible only to the network operators, but because HTC used an insecure communications mechanism, any third-party application on the user’s device that could connect to the internet could exploit the vulnerability to communicate with the CIQ Interface, allowing it to:

- i. Intercept the sensitive information being collected by the Carrier IQ software. This information could include, but was not limited to, GPS-based location information; web browsing and media viewing history; the size and number of all text messages; the content of each incoming text message; the names of applications on the user’s device; the numeric keys pressed by the user; and any other usage and device information specified for collection by certain network operators; and
- ii. In the case of HTC’s Android-based devices, perform potentially malicious actions, including, but not limited to, sending text messages without permission. As described in Paragraph 11, malware could exploit this vulnerability to perpetrate toll fraud. Moreover, in this case, the sent text messages would not appear in the user’s outbox, making it impossible for the user to verify that unauthorized text messages had been sent from the device.

DEBUG CODE

14. During the development of an application, developers may activate “debug code” in order to help test whether the application is functioning as intended. When developing its CIQ Interface for

Complaint

its Android-based devices, HTC activated debug code in order to test whether the CIQ Interface properly sent all of the information specified by the network operator. The debug code accomplished this by writing the information to a particular device log known as the Android system log, which could then be reviewed. However, HTC failed to deactivate the debug code before its devices shipped for sale to consumers. As a result of the active debug code, all information that the CIQ Interface sent to the Carrier IQ software from a consumer's device, including the information specified in Paragraph 13(b)(i), was also written to the Android system log on the device. This information was supposed to have been accessible only to the network operators, never written to the system log. Because it ended up in the system log, this sensitive information was:

- a. Accessible to any third-party application with permission to read the system log. Although users may provide third-party applications with permission to read the system log for certain purposes -- for example, to trouble-shoot application crashes -- those applications never should have had access to all the sensitive information, such as the contents of incoming text messages, that the Carrier IQ software was collecting.
- b. Sent to HTC. The information in the system log is sent to HTC when a user chooses to send HTC an error report through its "Tell HTC" error reporting tool, described in Paragraph 20. Accordingly, in some cases, HTC also received this sensitive information, including users' GPS-based location information.

15. HTC could have detected its failure to deactivate the debug code in its CIQ Interface had it had adequate processes and tools in place for reviewing and testing the security of its software code.

**CONSUMERS RISK HARM DUE TO HTC'S SECURITY
FAILURES**

16. Because of the potential exposure of sensitive information and sensitive device functionality through the security

Complaint

vulnerabilities in HTC mobile devices, consumers are at risk of financial and physical injury and other harm. Among other things, malware placed on consumers' devices without their permission could be used to record and transmit information entered into or stored on the device, including financial account numbers and related access codes or personal identification numbers, medical information, and personal information such as text messages and photos. Sensitive information exposed on the devices could be used, for example, to target spear-phishing campaigns, physically track or stalk individuals, and perpetrate fraud, resulting in costly bills to the consumer. Misuse of sensitive device functionality such as the device's audio recording feature would allow hackers to capture private details of an individual's life.

17. In fact, malware developers have targeted the types of sensitive information and sensitive device functionalities that potentially are exposed through the security vulnerabilities in HTC mobile devices. Text message toll fraud, for example, is one of the most common types of Android malware. Security researchers have also found Android malware that records and stores users' phone conversations and that tracks users' physical location.

18. Had HTC implemented an adequate security program, it likely would have prevented, or at least timely resolved, many of the serious security vulnerabilities it introduced through the process of customizing its mobile devices. HTC could have implemented readily-available, low-cost measures to address these vulnerabilities – for example, adding a few lines of permission check code when programming its pre-installed applications, or implementing its logging applications with secure communications mechanisms. Consumers had little, if any, reason to know their information was at risk because of the vulnerabilities introduced by HTC.

HTC'S PRIVACY AND SECURITY REPRESENTATIONS

19. Since at least October 2009, user manuals for HTC's Android-based mobile devices contained the following

Complaint

statements, or similar statements, regarding Android's permission-based security model:

Finding and Installing an Application

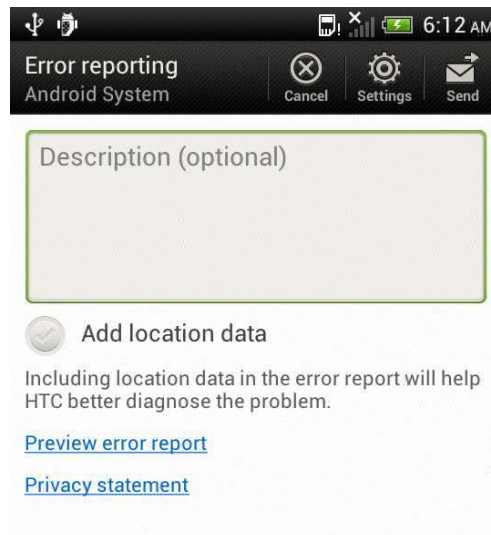
When you install apps from Android Market and use them on your device, they may require access to your personal information (such as your location, contact data, and more) or access to certain functions or settings of your device. Download and install only apps that you trust.

...

5. The subsequent screen notifies you whether the app will require access to your personal information or access to certain functions or settings of your device. If you agree to the conditions, tap **OK** to begin downloading and installing the app. If you selected a paid application, after tapping **OK**, you're redirected to the Google Checkout screen to pay for the application before it's downloaded to your device.

WARNING: Read it carefully! Be especially cautious with applications that have access to many functions or a significant amount of your data. Once you tap **OK** on this screen, you are responsible for the results of using this item on your device.

20. Since at least June 2011, HTC has, in many of its Android-based mobile devices, included the Tell HTC error reporting tool. The error reporting tool provides the user with an opportunity to send a report to HTC when there is an application or system crash. The report includes the information in the Android system log. The Tell HTC user interface provides the user with the additional option of submitting location information with the report by checking the button marked "Add location data," as depicted below:



Complaint

Through this user interface, HTC represents that the user's location data will not be sent to HTC if the user does not check the button marked "Add location data."

HTC'S UNFAIR SECURITY PRACTICES (Count 1)

21. As set forth in Paragraph 7-18, HTC failed to employ reasonable and appropriate security practices in the design and customization of the software on its mobile devices. HTC's practices caused, or are likely to cause, substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was, and is, an unfair act or practice.

HTC'S DECEPTIVE ANDROID USER MANUALS (Count 2)

22. As described in Paragraph 19, HTC has represented, expressly or by implication, that, through the Android permission-based security model, a user of an HTC Android-based mobile device would be notified when a third-party application required access to the user's personal information or to certain functions or settings of the user's device before the user completes installation of the third-party application.

23. In truth and in fact, in many instances, a user of an HTC Android-based mobile device would not be notified when a third-party application required access to the user's personal information or to certain functions or settings of the user's device before the user completes installation of the third-party application. Due to the security vulnerabilities described in Paragraphs 8-15, third-party applications could access a variety of sensitive information and sensitive device functionality on HTC Android-based mobile devices without notifying or obtaining consent from the user before installation. Therefore, the representation set forth in Paragraph 22 constitutes a false or misleading representation.

Complaint

**HTC'S DECEPTIVE TELL HTC USER INTERFACE
(Count 3)**

24. As described in Paragraph 20, HTC has represented, expressly or by implication, that, if a user does not check the button marked "Add location data" when submitting an error report through the Tell HTC application, location data would not be sent to HTC with the user's error report.

25. In truth and in fact, in some instances, if a user did not check the button marked "Add location data" when submitting an error report through the Tell HTC application, location data was nevertheless sent to HTC with the user's error report. Due to the security vulnerability described in Paragraph 14, in some instances, HTC collected the user's GPS-based location information through the Tell HTC error reporting tool even when the user had not checked the button marked "Add location data" in the Tell HTC user interface. Therefore, the representation set forth in Paragraph 24 constitutes a false or misleading representation.

26. The acts and practices of respondent 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 Trade Commission Act, 15 U.S.C. § 45(a).

THEREFORE, the Federal Trade Commission this twenty-fifth day of June, 2013, has issued this complaint against respondent.

By the Commission, Commissioner Ohlhausen recused.

Decision and Order

DECISION AND ORDER

The Federal Trade Commission (“Commission” or “FTC”), 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 complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge respondent with violations of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 45, *et seq.*;

The respondent, its attorney, and counsel for the Commission having thereafter executed an Agreement Containing Consent Order (“Consent Agreement”), which includes: a statement by respondent that it neither admits nor denies any of the allegations in the draft complaint, except as specifically stated in the Consent Agreement, and, only for purposes of this action, admits the facts necessary to establish jurisdiction; 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 FTC 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 comments received from interested persons pursuant to section 2.34 of its Rules, now in further conformity with the procedure prescribed in Commission Rule 2.34, 16 C.F.R. § 2.34, the Commission hereby issues its complaint, makes the following jurisdictional findings, and enters the following Order:

1. Respondent HTC America, Inc. (“HTC”) is a Washington corporation with its principal office or place of business at 13920 SE Eastgate Way, Suite #400, Bellevue, WA 98005.

Decision and Order

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:

1. Unless otherwise specified, “respondent” shall mean HTC America, Inc., and its successors and assigns.
2. “Commerce” shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.
3. “Covered device” shall mean any desktop computer, laptop computer, tablet, handheld or mobile device, telephone, or other electronic product or device developed by respondent or any corporation, subsidiary, division, or affiliate owned or controlled by respondent that has a platform on which to download, install, or run any software program, code, script, or other content and to play any digital audio, visual, or audiovisual content.
4. “Covered information” shall mean individually-identifiable information from or about an individual consumer collected by respondent through a covered device or input into, stored on, captured with, or transmitted through a covered device, including but not limited to (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a telephone number; (e) a Social Security number; (f) a driver’s license or other state-issued identification number; (g) a financial institution account number; (h) credit or debit card information; (i) a persistent identifier, such as a customer number held in a “cookie,” a static Internet

Decision and Order

Protocol (“IP”) address, a mobile device ID, or processor serial number; (j) precise geo-location data of an individual or mobile device, including GPS-based, WiFi-based, or cell-based location information; (k) an authentication credential, such as a username and password; or (l) any other communications or content that is input into, stored on, captured with, accessed or transmitted through a covered device, including but not limited to contacts, emails, text messages, photos, videos, and audio recordings.

5. “Covered device functionality” shall mean any capability of a covered device to capture, access, or transmit covered information.

I.

IT IS ORDERED that respondent and its officers, agents, representatives, and employees, directly or through any corporation, subsidiary, division, website, or other device or affiliate owned or controlled by respondent, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication, the extent to which respondent or its products or services, including any covered devices, use, maintain and protect the security of covered device functionality or the security, privacy, confidentiality, or integrity of any covered information from or about consumers.

II.

IT IS FURTHER ORDERED that respondent shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive security program that is reasonably designed to (1) address security risks related to the development and management of new and existing covered devices, and (2) protect the security, confidentiality, and integrity of covered information, whether collected by respondent or input into, stored on, captured with, accessed or transmitted through a covered device. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to

Decision and Order

respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the covered device functionality or covered information, including:

- A. the designation of an employee or employees to coordinate and be accountable for the security program;
- B. the identification of material internal and external risks to the security of covered devices that could result in unauthorized access to or use of covered device functionality, and assessment of the sufficiency of any safeguards in place to control these risks;
- C. the identification of material internal and external risks to the security, confidentiality, and integrity of covered information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, whether such information is in respondent's possession or is input into, stored on, captured with, accessed or transmitted through a covered device, and assessment of the sufficiency of any safeguards in place to control these risks;
- D. at a minimum, the risk assessments required by subparts B and C should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) product design, development and research; (3) secure software design and testing, including secure engineering and defensive programming; and (4) review, assessment, and response to third-party security vulnerability reports;
- E. the design and implementation of reasonable safeguards to control the risks identified through the risk assessments, including through reasonable and appropriate software security testing techniques, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures;

Decision and Order

- F. the development and use of reasonable steps to select and retain service providers capable of maintaining security practices consistent with this order, and requiring service providers by contract to implement and maintain appropriate safeguards; and
- G. the evaluation and adjustment of the security program in light of the results of the testing and monitoring required by subpart E, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its security program.

Provided, however, that this Part does not obligate respondent to identify and correct security vulnerabilities in third parties' software on covered devices to the extent the vulnerabilities are not the result of respondent's integration, modification, or customization of the third party software.

III.

IT IS FURTHER ORDERED that respondent shall develop security patches to fix the security vulnerabilities described in Attachment A for each affected covered device having an operating system version released on or after December 2010. Within thirty (30) days of service of this order, respondent shall release the applicable security patch(es) either directly to affected covered devices or to the applicable network operator for deployment of the security patch(es) to the affected covered devices. Respondent shall provide users of the affected covered devices with clear and prominent notice regarding the availability of the applicable security patch(es) and instructions for installing the applicable security patch(es).

IV.

IT IS FURTHER ORDERED that, in connection with its compliance with Part II of this order, respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who

Decision and Order

uses procedures and standards generally accepted in the profession. Professionals qualified to prepare such Assessments shall be: a person qualified as a Certified Secure Software Lifecycle Professional (CSSLP) with experience in secure mobile programming; or as a Certified Information System Security Professional (CISSP) with professional experience in the Software Development Security domain and secure mobile programming; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580. The reporting period for the Assessments shall cover: (1) the first one hundred eighty (180) days after service of the order for the initial Assessment; and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

- A. set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;
- B. explain how such safeguards are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the covered device functionality or covered information;
- C. explain how the safeguards that have been implemented meet or exceed the protections required by Part II of this order; and
- D. certify that respondent's security program is operating with sufficient effectiveness to provide reasonable assurance that the security of covered device functionality and the security, confidentiality, and integrity of covered information is protected and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been

Decision and Order

prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request. Unless otherwise directed by a representative of the Commission, the initial Assessment, and any subsequent Assessments requested, shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of HTC America, Inc.*, FTC File No. 1223049. Provided, however, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

V.

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:

- A. for a period of three (3) years after the date of preparation of each Assessment required under Part IV of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of the respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to respondent's compliance with Parts II and III of this order, for the compliance period covered by such Assessment;
- B. unless covered by V.A, for a period of three (3) years from the date of preparation or dissemination, whichever is later, all other documents relating to compliance with this order, including but not limited to:
 - 1. all advertisements and promotional materials containing any representations covered by this

Decision and Order

order, as well as all materials used or relied upon in making or disseminating the representation; and

2. any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this order.

VI.

IT IS FURTHER ORDERED that respondent shall deliver a copy of this order to all current and future subsidiaries, 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. Respondent shall deliver this order to such current subsidiaries and personnel within thirty (30) days after service of this order, and to such future subsidiaries and personnel within thirty (30) days after the person assumes such position or responsibilities.

VII.

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 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. Unless otherwise directed by a representative of the Commission, all notices required by this Part shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line In the matter of HTC America, Inc., FTC File No. 1223049. Provided, however, that in lieu of overnight courier, notices may be sent by

Decision and Order

first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

VIII.

IT IS FURTHER ORDERED that respondent within sixty (60) days after the date of service of this order, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of its compliance with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, it shall submit an additional true and accurate written report.

IX.

This order will terminate on June 25, 2033, 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
- C. this order if such complaint is filed after the order has terminated pursuant to this Part.

Decision and Order

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, Commissioner Ohlhausen recused.

Decision and Order

ATTACHMENT A

PERMISSION RE-DELEGATION

1. Permission re-delegation occurs when one application that has permission to access covered information or covered device functionality provides another application that has not been given the same level of permission with access to that information or functionality. Because HTC failed in numerous instances to include “permission check” code in its custom, pre-installed applications on its Android-based devices, any third-party application exploiting these vulnerabilities could command those HTC applications to access various covered information and covered device functionality on its behalf -- including enabling the device’s microphone; accessing the user’s GPS-based, cell-based, and WiFi-based location information; and sending text messages -- all without requesting the user’s permission.

APPLICATION INSTALLATION VULNERABILITY

2. HTC pre-installed a custom application on its Android-based devices that could download and install applications outside of the normal Android installation process. HTC failed to include appropriate permission check code to protect this pre-installed application from exploitation. As a result, any third-party application exploiting the vulnerability could command this pre-installed application to download and install any additional applications from any server onto the device without the user’s knowledge or consent.

INSECURE COMMUNICATIONS MECHANISMS

3. HTC failed to use readily-available and documented secure communications mechanisms in implementing logging applications on its devices, placing covered information at risk. Communications with logging applications should be secure to ensure that only designated applications can access the information. HTC implemented insecure communication mechanisms, as described below.

Decision and Order

ATTACHMENT A

- a. HTC Loggers. HTC installed its customer support and trouble-shooting tool HTC Loggers on Android-based mobile devices. Because HTC Loggers could collect sensitive information from various device logs, it was supposed to have been accessible only to HTC and network operators. Because HTC used an insecure communications mechanism, however, any third-party application on the user's device that could connect to the internet could exploit this vulnerability to communicate with HTC Loggers without authorization and command it to collect and transmit covered information from the device logs.
- b. Carrier IQ. HTC embedded Carrier IQ diagnostics software on Android-based mobile devices and Windows Mobile-based mobile devices at the direction of network operators who used Carrier IQ to collect a variety of covered information from user devices to analyze network and device problems. In order to embed the Carrier IQ software on its mobile devices, HTC developed a "CIQ Interface" that would pass the necessary information to the Carrier IQ software. Because HTC used an insecure communications mechanism, any third-party application on the user's device that could connect to the internet could exploit this vulnerability to communicate with the CIQ Interface, allowing it to:
 - i. Intercept the covered information being collected by the Carrier IQ software; and
 - ii. In the case of HTC's Android-based devices, perform potentially malicious actions, including, but not limited to, sending text messages without permission.

DEBUG CODE

4. During the development of its CIQ Interface for its Android-based devices, HTC activated "debug code" in order to help test whether the CIQ Interface was functioning as intended,

Decision and Order

ATTACHMENT A

but then failed to deactivate the code before its devices shipped for sale to consumers. As a result of the active debug code, covered information was written to the Android system log, and was accessible to any third-party application with permission to read the system log, and in many instances, was also sent to HTC.

Analysis to Aid Public Comment

**ANALYSIS OF CONSENT ORDER TO AID PUBLIC
COMMENT**

The Federal Trade Commission has accepted, subject to final approval, a consent order applicable to HTC America, Inc. (“HTC”).

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.

HTC is a mobile device manufacturer that develops and manufactures smartphones and tablet computers using Google Inc.’s Android operating system and Microsoft Corporation’s Windows Mobile and Windows Phone operating systems. HTC has customized its Android-based mobile devices by adding or modifying various pre-installed applications and components in order to differentiate its products from those of competitors also manufacturing Android-based mobile devices. HTC has also customized both its Android and Windows Mobile devices in order to comply with the requirements of certain network operators. As the customized applications and components are pre-installed on the device, consumers do not choose to install the customized applications and components, and the device user interface does not provide consumers with an option to uninstall or remove the customized applications and components from the device.

The Commission’s complaint alleges that HTC engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security in the design and customization of software on its mobile devices. Among other things, HTC:

- (1) failed to implement an adequate program to assess the security of products it shipped to consumers;

Analysis to Aid Public Comment

- (2) failed to implement adequate privacy and security guidance or training for its engineering staff;
- (3) failed to conduct assessments, audits, reviews, or tests to identify potential security vulnerabilities in its mobile devices;
- (4) failed to follow well-known and commonly-accepted secure programming practices, including secure practices that were expressly described in the operating system's guides for manufacturers and developers, which would have ensured that applications only had access to users' information with their consent;
- (5) failed to implement a process for receiving and addressing security vulnerability reports from third-party researchers, academics or other members of the public, thereby delaying its opportunity to correct discovered vulnerabilities or respond to reported incidents.

The complaint further alleges that, due to these failures, HTC introduced numerous security vulnerabilities in the process of customizing its mobile devices. Once in place, HTC failed to detect and mitigate these vulnerabilities, which, if exploited, provide third-party applications with unauthorized access to sensitive information and sensitive device functionality. The sensitive device functionality potentially exposed by the vulnerabilities includes the ability to send text messages without permission, the ability to record audio with the device's microphone without permission, and the ability to install other applications, including malware, onto the device without the user's knowledge or consent. The complaint alleges that malware placed on consumers' devices without their permission could be used to record and transmit information entered into or stored on the device, including financial account numbers and related access codes or personal identification numbers, and medical information. In addition, other sensitive information exposed by the vulnerabilities includes, but is not limited to, location information, the contents of text messages, the user's personal phone number, phone numbers of contacts, phone numbers of

Analysis to Aid Public Comment

those who send text messages to the user, and the user's web and media viewing history.

The proposed order contains provisions designed to prevent HTC from engaging in the future in practices similar to those alleged in the complaint.

Part I of the proposed order prohibits HTC from misrepresenting the extent to which HTC or its products or services -- including any covered device -- use, maintain and protect the security of covered device functionality or the security, privacy, confidentiality, or integrity of covered information from or about consumers. Part II of the proposed order requires HTC to (1) address security risks related to the development and management of new and existing covered devices, and (2) protect the security, confidentiality, and integrity of covered information, whether collected by respondent or input into, stored on, captured with, accessed or transmitted through a covered device. The security program must contain administrative, technical, and physical safeguards appropriate to HTC's size and complexity, nature and scope of its activities, and the sensitivity of the information collected from or about consumers. Specifically, the proposed order requires HTC 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 of covered devices that could result in unauthorized access to or use of covered device functionality, and assess the sufficiency of any safeguards in place to control these risks;
- identify material internal and external risks to the security, confidentiality, and integrity of covered information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, whether such information is in HTC's possession or is input into, stored on, captured with, accessed or transmitted through a covered device, and assess the sufficiency of any safeguards in place to control these risks;

Analysis to Aid Public Comment

- consider risks in each area of relevant operation, including but not limited to (1) employee training and management; (2) product design, development and research; (3) secure software design and testing, including secure engineering and defensive programming; and (4) review, assessment, and response to third-party security vulnerability reports;
- design and implement reasonable safeguards to control the risks identified through risk assessment, including through reasonable and appropriate software security testing techniques, 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 maintaining security practices consistent with the order, and require service providers by contract to implement and maintain appropriate safeguards; and
- evaluate and adjust its information security program in light of the results of testing and monitoring, any material changes to HTC's operations or business arrangement, or any other circumstances that it knows or has reason to know may have a material impact on its security program.

However, Part II does not require HTC to identify and correct security vulnerabilities in third parties' software on covered devices to the extent the vulnerabilities are not the result of respondent's integration, modification, or customization of the third party software.

Part III of the proposed order requires HTC to develop security patches to fix the security vulnerabilities in each affected covered device having an operating system version released on or after December 2010. Within thirty (30) days of service of the order, HTC must release the security patches either directly to affected covered devices or to the applicable network operator for deployment to the affected covered devices. HTC must provide users of the affected covered devices with clear and prominent

Analysis to Aid Public Comment

notice regarding the availability of the security patches and instructions for installing the security patches.

Part IV of the proposed order requires HTC to obtain, within the first one hundred eighty (180) days after service of the order and on a biennial basis thereafter for a period of twenty (20) years, an assessment and report from a qualified, objective, independent third-party professional, certifying, among other things, that: (1) it has in place a security program that provides protections that meet or exceed the protections required by Part II of the proposed order; and (2) its security program is operating with sufficient effectiveness to provide reasonable assurance that the security of covered device functionality and the security, confidentiality, and integrity of covered information is protected.

Parts V through IX of the proposed order are reporting and compliance provisions. Part V requires HTC to retain documents relating to its compliance with the order. The order requires that the documents be retained for a three-year period. Part VI requires dissemination of the order now and in the future to all current and future principals, officers, directors, and managers, and to persons with responsibilities relating to the subject matter of the order. Part VII ensures notification to the FTC of changes in corporate status. Part VIII mandates that HTC submit a compliance report to the FTC within 60 days, and periodically thereafter as requested. Part IX is a provision “sunsetting” the order after twenty (20) years, with certain exceptions.

The purpose of this analysis is to facilitate public comment on the proposed order. It is not intended to constitute an official interpretation of the proposed complaint or order or to modify the order’s terms in any way.

INTERLOCUTORY, MODIFYING, VACATING, AND MISCELLANEOUS ORDERS

PHOEBE PUTNEY HEALTH SYSTEM, INC., PHOEBE
PUTNEY MEMORIAL HOSPITAL, INC., PHOEBE NORTH,
INC., HCA INC., PALMYRA PARK HOSPITAL, INC.,
AND
HOSPITAL AUTHORITY OF ALBANY-DOUGHERTY
COUNTY

Docket No. D-9348. Order, March 14, 2013

Order granting Complaint Counsel's motion to lift the stay of the administrative proceedings and reset the hearing schedule, in light of the Supreme Court's decision in a collateral federal court action.

ORDER GRANTING COMPLAINT COUNSEL'S MOTION TO LIFT STAY

On July 15, 2011, on Respondents' unopposed motion and pursuant to Rule 3.41(f) of the Commission's Rules of Practice, 16 C.F.R. § 3.41(f), the Commission stayed the administrative proceeding in this matter pending the appellate resolution of a collateral federal court action. On February 19, 2013, the Supreme Court of the United States issued its decision in that collateral action, in view of which Complaint Counsel now moves the Commission to lift the administrative stay and to order the resetting of the administrative hearing schedule. For the reasons noted below, the Commission has determined to grant the motion, and to direct the Chief Administrative Law Judge to hold a scheduling conference in this matter promptly to reset the necessary scheduling deadlines, including a new hearing, which should begin as soon as is practicable but no later than July 15, 2013.

The Commission issued the administrative complaint in this matter on April 19, 2011, alleging that the then-proposed acquisition of Palmyra Park Hospital, Inc. (Palmyra) by Phoebe Putney Health System, Inc. ("PPHS"), Phoebe Putney Memorial Hospital, Inc. ("PPMH"), Phoebe North, Inc. ("PNI") and the Hospital Authority of Albany-Dougherty County from HCA Inc.

Interlocutory Orders, Etc.

would reduce competition substantially and allow the combined entity to raise prices for general acute-care hospital services charged to commercial health plans in Albany, Georgia, and the surrounding region, in violation of Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, and – if consummated – Section 7 of the Clayton Act, 15 U.S.C. § 18. Administrative proceedings began under Chief Administrative Law Judge Chappell, and a hearing was scheduled to begin on September 19, 2011.

On April 20, 2011, the Commission filed in the United States District Court for the Middle District of Georgia a complaint for a preliminary injunction pending resolution of the Commission’s administrative proceeding. The defendants there (Respondents here) did not contest the antitrust merits of the Commission’s complaint, but moved the district court to dismiss the collateral action on the ground that the state action doctrine exempts the challenged acquisition of Palmyra from federal antitrust law. The District Court agreed with the defendants and dismissed the complaint for failure to state a claim. The Commission appealed that ruling to the United States Court of Appeals for the Eleventh Circuit and, as noted above, stayed its administrative proceeding pending appellate resolution of the collateral court action.

Following the Eleventh Circuit’s affirmance of the district court’s ruling,¹ the Supreme Court granted certiorari to hear the case and, on February 19, 2013, unanimously reversed the judgment of the court of appeals, adopting instead the standard for state action antitrust exemption advocated by the Commission. *FTC v. Phoebe Putney Health Sys., Inc.*, No. 11-1160, Slip Op. (U.S. Feb. 19, 2013). The Court held that the challenged transaction was not exempt from federal antitrust law: “respondents’ claim for state-action immunity fails because there is no evidence the State affirmatively contemplated that hospital authorities would displace competition by consolidating hospital ownership.” Slip Op. 9. Accordingly, the Court remanded the case to the Eleventh Circuit for further proceedings in light of its decision.

¹ The court of appeals had issued a stay pending appeal to block the consummation of the challenged transaction, but following its appellate decision, it lifted that stay, and Phoebe Putney concluded its acquisition of Palmyra on December 15, 2011.

Interlocutory Orders, Etc.

With the only ground for the administrative stay now resolved, Complaint Counsel moves for lifting the stay on the administrative proceeding, noting that time is of the essence because “this is now a consummated acquisition in which significant integration of hospital assets and operations—and likely, interim harm to competition—may have taken place.” (Motion at 4.) We agree. “To the extent practicable and consistent with requirements of law, the Commission’s policy is to conduct [adjudicative] proceedings expeditiously.” 16 C.F.R. § 3.1; *see also id.* § 3.41(b) (“Hearings shall proceed with all reasonable expedition . . .”).

The sole ground for Respondents’ opposition to lifting the stay—that it would be premature because the Supreme Court’s decision is not yet final—does not withstand scrutiny. The Supreme Court’s decision concerns a separate (albeit related) action. The Commission’s stay order was discretionary, and it remains entirely proper, therefore, for the Commission to restart its own administrative proceeding. *See* Rule 3.41(f), 16 C.F.R. § 3.41(f) (“The pendency of a collateral federal court action that relates to the administrative adjudication shall not stay the proceeding unless a court of competent jurisdiction, or the Commission for good cause, so directs.”). Moreover, although Respondents argue that the Supreme Court’s decision would not be final until the 25-day period for a motion for reconsideration has elapsed, they have not indicated that they intend to file such a motion—nor indeed provided any grounds for the Court’s reconsideration of its unanimous decision. In light of these circumstances, we are unwilling to delay resolution of this matter any further.

Accordingly,

IT IS ORDERED THAT Complaint Counsel’s Motion to Lift Stay be, and it hereby is, **GRANTED**; and

IT IS FURTHER ORDERED THAT the Chief Administrative Law Judge is hereby directed to hold a scheduling conference in this matter promptly to reset the hearing schedule and set a new hearing date, with the new hearing date to be as

Interlocutory Orders, Etc.

soon as is practicable, but in no circumstance later than July 15, 2013.

By the Commission.

AEA INVESTORS 2006 FUND L.P.,
HHI HOLDING CORPORATION,
AND
HOUGHTON INTERNATIONAL, INC.

Docket No. C-4297. Order, April 30, 2013

Order reopening and setting aside the consent order with respect to AEA Investors 2006 Fund L.P. (“AEA”), in light of the fact that AEA sold its interest in the assets that raised the competitive concerns addressed by the consent order.

ORDER REOPENING AND MODIFYING FINAL ORDER

AEA Investors 2006 Fund L.P. (“AEA”) filed its Petition of Respondent AEA Investors 2006 Fund L.P. to Reopen and Modify Decision and Order (“Petition”) in this matter on January 3, 2013. AEA was named as a respondent in the consent order issued by the Commission in *AEA Investors 2006 Fund L.P., et al.*, Docket No. C-4297 (“Order”) because at the time it was the ultimate parent entity of HHI Holding Corporation and Houghton International, Inc. AEA has now sold its interest in HHI Holding Corporation and Houghton International, Inc. to Gulf Oil Corporation, and is requesting that the Commission reopen and modify the Order to set it aside as it applies to AEA. HHI and Houghton remain respondents to the Order, and Gulf has become a successor to AEA’s obligations under the Order. AEA bases its request to reopen and modify the Order on both changed facts and public interest grounds. For the reasons stated below, the Commission has determined to grant the Petition to reopen and modify the Order as requested.

Interlocutory Orders, Etc.

I. BACKGROUND

Houghton International, Inc. acquired D.A. Stuart Corporation on July 3, 2008, from Wilh. Werhahn KG. Houghton, at the time, was a wholly-owned subsidiary of HHI Holding Corporation, which itself was a subsidiary of AEA Investors 2006 Fund L.P., an investment fund managed by AEA Investors L.P., a private equity investment firm.

At the time of the acquisition, both Houghton and D.A. Stuart produced aluminum hot rolling oil for sale in North America. To resolve the competitive concerns resulting from the acquisition, the Commission ordered Houghton to divest the United States aluminum hot rolling assets that Houghton had acquired from D.A. Stuart to Quaker Chemical Corporation.¹ Because AEA and HHI owned and controlled Houghton at the time, they were also named as respondents in the Commission's complaint and Order. The Commission issued the Order on August 26, 2010, and it terminates on August 26, 2020.

In addition to requiring the divestiture and related provisions, the Order requires the respondents to comply with certain obligations until the Order terminates. These include maintaining the confidentiality of certain sensitive business information and refraining from reverse engineering certain components of the divested products,² as well as submitting annual reports and notification of corporate changes.³ Houghton completed the required divestiture to Quaker on July 16, 2010, and all respondents have complied with the requirements of the Order.

II. AEA'S PETITION

AEA states that, on November 6, 2012, HHI, Houghton's direct parent, entered into a purchase agreement whereby GHG

¹ Order, ¶¶ II.

² Order, ¶¶ IV.

³ Order, ¶¶ VIII., IX., and X.

Interlocutory Orders, Etc.

Lubricants Holdings Limited, a subsidiary of Gulf Oil Corporation Limited, acquired HHI and Houghton. The parties also complied with the premerger notification requirements of the Hart-Scott-Rodino Act with respect to the proposed acquisition, and were granted early termination of the waiting period on November 29, 2012.⁴ The sale to Gulf closed on December 20, 2012, at which time AEA divested its entire interest in Houghton and HHI and “no longer has any interest in any business relating to [aluminum hot rolling oil].”⁵

AEA contends that reopening and modification is warranted in light of the sale of its interest in Houghton and HHI to Gulf, which, according to AEA, “is a material and significant changed condition of fact.”⁶ The Order was issued to remedy the anticompetitive effects in the aluminum hot rolling oil market that resulted from the combination of Houghton and D.A. Stuart. AEA was included as a respondent because it was, at the time, the ultimate parent entity of Houghton and HHI. After the sale to Gulf, Houghton and HHI continue to be bound by the terms of the Order, and Gulf is bound as a successor to AEA. AEA has no remaining interest in Houghton, HHI, or any aluminum hot rolling oil assets. It will thus have no “ability to ensure compliance with the Order by HHI or Houghton, which are directly responsible for the operations of the [aluminum hot rolling oil] business.”⁷

III. STANDARD FOR REOPENING AND MODIFYING A FINAL ORDER

A final order may be reopened and modified on the grounds set forth in Section 5(b) of the Federal Trade Commission Act.⁸ Section 5(b) provides that the Commission shall reopen an order

⁴ Petition at 3.

⁵ *Id.*

⁶ Petition at 4.

⁷ Petition at 5. AEA also contends that modification is warranted on public interest grounds. *Id.* at 5-6.

⁸ 15 U.S.C. § 45(b).

Interlocutory Orders, Etc.

to consider whether it should be modified if the respondent “makes a satisfactory showing that changed conditions of law or fact” so require.⁹ A satisfactory showing sufficient to require reopening is made when a request to reopen identifies significant changes in circumstances and shows that the changes eliminate the need for the order or make continued application of it inequitable or harmful to competition.¹⁰ Section 5(b) also provides that the Commission may reopen and modify an order when, although changed circumstances would not require reopening, the Commission determines that the public interest so requires. Respondents are therefore invited in petitions to reopen to show how the public interest warrants the requested modification.¹¹

In all instances, whether the request is based on changed conditions or on public interest grounds, respondents’ showing must be supported by evidence that is credible and reliable.¹²

⁹ See also *Supplementary Information*, Amendment to the Commission’s Rules of Practice § 2.51(b), 16 C.F.R. 2.51(b) (August 15, 2001).

¹⁰ S. Rep. No. 96-500, 96th Cong., 2d Sess. 9 (1979) (significant changes or changes causing unfair disadvantage); *Louisiana-Pacific Corp.*, Docket No. C-2956, Letter to John C. Hart (June 5, 1986), at 4 (unpublished) (“Hart Letter”). See also *United States v. Louisiana-Pacific Corp.*, 967 F.2d 1372, 1376-77 (9th Cir. 1992) (“A decision to reopen does not necessarily entail a decision to modify the Order. Reopening may occur even where the petition itself does not plead facts requiring modification.”).

¹¹ Hart Letter at 5; 16 C.F.R. § 2.51.

¹² In the case of a public interest request, Rule 2.51(b) requires an initial satisfactory showing of how modification would serve the public interest before the Commission determines whether to reopen an order and consider all of the reasons for and against its modification. 16 C.F.R. § 2.51(b). A “satisfactory showing” requires that the requester make a *prima facie* showing of a legitimate public interest reason or reasons justifying relief, and this requirement will not be satisfied if the request is merely conclusory or otherwise fails to set forth by affidavit(s) specific facts demonstrating in detail the reasons why the public interest would be served by the modification. *Id.* A sufficient showing requires the requester to demonstrate, *e.g.*, that there is a more effective or efficient way of achieving the purposes of the order, that the order in whole or part is no longer needed, or that there is some other clear public interest that would be served if the Commission were to grant the requested relief.

Interlocutory Orders, Etc.

Commission Rule 2.51(b) requires a “satisfactory showing” to include affidavits setting forth admissible facts, and that all information and material that the requester wishes the Commission to consider must be contained in the request at the time of filing.¹³

If, after determining that the requester has made the required showing, the Commission decides to reopen the order, the Commission will then consider and balance all of the reasons for and against modification. In no instance does a decision to reopen an order oblige the Commission to modify it,¹⁴ and the burden remains on the requester in all cases to demonstrate why the order should be reopened and modified. The petitioner's burden is not a light one in view of the public interest in repose and the finality of the Commission's orders.¹⁵

IV. THE ORDER WILL BE REOPENED AND MODIFIED

We agree that changed circumstances warrant reopening and setting aside the Order as to AEA. At the time the Commission issued the Order, AEA was made a party to the complaint and Order because it was the ultimate parent entity of Houghton and HHI and, thus, necessary to assure the compliance of its subsidiaries. AEA no longer has any relationship with Houghton or HHI and can thus exert no influence over them. Houghton and HHI remain respondents to the Order, and Gulf succeeds to AEA's obligations under the Order and will be in a position to assure compliance of its newly-acquired subsidiaries. There is thus no longer any need to require AEA's compliance with the Order.

¹³ 16 C.F.R. § 2.51(b).

¹⁴ See *United States v. Louisiana-Pacific Corp.*, 967 F.2d 1372, 1376-77 (9th Cir. 1992) (reopening and modification are independent determinations).

¹⁵ See *Federated Department Stores, Inc. v. Moitie*, 425 U.S. 394 (1981) (strong public interest considerations support repose and finality).

Interlocutory Orders, Etc.

Accordingly,

IT IS ORDERED that the Order in Docket No. C-4297 be, and it hereby is, reopened; and

IT IS FURTHER ORDERED that the Order be, and it hereby is, modified by setting aside the Order as to AEA Investors 2006 Fund L.P. as of the date of issuance of this order.

By the Commission.

UNIVERSAL HEALTH SERVICES, INC., ET AL.

Docket No. C-4372. Order, May 14, 2013

Letter approving divestiture by Universal Health Services, Inc. of the Peak Behavioral Health Assets to Strategic Behavioral Health, LLC.

LETTER APPROVING APPLICATION FOR DIVESTITURE

Dear Ms. Varney and Ms. Viswanatha:

This letter responds to the Application for Approval of Divestiture of the Peak Behavioral Health Assets (“Application”) filed by Universal Health Services, Inc. (“Universal”), on March 14, 2013. The Application requests that the Federal Trade Commission approve, pursuant to the order in this matter, Universal’s proposed divestiture of the Peak Behavioral Health Assets to Strategic Behavioral Health, LLC. The Application was placed on the public record for comments until April 29, 2013, and one comment was received.

After consideration of the proposed divestiture as set forth in Universal’s Application and supplemental documents, as well as other available information, the Commission has determined to approve the proposed divestiture. In according its approval, the

Interlocutory Orders, Etc.

Commission has relied upon the information submitted and representations made in connection with Universal's Application and has assumed them to be accurate and complete.

By direction of the Commission, Commissioner Wright not participating.

RESPONSES TO PETITIONS TO QUASH OR LIMIT COMPULSORY PROCESS

UNNAMED TELEMARKETERS

FTC File No. 012 3145. Order, March 4, 2013.

ORDER DENYING PETITION TO QUASH DECEMBER 12, 2012, CIVIL
INVESTIGATIVE DEMAND ISSUED TO THE WESTERN UNION
COMPANY AND NOVEMBER 5, 2012 CIVIL INVESTIGATIVE DEMAND
ISSUED TO LONNIE KEENE, MONITOR, STATE OF ARIZONA V.
WESTERN UNION FINANCIAL SERVICES, INC.

By OHLHAUSEN, Commissioner.

Western Union Company (“Western Union”) has filed a petition to quash civil investigative demands (“CIDs”) issued by the Federal Trade Commission (“FTC” or “Commission”) to Western Union and to Mr. Lonnie Keene, an independent monitor appointed pursuant to Western Union’s settlement of money laundering charges by the State of Arizona. *See Arizona v. Western Union Financial Services, Inc.*, No. CV 2010-5807 (Ariz. Super. Ct. Maricopa Cnty. Feb. 24, 2010). For the reasons stated below, the petition is denied.

I. BACKGROUND

Over the past several years, money transfers have become the payment method of choice for those seeking to defraud consumers in the U.S. and abroad. There are several reasons for this development. First and foremost, a money transfer through companies like Western Union or MoneyGram is essentially the same as sending cash. Thus, consumers have no chargeback rights, as they would have if they had paid by credit card. A money transfer also enables the perpetrators of a scheme to get consumers’ funds quickly. Indeed, a money transfer can be picked up by the recipient within a matter of minutes at multiple locations virtually anywhere in the world, rather than a single designated location. In many instances, the recipient is not even required to provide identification. All of these factors make it extremely difficult for the FTC and other enforcement agencies to

Responses to Petitions to Quash

identify and take action against perpetrators of frauds that employ money transfers.

The FTC continues to receive a high volume of complaints about fraudulent and deceptive practices that rely on money transfers as the method of payment. In 2012 alone, the FTC's database of consumer complaints ("Consumer Sentinel") received more than 102,000 complaints from consumers who lost money through a fraud-induced money transfer, with reported losses exceeding \$450 million. In the same year, money transfers were by far the most common payment method for consumers complaining of fraudulent or deceptive practices, accounting for 47% of all Consumer Sentinel complaints that reported a method of payment.¹ In many of these schemes perpetrators outside the U.S. target U.S. consumers.

Money transfer companies can play an important role in addressing the use of money transmission services to facilitate fraud. They can often identify suspicious outlets, locations, or agents, and can detect patterns of transactions consistent with ongoing fraudulent and deceptive practices. Through diligent and effective antifraud policies and procedures, these companies can address and deter those activities. For example, as required by the consent order in *FTC v. MoneyGram Int'l, Inc.*, No. 09-cv-6576 (N.D. Ill. Oct. 19, 2009), MoneyGram must establish, implement, and maintain a comprehensive antifraud program that "is reasonably designed to protect Consumers by detecting and preventing Fraud-Induced Money Transfers *worldwide* and to avoid installing and doing business with MoneyGram agents *worldwide* who appear to be involved in or complicit in processing Fraud-Induced Money Transfers."²

Following the consent order with MoneyGram, FTC staff asked Western Union to provide, on a voluntary basis, information about steps the company was taking to reduce fraud-

¹ See FTC, Consumer Sentinel Network Data Book for January B December 2012, at 8 (Feb. 2013), *available at* <http://ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2012.pdf>.

² Stipulated Order for Permanent Injunction and Final Judgment at 7-8, *FTC v. MoneyGram Int'l, Inc.*, No. 09-cv-6576 (N.D. Ill. Oct. 19, 2009) (emphasis added).

Responses to Petitions to Quash

induced money transfers. In June 2012, FTC staff requested that Western Union voluntarily provide the FTC with reports produced by a monitor appointed pursuant to an agreement with the State of Arizona that settled charges that Western Union's money transfer business was being used to facilitate human smuggling or narcotics trafficking.

After Western Union refused to provide the reports voluntarily,³ the Arizona Attorney General sought an order clarifying that the terms of the settlement were broad enough to allow Arizona to share the Monitor's reports with the FTC.⁴ The reports had been filed under seal (and therefore kept off the public record) pursuant to a provision in the Settlement Agreement allowing – but not requiring – either Western Union or the Arizona Attorney General to request that the reports be filed under seal.⁵

The state court denied the Arizona Attorney General's request, without prejudice, on September 25, 2012. The ruling was premised on the court's view that “for the Court to order disclosure to [the FTC and Department of Homeland Security] pursuant to the agreement, I would want them in the courtroom to know what the scope of the agreement is, that it is going to be a two-way street. It would benefit the monitor in doing the monitor's job.”⁶ The court made clear that it was making no comment on “the extent that the FTC or Homeland Security has a

³ Western Union did provide other information about its antifraud program and contributed complaints from U.S.-based consumers to the Commission's online complaints database. Starting in August 2012, FTC staff also requested foreign complaints, but Western Union declined based on privacy concerns.

⁴ Pet. Ex. E. The Arizona Attorney General pointed out that such a release is consistent with the Monitor Engagement Letter (“MEL”) (see Pet. Ex. E, at 5-6; see also Pet. Ex. B ¶ 9) and is specifically authorized by Paragraph 17.1.4 of the Settlement Agreement (providing that the state has leave to disclose any materials or information provided by Western Union where such disclosure “is required by law, otherwise authorized by this Agreement, or is in the proper discharge of or otherwise furthers the State's official duties or responsibilities.”).

⁵ Pet. Ex. D, at 4.

⁶ Pet. Ex. F, at 21-22.

Responses to Petitions to Quash

right to secure information that the monitor has or the Attorney General's Office has.”⁷

The Commission then issued CIDs to obtain the reports and related materials, first to the Monitor and then to Western Union directly. Specifically, on November 5, 2012, the Commission issued a CID to the Monitor, seeking

All documents referring or relating to the Periodic Reviews of the Monitor appointed by the court in *State of Arizona ex rel. Horne v. Western Union Financial Services, Inc.*, No. CV 2010-005807, including, but not limited to, all drafts of any reports, reviews, or correspondence with Western Union.

The Commission directed a separate CID to Western Union on December 12, 2012. In addition to the Monitor's reports, the CID requires Western Union to produce (1) internal documents that refer or relate to communications with the Monitor B *i.e.*, documents showing Western Union's internal reaction to the findings and recommendations in the Monitor's reports; and (2) complaints from consumers worldwide referring or relating to fraud-induced transactions. As defined, such complaints include complaints made by foreign consumers about transactions that were picked up either in the U.S. or in a foreign jurisdiction.

After receiving the CID, the Monitor sought to confirm his authority to provide the requested materials to the FTC by filing a motion in the settled Arizona action. On January 28, 2013, [redacted].⁸ [redacted].⁹ [redacted].¹⁰

On January 31, 2013, Western Union filed the instant petition to quash.¹¹

⁷ Pet. Ex. F, at 21.

⁸ Pet. Ex. G, at 4.

⁹ Pet. Ex. G, at 2-3.

¹⁰ Pet. Ex. G, at 3-4.

¹¹ It is by no means certain that Western Union has standing to seek to quash the CID issued to the Monitor. Generally, the target of a government investigation lacks standing to dispute the validity of administrative subpoenas

Responses to Petitions to Quash

II. ANALYSIS**A. The Applicable Legal Standards.**

Compulsory process such as a CID is proper if the inquiry is within the authority of the agency, the demand is not too indefinite and the information sought is reasonably relevant to the inquiry, as defined by the Commission's investigatory resolution.¹² Agencies have wide latitude to determine what information is relevant to their law enforcement investigations and are not required to have "a justifiable belief that wrongdoing has actually occurred."¹³

Western Union argues that the CIDs should be quashed because they do not satisfy these standards. First, Western Union claims that the CIDs were not issued pursuant to a valid resolution. Second, Western Union claims that the requested materials are not relevant to the purpose of the investigation. Third, it claims that the FTC lacks authority to compel the production of materials prepared pursuant to, or as a consequence

directed to a third party. See, e.g., *Greene v. Phila. Hous. Auth.*, 789 F. Supp. 2d 582, 586 (E.D. Pa. 2011); see also *FTC v. Trudeau*, 2012 U.S. Dist. LEXIS 160545, at *8 (N.D. Ohio Nov. 8, 2012). Western Union contends that its privacy interests are sufficient to confer standing. Pet. 7 n.3. We note, however, that Western Union's claimed privacy interests are inconsistent with the terms of the MEL. See Pet. Ex. B ¶ 5 ("The Monitor shall be independent of Western Union and the State, and no attorney-client relationship shall be formed between them."). Thus, the decision of the Sixth Circuit in *American Motors Corp. v. FTC*, 601 F.2d 1329, 1338-39 (6th Cir. 1979), cited by petitioner, is questionable authority for Western Union's assertion that it has retained "privacy rights." Pet. 7 n.3. In any event, even if Western Union has an interest that is sufficient to confer standing, its petition to quash the Monitor's CID is without merit for the reasons discussed herein.

¹² *United States v. Morton Salt Co.*, 338 U.S. 632, 652 (1950); *FTC v. Invention Submission Corp.*, 965 F.2d 1086, 1089 (D.C. Cir. 1992); *FTC v. Texaco, Inc.*, 555 F.2d 862, 874 (D.C. Cir. 1977).

¹³ See, e.g., *Morton Salt*, 338 U.S. at 642-43 (A[Administrative agencies have] a power of inquisition, if one chooses to call it that, which is not derived from the judicial function. It is more analogous to the Grand Jury, which does not depend on a case or controversy for power to get evidence but can investigate merely on suspicion that the law is being violated, or even just because it wants an assurance that it is not.").

Responses to Petitions to Quash

of, a state court settlement. Fourth, Western Union contends that the Commission exceeded its authority in seeking complaints and information related to money transfers between foreign countries. As explained below, we are not persuaded that these contentions have merit.

B. The CIDs Are Supported by a Specific and Valid Resolution.

Western Union's contention that the resolution would permit the FTC to investigate any party "engaged in sales with respect to any form of practice or conduct" is not borne out by the text of the resolution. In issuing the CIDs, the Commission relied on omnibus resolution No. 0123145, *Resolution Directing Use of Compulsory Process in a Nonpublic Investigation of Telemarketers, Sellers, Suppliers, or Others* (Apr. 11, 2011). The resolution authorizes the use of compulsory process to determine whether telemarketers, sellers, or others assisting them have or are violating Section 5 of the FTC Act, 15 U.S.C. § 45, or the Telemarketing Sales Rule, 16 C.F.R. Part 310.¹⁴ The resolution also provides specific notice that it pertains to investigations relating to telemarketing activities, and includes investigations of telemarketers or sellers as well as entities such as Western Union

¹⁴ The resolution describes the nature and scope of the investigation as follows:

To determine whether unnamed telemarketers, sellers, or others assisting them have engaged in or are engaging in: (1) unfair or deceptive acts or practices in or affecting commerce in violation of Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 (as amended); and/or (2) deceptive or abusive telemarketing acts or practices in violation of the Commission's Telemarketing Sales Rule, 16 C.F.R. pt 310 (as amended), including but not limited to the provision of substantial assistance or support B such as mailing lists, scripts, merchant accounts, and other information, products, or services B to telemarketers engaged in unlawful practices. The investigation is also to determine whether Commission action to obtain redress for injury to consumers or others would be in the public interest.

Resolution Directing Use of Compulsory Process in a Nonpublic Investigation of Telemarketers, Sellers, Suppliers, or Others, File No. 0123145 (Apr. 11, 2011).

Responses to Petitions to Quash

who may be providing substantial assistance or support to telemarketers or sellers.

This statement of the purpose and scope of the investigation is more than sufficient under applicable standards, and courts have enforced compulsory process issued under similar resolutions.¹⁵ Indeed, this resolution has been in effect for many years and has supported multiple other investigations, including CIDs issued to Western Union's competitor, MoneyGram, in 2007 and 2008.

Western Union's reliance on the decision of the D.C. Circuit in *FTC v. Carter*, 636 F.2d 781, 788 (D.C. Cir. 1980), is misplaced. Although *Carter* held that a bare reference to Section 5 of the FTC Act, without more, "would not serve very specific notice of purpose," the Court approved the resolution at issue, noting that it also referred to specific statutory provisions of the Cigarette Labeling and Advertising Act, and further related it to the subject matter of the investigation.¹⁶ With this additional information, the Court felt "comfortably apprised of the purposes of the investigation and the subpoenas issued in its pursuit."¹⁷ Similarly, the resolution here provides substantially more information than the bare text of Section 5, and thus adequately notifies Western Union of the nature and scope of the investigation.

¹⁵ See Opinion and Order at 11-12, *FTC v. LabMD, Inc.*, No. 1:12-cv-3005-WSD (N.D. Ga. Nov. 26, 2012); *FTC v. Nat'l Claims Serv., Inc.*, 1999 WL 819640, at *2 (E.D. Cal. Feb. 9, 1999) (approving use of omnibus resolution citing provisions of the FTC Act and the Commission's Franchise Rule); *FTC v. O'Connell Assocs., Inc.*, 828 F. Supp. 165, 171 (E.D.N.Y. 1993) (enforcing CIDs issued pursuant to omnibus resolution citing provisions of the FTC Act and the Fair Credit Reporting Act). The Commission has repeatedly rejected similar arguments about such omnibus resolutions. See, e.g., *LabMD, Inc.*, No. 123099, at 9 (Apr. 20, 2012); *Firefighters Charitable Found.*, No. 102-3023, at 4 (Sept. 23, 2010); *D.R. Horton, Inc.*, Nos. 102-3050, 102-3051, at 4 (July 12, 2010); *CVS Caremark Corp.*, No. 072-3119, at 4 (Dec. 3, 2008).

¹⁶ *Carter*, 636 F.2d at 788.

¹⁷ *Id.* Western Union also contends that the resolution fails to conform to the FTC's Operating Manual. Pet. 9. But for the reasons stated above, the resolution at issue is sufficiently specific to comply with the Operating Manual. FTC Operating Manual, Ch. 3.3.6.7.4.1. In any event, the manual itself confers no rights on Western Union. *Id.*, Ch. 1.1.1; see also *FTC v. Nat'l Bus. Consultants, Inc.*, 1990 U.S. Dist. LEXIS 3105, 1990-1 Trade Cas. (CCH) & 68,984, at *29 (E.D. La. Mar. 19, 1990).

Responses to Petitions to Quash

Western Union's argument also fails in light of the history of communications between the company and the FTC. The purpose of an authorizing resolution is to notify a CID recipient of the nature and scope of the investigation.¹⁸ Given the lengthy dialogue between staff and Western Union, there is no doubt that the company is aware of the nature of staff's investigation. The Commission has previously found that such interactions may be considered along with the resolution in evaluating the notice provided to Petitioners: "[T]he notice provided in the compulsory process resolutions, CIDs, and other communications with Petitioner more than meets the Commission's obligation of providing notice of the conduct and the potential statutory violations under investigation."¹⁹

C. The Documents Sought Are Relevant to the Commission's Investigation.

Western Union claims that the CID specification calling for the Monitor's reports and related documents is irrelevant to the FTC's investigation into consumer fraud and telemarketing. Specifically, Western Union claims that the Monitor's reports relate to human and drug trafficking in the Southwest border area and that these issues are far outside the stated purposes of the FTC's investigation.²⁰

In the context of an administrative CID, "relevance" is defined broadly and with deference to an administrative agency's determination.²¹ An administrative agency is to be accorded "extreme breadth" in conducting an investigation.²² As the D.C. Circuit has stated, the standard for judging relevance in an administrative investigation is "more relaxed" than in an

¹⁸ *O'Connell Assocs., Inc.*, 828 F. Supp. at 170-71.

¹⁹ *Assoc. First Capital Corp.*, 127 F.T.C. 910, 915 (1999).

²⁰ Pet. 13-14.

²¹ *FTC v. Church & Dwight Co., Inc.*, 665 F.3d 1312, 1315-16 (D.C. Cir. 2011); *FTC v. Ken Roberts Co.*, 276 F.3d 583, 586 (D.C. Cir. 2001).

²² *Linde Thomsen Langworthy Kohn & Van Dyke, P.C. v. RTC*, 5 F.3d 1508, 1517 (D.C. Cir. 1993).

Responses to Petitions to Quash

adjudicatory proceeding.²³ As a result, the agency is entitled to the documents unless the CID recipient can show that the agency's determination is "obviously wrong" or the documents are "plainly irrelevant" to the investigation's purpose.²⁴ We find that Western Union has not met this burden.

Although Western Union tries to couch the settlement and the Monitor's tasks as relating to human or drug trafficking, a review of the Monitor Engagement Letter shows that it is more general and relates to oversight by the Monitor of Western Union's anti-money laundering ("AML") program as required by the Bank Secrecy Act ("BSA") and related guidance.²⁵ The statutory and regulatory provisions relating to Western Union's money services business ("MSB") authorities do not segregate AML and antifraud programs. Western Union is required by the BSA and its implementing regulations to implement an AML program,²⁶ which includes filing Suspicious Activity Reports ("SARs") for "possible violation[s] of law or regulation."²⁷ Those reports are not limited to money laundering. Instead, the BSA is clear that the SARs required from Western Union's AML program must report *any* type of suspicious transaction, including consumer fraud.²⁸ Indeed, in guidance published to examiners of money

²³ *Invention Submission Corp.*, 965 F.2d at 1090.

²⁴ *Id.* at 1089; *Carter*, 636 F.2d at 788. We note that Western Union has not contested the relevance of the worldwide complaints that are the subject of Specification 1. Its arguments on relevance are limited to the Monitor's reports and related documents sought under Specification 2.

²⁵ "To ensure that its Program adheres to the principles enunciated in the Financial Action Task Force Risk-Based Approach to Combating Money Laundering and Terrorist Financing ('FATF RBA Guidance'), to its legal obligations, to the Agreement, and to this Monitor Engagement Letter, Western Union has agreed to be overseen by an independent Monitor" Pet. Ex. B ¶ 2.

²⁶ 31 U.S.C. §§ 5312(a)(2)(R), 5318(h); 31 C.F.R. § 1022.210(d).

²⁷ 31 U.S.C. § 5318(g); 31 C.F.R. § 1022.320(a).

²⁸ 31 U.S.C. § 5318(g) ("The Secretary may require any financial institution, and any director, officer, employee, or agent of any financial institution, to report any suspicious transaction relevant to a possible violation of law or regulation."); 31 C.F.R. § 1022.320(a) ("Every money services business . . . shall file with the Treasury Department, to the extent and in the manner required by this section, a report of any suspicious transaction relevant to a possible violation of law or regulation.").

Responses to Petitions to Quash

services businesses for compliance with the BSA, the Department of the Treasury made it plain that an AML program must detect and report on transactions that involve more than just money laundering, and that the business itself should not try to distinguish one type of illegal conduct from another for purposes of its reporting requirement:

MSBs are required to report suspicious activities above prescribed dollar thresholds that may involve money laundering, BSA violations, terrorist financing, *and certain other crimes*. However, MSBs cannot be expected and are not required to investigate or confirm the underlying crime (e.g., terrorist financing, money laundering, tax evasion, identity theft, *or fraud*).²⁹

Thus, from a regulatory perspective, there is substantial overlap between an AML program and a program to detect consumer fraud and other illegal activities. Indeed, until the summer of 2012, Western Union's AML and antifraud personnel were housed within the same corporate group, meaning that a common set of personnel were involved in responding to complaints of consumer fraud as well as suspected money laundering activity.

The overlap is further demonstrated by a comparison of the Monitor's obligations for overseeing the AML program, as outlined in the MEL, and Western Union's antifraud program, as described in the overview document that Western Union provided to FTC staff in September 2012.³⁰ For example, the Monitor is required to evaluate whether Western Union's AML program, among other things:

- Provides for adequate oversight and controls of Agents, consumers, transactions, products, services, and

²⁹ Fin. Crimes Enforcement Network & Internal Revenue Serv., Bank Secrecy Act/Anti-Money Laundering Examination Manual for Money Services Businesses 86 (2008) (emphasis added) (footnote omitted), *available at* http://www.fincen.gov/news_room/rp/files/MSB_Exam_Manual.pdf.

³⁰ Letter from John R. Dye, EVP, Gen. Counsel & Sec'y, Western Union, to David Vladeck, Dir., Bureau of Consumer Prot., FTC (Sept. 14, 2012) [hereinafter Anti-Fraud Program].

Responses to Petitions to Quash

geographic areas that are more vulnerable to abuse by money launderers and other criminals;

- Provides for regular review of the risk assessment and risk management processes;
- Contains channels for informing senior management of compliance initiatives, compliance deficiencies, corrective actions, and filing of suspicious activity reports;
- Provides for appropriate initial and refresher training for Agents to be given at appropriate intervals.³¹

None of these tasks is unique to anti-money laundering activities. Indeed, the same tasks are specifically mentioned in Western Union's Anti-Fraud Program overview.³²

Similarly, the Monitor is charged with developing an "Implementation Plan" that includes the Monitor's own recommendations for Western Union and that presumptively includes certain "existing measures" already employed by Western Union as part of its AML program.³³ Many of these existing AML measures are also part of Western Union's antifraud program, as described in the company's own materials:

- One of the "existing measures" for the AML program is "developing the ability to aggregate consumer transactions to identify unusual activity on a real-time basis (through its Real Time Risk Assessment initiative)."³⁴ [redacted].³⁵
- Another "existing measure" is "developing, to the extent reasonably feasible, Real Time Risk Assessment that will provide the ability to block noncompliant transactions

³¹ Pet. Ex. B, at 6-7.

³² See, e.g., Anti-Fraud Program 7 [redacted]; *id.* at 4 [redacted]; *id.* at 5-6 [redacted]; *id.* at 23-24 [redacted].

³³ Pet. Ex. B ¶¶ 18-23. Specifically, paragraph 23 of the MEL, entitled "Presumed Program Measures," provides that Western Union's existing AML measures will become part of the Monitor's recommendations "unless the Monitor, with input from Western Union and the State, determines that it is not technically feasible or would not improve the Program." Pet. Ex. B ¶ 23.

³⁴ Pet. Ex. B ¶ 23.1.2.

³⁵ Anti-Fraud Program 14-16 [redacted].

Responses to Petitions to Quash

before they are processed, so that when a transaction violates established business rules, a ‘pop-up screen’ will immediately notify the Agent that the transaction cannot be completed.”³⁶ [redacted]³⁷

- A third “existing measure” is “implementing Transaction Risk Index (‘TRI’) model variables and formulas . . . to more strategically mitigate the risks associated with certain geographies (e.g., Arizona) and ‘red flags’ such as structuring, sharing of consumer identifying information, high volume, high frequency, and SARs filed by Western Union on transactions facilitated by/through the Agent.”³⁸ [redacted].³⁹

We conclude, therefore, that the steps Western Union must take to eliminate various forms of any suspected illegal transactions from its system are essentially the same. Both the AML and antifraud programs are intended to prevent illegal transactions occurring through the company’s money transfer system, and both programs employ similar tools to do so: analysis of transaction data to identify patterns, computer-based rules that prevent illegal transactions from entering the system, training to help agents identify illegal transactions, and disciplinary action against agents that are complicit in the illegal activity or continue to generate high levels of complaints.⁴⁰ To the extent the Monitor’s reports include an assessment of, and recommendations for, each of these facets of Western Union’s AML program, they

³⁶ Pet. Ex. B ¶ 23.1.8.

³⁷ Anti-Fraud Program 4.

³⁸ Pet. Ex. B ¶ 23.1.5.

³⁹ Anti-Fraud Program 3.

⁴⁰ To provide another example of the overlap between Western Union’s AML and antifraud programs: one of the key issues identified in the Arizona action was Western Union’s awareness of, and failure to terminate, complicit U.S. and foreign agents who “were knowingly engaged in a pattern of money laundering violations.” See Settlement Agreement Ex. A (“Statement of Admitted Facts”), *Arizona v. W. Union Fin. Servs., Inc.*, No. CV 2010-5807 (Ariz. Super. Ct. Maricopa Cnty. Feb. 24, 2010), available at <https://www.azag.gov/sites/default/files/sites/all/docs/swbamla/State%20of%20Arizona%20v.%20Western%20Union%20Settlement%20Agreement%20compact.pdf>. [redacted]. Anti-Fraud Program 4.

Responses to Petitions to Quash

are highly relevant to the current inquiry into the adequacy of the company's antifraud program.⁴¹

It is also important to note that the CID directed to Western Union is not limited to the Monitor's reports. Rather, the CID requests "[a]ll documents referring or relating to communications with the Monitor."⁴² The CID thus encompasses Western Union's internal communications and reactions to the findings and recommendations of the Monitor, which are relevant to determining the strength of the company's culture of compliance and whether there is a widespread commitment to eliminating illegal transactions from Western Union's system. These documents, which have not been shared with the Monitor or with the Arizona Attorney General, are not covered by any confidentiality provisions in the settlement documents and thus must be produced in response to the CID directed at Western Union.

In short, the Monitor's reports and related materials are relevant to assessing Western Union's commitment to eliminating illegal transactions from its system, and thus are "reasonably relevant" to the purposes of the Commission's investigation. Western Union has not satisfied its burden to demonstrate that the information requested by the CID is "plainly irrelevant" or "obviously wrong."⁴³

⁴¹ The Monitor's reports are also uniquely valuable because they provide the perspective of an independent third party who owes no duties to Western Union. Indeed, to ensure the Monitor's independence, the MEL specifies that neither Western Union nor the State of Arizona shall provide any personal benefit to the Monitor during the term of the Monitor's engagement or for five years afterward. Pet. Ex. B ¶ 4.

⁴² Pet. Ex. A, at 7-8.

⁴³ *Invention Submission Corp.*, 965 F.2d at 1089; *Carter*, 636 F.2d at 788.

Responses to Petitions to Quash

D. The CIDs Are Valid Exercises of the Commission's Authority.

1. The FTC Has Authority to Obtain the Monitor's Reports and Related Documents.

Western Union next argues that the Commission may not use its process to obtain access to documents that are subject to confidentiality restrictions imposed by an Arizona state court. [redacted].⁴⁴ We are not persuaded.

First, the confidentiality provisions of the Arizona settlement documents do not by their terms limit the Commission's ability to use investigatory process to obtain the Monitor's reports and related information. The settlement documents do not address the question of whether the reports and related documents must be released in response to compulsory process of a federal agency. On the contrary, the Settlement Agreement specifically states that it "does not bind any federal agencies or any other state's authorities."⁴⁵ Indeed, the settlement documents state that the Monitor's reports and the underlying information may be shared in certain circumstances — including with investigative agencies or in furtherance of the Attorney General's duties.⁴⁶

Second, Western Union errs in contending that CIDs represent an improper attempt to circumvent an order of a state court. The

⁴⁴ Pet. 15-16.

⁴⁵ Pet. Ex. C ¶ 28.

⁴⁶ For example, the Monitor is required to "take appropriate steps to maintain the confidentiality of any information entrusted to him or her" and to "share such information only with the State, *appropriate investigative agencies*, and individuals or entities hired by him or her." Pet. Ex. B ¶ 36 (emphasis added). For its part, the office of the Arizona Attorney General must "maintain the confidentiality of any materials or information provided by Western Union under this paragraph and shall not provide such material or information to any third party, except to the extent that disclosure is required by law, otherwise authorized by this Agreement, or *is in the proper discharge of or otherwise furthers the State's official duties and responsibilities*." *Id.*, Ex. C ¶ 17.1.4 (emphasis added). With respect to the reports themselves, the Arizona Attorney General is required to maintain their confidentiality "*except to the extent that disclosure may be necessary by the State in connection with the discharge of its official duties*." *Id.*, Ex. B ¶ 37 (emphasis added).

Responses to Petitions to Quash

September 2012 ruling dealt solely with the Arizona Attorney General's request to share copies of the reports that had been provided to him.⁴⁷ [redacted].⁴⁸ Neither the ruling [redacted] purports to address the copies of the Monitor's reports that reside in Western Union's own files, or the other materials sought in Specification 2 of the CID addressed to Western Union – which includes materials besides the Monitor's reports, such as “information Western Union provided to the Monitor” and Western Union's internal reactions to the Monitor's reports.⁴⁹ The state court's ruling [redacted], by their own terms, are simply inapplicable to the documents that Western Union seeks to shield from disclosure.

Third, the Arizona state court did not purport to prohibit the Commission from using its process to obtain the reports or related information either from the Monitor or the State of Arizona. On the contrary, [redacted] the court specifically noted that it was not addressing the scope of the Commission's process authority. When ruling on the Arizona Attorney General's request, the state court explained that it was “mak[ing] no comment” on “the extent that the FTC or Homeland Security has a right to secure information that the monitor has or the Attorney General's Office has.”⁵⁰ [redacted].⁵¹

Fourth, even if the Arizona state court had intended to prohibit the FTC from obtaining the Monitor's reports and related materials, confidentiality restrictions under state law must give way if they conflict with federal agencies' statutory power to gather evidence. Agencies of the United States may use their

⁴⁷ Pet. Exs. E, F.

⁴⁸ Pet. Ex. G.

⁴⁹ Although the MEL requires the State of Arizona and Western Union to “maintain the confidentiality of all such information provided to them by the Monitor,” Pet. Ex. B ¶ 37, there is nothing in the settlement documents or the state court's subsequent ruling [redacted] that restricts Western Union from disclosing its own business records – such as its communications to the Monitor and its internal documents discussing the Monitor's reports and recommendations.

⁵⁰ Pet. Ex. F, at 21.

⁵¹ Pet. Ex. G, at 3-4.

Responses to Petitions to Quash

compulsory process to obtain documents whose disclosure would otherwise be barred by state statute.⁵² Put differently, even when a state legislature has specifically acted to prohibit disclosure of certain information, those state statutes are preempted to the extent they frustrate the federal statutory schemes that entitle federal agencies to “have access to relevant evidence.”⁵³ The same considerations apply when a state court purports to restrict the Commission’s ability to use its investigative process. ““To . . . federal statute and policy, conflicting state law and policy must yield. Constitution, Art. VI, cl. 2.””⁵⁴

Fifth, the fact that the requested documents were generated as a result of Western Union’s settlement with the Arizona Attorney General does not change the analysis. Documents created pursuant to settlement or in reliance on confidentiality protections are not automatically shielded from all disclosure. For example, even in the context of purely private rights, the Third Circuit has recognized that parties’ reliance on a confidentiality order is only one of several factors that must be considered when nonparties

⁵² See, e.g., *EEOC v. Ill. Dep’t of Emp’t Sec.*, 995 F.2d 106, 107 (7th Cir. 1993) (enforcing EEOC subpoena for transcript of unemployment compensation hearing, despite state statute making such proceedings confidential); *United States ex rel. Office of Inspector Gen., U.S. Dep’t of Hous. & Urban Dev. v. Phila. Hous. Auth.*, 2011 WL 382765, at *5 (E.D. Pa. Feb. 4, 2011) (enforcing HUD OIG subpoena seeking employees’ partial Social Security Numbers, despite state statutes restricting disclosure of sensitive personal information); *United States v. United Network for Organ Sharing*, 2002 WL 1726536, at *1-*2 (N.D. Ill. May 17, 2002) (enforcing HHS OIG subpoena, despite state statute restricting disclosure of peer review documents); *United States ex rel. Agency for Int’l Dev. v. First Nat’l Bank of Md.*, 866 F. Supp. 884, 887 (D. Md. 1994) (enforcing USAID OIG subpoena, despite state statute restricting disclosure of financial documents); *United States v. N.Y. State Dep’t of Taxation & Fin.*, 807 F. Supp. 237, 240-43 (N.D.N.Y. 1992) (enforcing DOL OIG subpoena, despite state statute restricting disclosure of tax and wage records); *EEOC v. County of Hennepin*, 623 F. Supp. 29, 32 (D. Minn. 1985) (enforcing EEOC subpoena, despite state statute permitting production of government personnel information only in response to a court order).

⁵³ *County of Hennepin*, 623 F. Supp. at 32.

⁵⁴ *Liner v. Jafco, Inc.*, 375 U.S. 301, 309 (1964) (quoting *Sola Elec. Co. v. Jefferson Elec. Co.*, 317 U.S. 173, 176 (1942)).

Responses to Petitions to Quash

seek access to confidential settlement materials.⁵⁵ The threshold to forestall disclosure of documents submitted to facilitate settlement is even higher when a case involves – as it does here – “a government agency and an alleged series of deceptive trade practices culminating (it is said) in widespread consumer losses,” because “[t]hese are patently matters of significant public concern.”⁵⁶

Moreover, Western Union’s cited cases – *United States v. Bleznak*, 153 F.3d 16 (2d Cir. 1998), and *McCoo v. Denny’s Inc.*, 2000 WL 156824 (D. Kan. Feb. 11, 2000) – do not support the proposition that the Commission may not use process to obtain documents that would not exist but for the Arizona settlement agreement. Notably, the persons seeking disclosure in *Bleznak* and *McCoo* were seeking evidence to use in vindicating their purely private rights. By contrast, the Commission is an agency of the United States and seeks materials in connection with its statutory mandate to prevent unfair and deceptive practices in furtherance of the public interest. Furthermore, in both cases, the consent decree at issue specifically barred the requested disclosure.⁵⁷ As noted above, the Arizona settlement documents

⁵⁵ *Pansy v. Borough of Stroudsburg*, 23 F.3d 772, 787-90 (3d Cir. 1994) (noting that parties’ reliance “should not be outcome determinative,” and instructing courts to also consider factors such as privacy interests, the purpose for which the information is being sought, whether the information is important to public health and safety, whether sharing would promote fairness and efficiency, and whether the case involves issues important to the public); see also *Daines v. Harrison*, 838 F. Supp. 1406, 1408-09 (D. Colo. 1993) (finding that parties’ reliance on confidentiality order was “not enough to tip the balance in their favor” in light of competing interests favoring disclosure, such as the public right of access to court records and the involvement of public agencies and public funds); cf. *Palmieri v. New York*, 779 F.2d 861, 864-66 (2d Cir. 1985) (recognizing that orders sealing court records and a settlement agreement could be modified if warranted by “extraordinary circumstances” or “compelling need”).

⁵⁶ *FTC v. Standard Fin. Mgmt. Corp.*, 830 F.2d 404, 412 (1st Cir. 1987).

⁵⁷ The intervenors in *Bleznak*, who were parties in a separate private action against the defendants, sought to circumvent specific language in the consent decree that the tapes created pursuant to the settlement would not be “subject to civil process” or “admissible in evidence in civil proceedings.” 153 F.3d at 19. Similarly, the *McCoo* plaintiffs were using discovery to seek the materials at issue, an act specifically prohibited by the consent decree provisions barring the Monitor and the parties from disclosing “Confidential Information to any

Responses to Petitions to Quash

specifically contemplate that the Monitor's reports and the underlying information may be shared in certain circumstances, including with investigative agencies or in furtherance of the Attorney General's duties. Thus, the provisions considered in *Bleznak* and *McCoo* are not comparable to the confidentiality provisions at issue here.

Finally, Western Union suggests that the "appropriate procedure" would be for the Commission to appear before the Arizona state court or seek to intervene.⁵⁸ However, the Commission is an agency of the United States not subject to the jurisdiction of state courts. A state may not interfere with a valid exercise of federal authority.⁵⁹ Thus, there is no basis for the contention that the Commission must appear before a state tribunal or seek to intervene in a state proceeding to use its statutory process authority to obtain the requested documents – [redacted].⁶⁰

2. The FTC May Obtain Western Union's Worldwide Complaints.

Specification 1 of the CID requires Western Union to produce "[a]ll documents referring or relating to complaints made to Western Union by consumers anywhere in the world, referring or relating to fraud-induced money transfers."⁶¹ Under the governing law, this specification must be enforced if the inquiry is within the authority of the agency, the demand is not too indefinite, and the information sought is reasonably relevant to the purpose of the inquiry, as set forth in the Commission's investigatory resolution.

person who is not a party to this Decree, including without limitation any person who seeks such Confidential Information in other litigation through discovery process in other courts." 2000 WL 156824, at *2.

⁵⁸ Pet. 16.

⁵⁹ See *Goodyear Atomic Corp. v. Miller*, 486 U.S. 174, 180 n.1 (1988) (Supremacy Clause "immunizes the activities of the Federal Government from state interference"); *Mayo v. United States*, 319 U.S. 441, 445 (1943) ("[T]he activities of the Federal Government are free from regulation by any state.").

⁶⁰ Pet. Ex. G, at 3.

⁶¹ Pet. Ex. A, at 7 (Specification III.1).

Responses to Petitions to Quash

Western Union does not claim that the specification is too indefinite or not reasonably relevant. It contends, however, that the Commission has exceeded its authority in requesting information about transactions that occurred outside the U.S. and further, that the request cannot be reconciled with foreign data privacy laws. We are not persuaded by either of these claims.

The FTC is authorized to obtain through compulsory process Western Union's worldwide complaints about fraud-induced money transfers. In 2006, Congress passed the U.S. SAFE WEB Act, which enhanced the FTC's ability to protect U.S. consumers from perpetrators of fraud operating abroad and to prevent the U.S. from becoming a haven for fraudulent activity targeting foreign victims by amending Section 5's core provisions to confirm the agency's cross-border jurisdictional authority. The SAFE WEB amendments provide that the term "unfair or deceptive acts or practices" in Section 5(a) of the FTC Act "includes such acts or practices involving foreign commerce" that either: "(i) cause or are likely to cause reasonably foreseeable injury within the United States; or (ii) involve material conduct occurring within the United States." 15 U.S.C. § 45(a)(4)(A).

Indeed, the Senate Report on the U.S. SAFE WEB Act cited by Western Union makes it clear that Congress intended to empower the FTC to combat cross-border fraud by obtaining and sharing information from foreign jurisdictions. The report states that the Act will

authorize the FTC to: (1) share information involving cross-border fraud with foreign consumer protection agencies; (2) secure confidential information from those foreign consumer protection agencies; (3) take fraud-based legal action in foreign jurisdictions; (4) seek redress on behalf of foreign consumers victimized by United States-based wrongdoers; (5) make criminal referrals for cross-border criminal activity; [and] (5) strengthen its relationship with foreign consumer protection agencies.⁶²

⁶² S. Rep. No. 109-219, at 3 (2006).

Responses to Petitions to Quash

For this reason, Western Union's reliance on the Supreme Court's decision in *Morrison v. National Australia Bank Ltd.*, 130 S. Ct. 2869 (2010), is misplaced. In *Morrison*, the Supreme Court held, in the context of a private class action involving foreign buyers and sellers operating on foreign security exchanges, that there was no "affirmative indication" that Section 10(b) of the SEC Act applies extraterritorially. The "presumption against extraterritoriality" affirmed in *Morrison* does not apply to the FTC's CID here, given Congress' express intent in extending the FTC Act to specified acts and practices involving foreign commerce. See 15 U.S.C. § 45(a)(4).

Further, the request in the CID for Western Union's worldwide complaints is proper under both the "material conduct" and "cause or likely to cause reasonably foreseeable injury" tests in Section 45(a)(4).

For one, the FTC's investigation has focused primarily on whether Western Union has adopted and implemented policies and procedures that are sufficient to prevent or limit wrongdoers from using its money transfer system to perpetrate fraud. The "material conduct" at issue is therefore Western Union's actions in developing and administering its antifraud program – activities that Western Union does not dispute occur within the United States.⁶³ Any complaints from foreign consumers related to fraud-induced money transfers in non-U.S. jurisdictions certainly "involve" this "material conduct" and call into question the effectiveness of these policies and procedures to protect U.S. and

⁶³ Western Union asserts that its oversight of its antifraud program cannot be "material conduct" because it is an "act of omission" involving an alleged failure to act. Pet. 11. This argument ignores the affirmative duty imposed by the BSA on Western Union to implement an AML program. See II.C., *supra*. It also ignores the detailed information Western Union already provided the Commission that describes its antifraud program, including program documentation. This information confirms that, far from performing an "act of omission," Western Union affirmatively sets policy and dictates procedures within the U.S. that are designed to detect and curtail fraudulent activities both within and outside the U.S. Western Union also employs procedures developed here to receive complaints, analyze complaint data, and to take remedial action in response to that data. See *generally* Anti-Fraud Program 5-24, 29-33. In further support, we note that the complaints sought by the CID are maintained in the United States.

Responses to Petitions to Quash

non-U.S. consumers alike.⁶⁴ The FTC is entitled to such worldwide complaints to help it assess the levels of fraud perpetrated through Western Union's network, the extent of Western Union's knowledge of the number of any fraud-induced money transfers being picked up at particular agent locations, and the adequacy of Western Union's actions in response to such complaints.⁶⁵

For similar reasons, any failure by Western Union to take effective remedial action against a problematic foreign agent would necessarily cause or be likely to cause reasonably foreseeable injury to consumers within the U.S. As explained above, if Western Union, through complaints it receives from U.S. and foreign victims, or even from foreign victims alone, is able to identify a problem agent abroad, then it may need to take immediate action to suspend or terminate that agent from its system to prevent additional consumers from being victimized. Any future victims may include both U.S. and foreign consumers, because a problem agent in a foreign jurisdiction that is receiving fraud-induced transactions from foreign victims may also likely be receiving fraud-induced transactions from U.S. victims.

Western Union's assertions on this issue fail to account for the worldwide nature of the networks that may be perpetrating fraud through its system. As we have learned, funds transferred by a

⁶⁴ We note that Western Union does not address the fact that documents responsive to Specification 1 include any complaints by non-U.S. consumers about fraudulent transactions picked up in the U.S. Such complaints, which the company has also refused to provide, directly touch the U.S., and none of the arguments advanced by Western Union calls into question the Commission's authority to use its investigative process to require the company to produce them.

⁶⁵ Western Union's claim that fraud is somehow being conducted "unbeknownst" to the company by foreign con artists is troubling and serves to underscore the need for staff to investigate. Pet. 12. The FTC and other law enforcers have put the company on notice that the perpetrators of fraudulent or deceptive practices may be using its money transfer services, and the company has acknowledged and committed to improving its processes for detecting such activities. Indeed, Western Union has a legal obligation to detect and report such unlawful conduct. If Western Union now claims that it is unaware of this fraud, this highlights a need to examine the antifraud program more closely and its ability to detect such conduct.

Responses to Petitions to Quash

single consumer victim may subsequently be transferred multiple times through a money transfer network before the funds reach the ultimate perpetrator of the scheme. For example, a U.S. consumer who is the victim of a lottery scheme could transfer funds to a money transfer outlet in Canada, which, in turn, may transfer the funds to another outlet in Romania. The transfer from Canada to Romania injures the U.S. consumer, because it was her funds that were transferred. Similarly, the funds transferred by consumer victims in the U.K. that are picked up in Romania may subsequently be transferred to a con artist operating in the U.S. The fact that the complained-of transfer might have been routed through an agent in Romania, rather than directly to the U.S., would not negate the effects of such a transfer on the U.S.⁶⁶

Western Union's references to the need to promote international comity and avoid conflicts among data protection laws do not provide any basis for quashing the CID. Western Union has not cited any actual foreign data protection law, or described how such law would preclude Western Union from providing the FTC with any worldwide complaints.

Furthermore, Western Union's reliance on *Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Ct.*, 482 U.S. 522, 546 (1987), is misplaced. First, *Aerospatiale* involved private interests, not a federal agency's use of compulsory process in a law enforcement investigation. Second, contrary to Western Union's assertion, nothing in *Aerospatiale* stands for the proposition that discovery rules "ought never to be construed to violate the law of nations if any other possible construction remains" ⁶⁷ Instead, the Supreme Court concluded that the

⁶⁶ Though Western Union does not address it, Section 5(a)(4)(B) of the FTC Act, which addresses remedies for U.S. and foreign victims of consumer frauds, also supports the CID's request for worldwide complaints. If Western Union's failure to take reasonable steps to detect and prevent con artists from using its money transfer system causes harm to U.S. and foreign victims, the FTC is empowered by the SAFE WEB Act to remedy this harm. Any complaints from worldwide victims could bear on the scope of the harm and the proper amount of restitution.

⁶⁷ Pet. 12-13 (quoting *Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Ct.*, 482 U.S. 522, 546 (1987)). The text quoted by Western Union actually appears in a much older case, *Murray v. Schooner Charming Betsy*, 6 U.S. (2 Cranch) 64, 118 (1804), and was intended to promote international

Responses to Petitions to Quash

litigants were not required to use the procedures of the Hague Convention to obtain documents maintained outside the United States -- even from foreign corporations.⁶⁸ Indeed, federal courts analyzing the *Aerospatiale* decision have often applied the factors described there to order compliance with U.S. discovery requests even in the face of a foreign blocking or other statute.⁶⁹

Finally, Western Union fails to cogently explain how the CID undermines the FTC's role in enforcing the U.S.-EU Safe Harbor Framework.⁷⁰ Generally, the European Union's Directive on Data Protection requires that transfers of personal data take place only to non-EU countries that provide an "adequate" level of protection. The Framework is deemed adequate and provides a "safe harbor" to receive personal data from the European Union for those U.S. organizations that pledge to comply with a defined

comity as was the Court's decision in *Aerospatiale*. But the *Aerospatiale* Court also explicitly recognized the interests of the United States as an important factor in developing a comity analysis, following the *Charming Betsy* canon, that balances respect for other countries' judicial sovereignty against U.S. discovery requirements.

⁶⁸ 482 U.S. at 538-43. The Court explained that foreign blocking statutes

do not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that statute. Nor can the enactment of such a statute by a foreign nation require American courts to engraft a rule of first resort onto the Hague Convention, or otherwise to provide the nationals of such a country with a preferred status in our courts.

Id. at 544 n. 29 (citations omitted, citing *Societe Internationale Pour Participations Industrielles et Commerciales, S.A. v. Rogers*, 357 U.S. 197, 204-206 (1958)).

⁶⁹ See, e.g., *Devon Robotics v. Deviedma*, No. 09-cv-3522, 2010 U.S. Dist. LEXIS 108573, *10-*17 (E.D. Pa. Oct. 8, 2010) (ordering disclosure notwithstanding an Italian blocking statute); *Accessdata Corp. v. Alste Techn*, No. 2:08-cv-569, 2010 U.S. Dist. LEXIS 4566, *4-*8 (D. Utah. Jan. 21, 2010) (ordering disclosure notwithstanding a German blocking statute). This is particularly true in cases involving the enforcement of U.S. law. See, e.g., *In re Air Cargo Shipping Services Antitrust Litigation*, 278 F.R.D. 51, 52-54 (E.D.N.Y. 2010) (finding that "strong national interest[]" in U.S. enforcing antitrust laws outweighed France's interest in controlling access to information within its borders).

⁷⁰ Pet. at 13.

Responses to Petitions to Quash

set of privacy principles and certify to that commitment.⁷¹ The FTC then enforces that commitment and certification under Section 5 of the FTC Act. Contrary to what Western Union's brief appears to suggest,⁷² the FTC has not brought cases for violations of EU data protection laws.⁷³ Instead, the FTC may treat false certifications of compliance with the Framework as deceptive acts or practices.⁷⁴ As the European Commission itself has recognized, "U.S. law will apply to questions of interpretation and compliance with the Safe Harbor principles."⁷⁵ The Safe Harbor framework is clear that in the event of a conflict between U.S. law and the law of another jurisdiction, U.S. companies must still follow U.S. law. The Safe Harbor Framework itself provides that "where U.S. law imposes a conflicting obligation, U.S. organizations whether in the safe harbor or not must comply with the law."⁷⁶

⁷¹ See Export.gov, U.S.-E.U. Safe Harbor Overview, http://export.gov/safeharbor/eu/eg_main_018476.asp (last updated Apr. 26, 2012). As stated in that overview, "the Principles were solely designed to [deem the Framework to be adequate and] ... cannot be used as a substitute for national provisions implementing the Directive that apply to the processing of personal data in the Member States."

⁷² Pet. 13.

⁷³ The cases referenced by Western Union all involved allegations that companies falsely self-certified that they met the Safe Harbor requirements.

⁷⁴ See, e.g., *In re Facebook, Inc.*, FTC File No. 092 3184 (July 27, 2012).

⁷⁵ See Commission Decision of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce, at Annex 1 (attaching U.S. Department of Commerce Safe Harbor Privacy Principles (July 21, 2000)), <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:en:NOT>.

⁷⁶ See Export.gov, Damages for Breaches of Privacy, Legal Authorizations and Mergers and Takeovers in U.S. Law, at § B, http://export.gov/safeharbor/eu/eg_main_018482.asp (last updated Jan. 30, 2009). We note that Western Union is not presently among the organizations that have certified their compliance with the Safe Harbor privacy requirements. See <http://safeharbor.export.gov/list.aspx> (last visited March 4, 2013).

Responses to Petitions to Quash

IV. CONCLUSION

For the foregoing reasons, **IT IS HEREBY ORDERED THAT** the Petition of Western Union to Quash Civil Investigative Demands be, and it hereby is, **DENIED**.

IT IS FURTHER ORDERED THAT all responses to the specifications in the Civil Investigative Demand to Western Union must now be produced on or before March 18, 2013.

By the Commission, Commissioner Leibowitz not participating.

POLITICAL OPINIONS OF AMERICA

FTC File No. 122 3196. Order, May 9, 2013.

ORDER DENYING PETITION TO LIMIT OR QUASH MARCH 22, 2013,
CIVIL INVESTIGATIVE DEMAND ISSUED TO CARIBBEAN CRUISE
LINE, INC.

By OHLHAUSEN, Commissioner.

Caribbean Cruise Line, Inc. (“CCL”) has filed a petition to quash or limit the civil investigative demand (“CID”) issued by the Federal Trade Commission (“FTC” or “Commission”) on March 22, 2013. For the reasons stated below, the petition is denied.

I. INTRODUCTION

In 2012, the Commission received thousands of complaints about the following version, or a nearly identical version, of an unsolicited robocall that began,

Responses to Petitions to Quash

Hello, this is John from Political Opinions of America. You've been carefully selected to participate in a short 30 second research survey and for participating, you'll receive a free two-day cruise for two people to the Bahamas, courtesy of one of our supporters, gratuitous of the small port tax that will apply.

The consumer complaints alleged that, if consumers participated in the survey, they were given three automated political survey questions. Following each question, consumers were asked to select from a series of multiple-choice answers. They were then asked whether they were "interested in reserving a free cruise to the Bahamas" and were instructed to press 1 for "yes."

Consumers who pressed 1 were transferred to a live CCL telemarketer.¹ The telemarketer told consumers that the "free" cruise would cost \$59 per person in port taxes and attempted to "up-sell" the consumer with lodging in pre-boarding hotels, cruise excursions, enhanced accommodations, and other things.

In response to the complaints, the Commission opened an investigation of several entities, including CCL, which was identified in some complaints, to determine whether their practices constituted unfair or deceptive acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45 (as amended), or deceptive or abusive practices in violation of the Telemarketing Sales Rule, 16 C.F.R. pt 310 (as amended). On August 28, 2012, pursuant to a Commission resolution authorizing the use of compulsory process,² the FTC issued a CID

¹ CCL's business includes marketing and selling cruises [redacted].

² See Resolution Directing Use of Compulsory Process in a Nonpublic Investigation of Telemarketers, Sellers, Suppliers, or Others, File No. 0123145 ("Resolution"); Caribbean Cruise Line, Inc.'s Petition to Limit or Quash Civil Investigation Demand, at 6 n.17 (quoting Resolution) ("Petition"). The Resolution authorizes the use of compulsory process:

To determine whether unnamed telemarketers, sellers, or others assisting them have engaged or are engaging in: (1) unfair or deceptive acts or practices in or affecting commerce in violation of Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 (as amended); and/or deceptive or abusive telemarketing acts or practices in violation of the Commission's Telemarketing Sales Rule, 16 C.F.R. pt 310 (as

Responses to Petitions to Quash

to CCL seeking, among other things, information concerning the company's role in robocall campaigns and its telemarketing practices.³ Although CCL filed a petition to quash or modify the CID,⁴ it later withdrew that petition and provided a number of responses. After staff alerted CCL to certain deficiencies, CCL made a supplemental production.⁵ Further review of the original and supplemental productions made it apparent to FTC staff that CCL had withheld information about its telemarketing lead generators.⁶ Accordingly, on March 22, 2013, the Commission issued a follow-up CID specifically seeking such materials.⁷ In particular, the CID seeks:

- D-2 All documents that relate to any entity that used or uses phone calls to generate potential leads or customers for Caribbean Cruise Line, Inc.

amended), including but not limited to the provision of substantial assistance or support – such as mailing lists, scripts, merchant accounts and other information, products or services – to telemarketers engaged in unlawful practices. The investigation is also to determine whether Commission action to obtain redress for injury to consumers or others would be in the public interest.

³ Petition at 5.

⁴ *Id.* at 2 n.1, 5.

⁵ *Id.* at 5.

⁶ When staff inquired about the absence of any information or materials about CCL's telemarketing lead generators, CCL responded that it believed that such information and materials were not responsive.

⁷ CCL suggests that by issuing the follow-up CID to obtain the materials that CCL claimed were not responsive to the first CID, the FTC was "seek[ing] an end-run around" its duty to enforce the first CID. Petition at 5. The Commission does not have such a duty. It is well established that agencies have discretion with regard to the manner in which they approach such decisions. *See, e.g., Weight Watchers Int'l, Inc. v. FTC*, 47 F.3d 990, 992 (9th Cir. 1995). Here, the Commission issued a follow-up CID to request those materials that were not produced in response to the original CID as well as additional materials related to new areas of concern.

Responses to Petitions to Quash

- D-4 All documents that relate to any entity that provided or used automated dialers to generate potential leads or customers for Caribbean Cruise Line, Inc.⁸

The CID also sought information about additional named entities and individuals that, based on staff's review of documents provided by CCL in its delayed supplemental response to the first CID and other investigative leads, appear to have been involved in the robocall campaign.⁹ That specification in the CID seeks:

- D-1 All correspondence, electronic mails, notes on conversations, work orders, and other documents that relate to Firebrand Group SL, LLC, Employment for America, Inc., Political Boost LLC also dba CFPP Research Group, Linked Service Solutions, LLC, Jacob deJongh, Scott Broomfield or Jason Birkett.

Counsel for CCL and FTC staff conferred regarding possible limitations to the CID, but were unable to reach agreement.¹⁰ Accordingly, on April 9, 2013, CCL filed a petition to quash or limit the CID.

II. ANALYSIS

A. CCL Has Not Shown that the CID is Overbroad or Seeks Irrelevant Information

CCL's principal claim is that the CID seeks irrelevant information that falls outside the scope of the FTC's investigation. In particular, CCL claims that Specification D-1, which requires the production of correspondence, notes, work orders and other documents that relate to particular named entities or individuals, is overbroad and seeks information that "has nothing to do with the nature of the FTC's investigation." Similarly, CCL argues that "it is an absurdity to state that the names of CCL's customers

⁸ Petition at 6, 7.

⁹ *Id.* at 2.

¹⁰ *Id.* at 10.

Responses to Petitions to Quash

and/or lead generators [demanded by Specifications D-2 and D-4] are reasonably related to the FTC's inquiry, as names logically cannot contain information related to an entity's conduct."¹¹

We find CCL's objection to be without merit. Agency compulsory process is proper if the inquiry is within the authority of the agency, the demand is not too indefinite, and the information sought is reasonably relevant to the inquiry, as that inquiry is defined in the investigatory resolution.¹² It is well established that agencies have wide latitude to determine what information is relevant to their law enforcement investigations.¹³ In the context of an administrative CID, "relevance" is defined broadly and with deference to the administrative agency's determination.¹⁴ The specifications of the CID must be upheld so long as the information sought is "reasonably relevant" to the purpose and "not plainly incompetent or irrelevant to any lawful purpose" of the agency.¹⁵ Here, the Commission's investigation examines whether telemarketers, sellers, or others assisting them may have violated Section 5 of the FTC Act or the Commission's Telemarketing Sales Rule.¹⁶ The requested materials are plainly relevant to such an inquiry.

CCL also argues that Specification D-1 should be quashed because the request is over-inclusive to the extent that it demands *all* documents regarding the particular named entities or

¹¹ *Id.* at 6-7.

¹² *United States v. Morton Salt Co.*, 338 U.S. 632, 652 (1950); *FTC v. Invention Submission Corp.*, 965 F.2d 1086, 1088 (D.C. Cir. 1992); *FTC v. Texaco, Inc.*, 555 F.2d 862, 874 (D.C. Cir. 1977).

¹³ *See, e.g., Linde Thomsen Langworthy Kohn & Van Dyke, P.C. v. RTC*, 5 F.3d 1508, 1517 (D.C. Cir. 1993) (citing *Texaco, Inc.*, 555 F.2d at 882) (acknowledging that relevance is defined within the scope of investigation that may itself have broad scope).

¹⁴ *FTC v. Church & Dwight Co., Inc.*, 665 F.3d 1312, 1315-16 (D.C. Cir. 2011); *FTC v. Ken Roberts Co.*, 276 F.3d 583, 586 (D.C. Cir. 2001).

¹⁵ *Invention Submission*, 965 F.2d at 1091-92.

¹⁶ *See* Resolution, File No. 0123145, *supra* note 2.

Responses to Petitions to Quash

individuals.¹⁷ CCL admits that the specification calls for relevant material.¹⁸ Specification D-1 calls for the production of documents related to entities and individuals that CCL's response to the first CID and other investigative leads show either [redacted]. Documents that relate to such companies and individuals are of obvious relevance to the investigation.

Looking at the details of CCL's argument reveals that CCL's claim of over-inclusiveness is, at best, only a theoretical objection to the specification. CCL has not provided any factual basis to support its claim that the CID requires it to produce documents that are not relevant to the investigation.¹⁹ We find that the specification is reasonable. Given staff's prior dealings with CCL with the first CID, staff drafted the specification in a manner that directly identified the relevant information by naming the entities and individuals. [Redacted], the exploration of documents and areas that do not directly discuss one particular robocall campaign may nonetheless lead to information and materials that are directly relevant to the investigation, and courts have found such inquiries to be relevant.²⁰ Because relevance is defined broadly during the investigation stage,²¹ there is no basis to quash or limit

¹⁷ Petition at 7.

¹⁸ Petition at 6-7 ("request D-1 not only calls for information that is relevant to the investigation, but also *any* information between the parties regardless of subject matter").

¹⁹ See *FTC v. Church & Dwight Co., Inc.*, 756 F. Supp. 2d 81, 85 (D.D.C. 2010) (it is the burden of the party receiving the CID "to show that the information it wishes to withhold is irrelevant to the investigation"), *aff'd*, 665 F.3d 1312 (D.C. Cir. 2011); *FDIC v. Garner*, 126 F.3d 1138, 1144 (9th Cir. 1997) ("Once the [agency] has established relevancy, the party opposing the subpoena bears the burden of demonstrating the subpoena is unreasonable."); *Invention Submission*, 965 F.2d at 1090 (citing *Texaco*, 555 F.2d at 882) (it is petitioner's burden to demonstrate that the FTC has exceeded the broad standard for relevance).

²⁰ See *FTC v. Church & Dwight Co., Inc.*, 747 F. Supp. 2d 3, 9 (D.D.C. 2010) (rejecting claim that "FTC [must show] like any litigant, that the document demanded will lead to reasonably relevant and ultimately admissible evidence" as mischaracterizing the nature of the FTC's investigative authority) (citing *Morton Salt*, 338 U.S. at 642, and *Texaco*, 555 F.2 at 874.).

²¹ See, e.g., *Church & Dwight*, 747 F. Supp. 2d at 6 ("Speculations made by the FTC as to the possible relevance of the disputed information were

Responses to Petitions to Quash

the CID based on CCL's unsupported allegation that the specification calls for material outside the scope of the FTC's investigation.

CCL also objects to the scope of Specifications D-2 and D-4, which seek documents concerning entities that use phone calls or automated dialers to generate potential leads or customers for CCL. CCL claims that – because the “investigation merely concerns CCL's conduct” – “it is an absurdity to state that the names of CCL's customers and/or lead generators are reasonably related to the FTC's inquiry, as names cannot contain information related to an entity's conduct.”²² We disagree. As stated previously, “The standard for judging relevancy in an investigatory proceeding is more relaxed than in an adjudicatory one. . . . The requested material, therefore need only be relevant to the investigation – the boundary of which may be defined quite generally[.]”²³ Documents related to third-party telemarketing lead generators used by CCL go to the heart of an investigation looking into, among other things, possible violations of the Telemarketing Sales Rule. The names of CCL's customers and lead generators are similarly reasonably related to the investigation. Even if we accept CCL's characterization of the investigation's scope, such documents may provide material directly relevant to CCL's conduct or may lead to other material that is relevant to CCL's conduct.

B. The CID Properly Asks for Documents Within CCL's Possession and Control

CCL further objects to Specifications D-1, D-2, and D-4 “to the extent that they purport to require CCL to produce documents that are not in its possession.” According to CCL, the specifications “have no limitations with regard to CCL's liability

sufficient as long as they were not ‘obviously wrong.’”); *Genuine Parts Co. v. FTC*, 445 F.2d 1382, 1391 (5th Cir. 1971) (explaining that the court recognizes the extreme breadth that must be accorded the FTC in conducting an investigation).

²² Petition at 7.

²³ *Invention Submission*, 965 F.2d at 1090.

Responses to Petitions to Quash

to produce information not within CCL's possession." CCL contends that it is a separate legal entity than the companies named or identified in the specifications, and consequently, it asks that the requests be limited to make it clear that CCL is responsible for producing only those documents and information within its possession and control.

CCL's request for relief is unnecessary because the CID already provides appropriate limiting instructions. Specifically, Instruction I provides:

Scope of Search: This CID covers documents and information in your possession or under your actual or constructive custody or control including, but not limited to, documents and information in the possession, custody, or control of your attorneys, accountants, directors, officers, employees, and other agents and consultants, whether or not such documents and information were received from or disseminated to any person or entity.

These instructions are consistent with the applicable precedent. In the present context, "control" means the legal or practical ability to obtain the responsive documents.²⁴ Thus, a party can be said to control documents if they are available through a contractual right of access,²⁵ in the possession of a party's agents,²⁶ in the

²⁴ See, e.g., *In re NTL, Inc. Secs. Litig.*, 244 F.R.D. 179, 195 (S.D.N.Y. 2007) (applying Fed. R. Civ. P. 34) (citing *Bank of New York v. Meridien BIAO Bank Tanzania Ltd.*, 171 F.R.D. 135, 146-47 (S.D.N.Y. 1997)). See also, e.g., *In re Flag Telecom Holdings, Ltd. Sec. Litig.*, 236 F.R.D. 177, 180 (S.D.N.Y. 2006); *Dietrich v. Bauer*, 2000 WL 1171132 at *3 (S.D.N.Y. 2000) ("Control" has been construed broadly by the courts as the legal right, authority or practical ability to obtain the materials sought upon demand.").

²⁵ *Flagg v. City of Detroit*, 252 F.R.D. 346, 353 (E.D. Mich. 2008) (citing *Anderson v. Cryovac, Inc.*, 862 F.2d 910, 928-29 (1st Cir. 1988); *Golden Trade, S.r.L. v. Lee Apparel Co.*, 143 F.R.D. 514, 525 (S.D.N.Y. 1992)).

²⁶ *Flagg*, 252 F.R.D. at 353 (citing *Commercial Credit Corp. v. Repper*, 309 F.2d 97, 98 (6th Cir. 1962); *Am. Soc. for the Prevention of Cruelty to Animals v. Ringling Bros. & Barnum & Bailey Circus*, 233 F.R.D. 209, 212 (D.D.C. 2006); *Gray v. Faulkner*, 148 F.R.D. 220, 223 (N.D. Ind. 1992); *Cooper Indus. v. British Aerospace, Inc.*, 102 F.R.D. 918, 920 (S.D.N.Y. 1984)).

Responses to Petitions to Quash

possession of a party's officers or employees,²⁷ or maintained by a third party on the party's behalf.²⁸ CCL's obligation to produce documents includes the entities or individuals named or described by the CID that fall within these categories. Thus, we find that there is no basis to limit or quash the CID merely because CCL is organized separately from the named companies or individuals. If CCL has a legal right to control the documents,²⁹ including a right to obtain them on demand from the companies and individuals, then CCL must produce those documents and materials to respond to the CID.

C. A Demand for Trade Secret or Proprietary Information is Not a Reason to Quash or Limit the CID

CCL further contends that the CID should be limited or quashed because Specifications D-2 and D-4 demand documents and information that are trade secrets or constitute proprietary information.³⁰ Even assuming that CCL is correct in describing the materials, that would not be a basis for quashing the CID. The Commission's authority to use investigatory process and obtain relevant materials does not turn on the sensitivity of the information sought.³¹ As courts have recognized, "The fact that information sought by the Commission in an investigation

²⁷ *Flagg*, 252 F.R.D. at 353 (citing *Riddell Sports Inc. v. Brooks*, 158 F.R.D. 555, 558 (S.D.N.Y. 1994)).

²⁸ *Flagg*, 252 F.R.D. at 354 (citing *Tomlinson v. El Paso Corp.*, 245 F.R.D. 474, 477 (D. Colo. 2007)).

²⁹ CCL argues that the FTC cannot request CCL to produce documents that are possessed by the companies and individuals identified by Specifications D-1, D-2, and D-4, and cites *Power Integrations, Inc. v. Fairchild Semiconductor Int'l, Inc.*, 233 F.R.D. 143 (D. Del. 2005) and *Linde v. Arab Bank, PLC*, 262 F.R.D. 136 (E.D.N.Y. 2009). The cited cases are inapposite. The courts in both cases considered only whether American subsidiaries of a foreign parent corporation or foreign bank exerted control over the foreign parent. Here, in contrast, the companies and individuals are not corporate parents of CCL and CCL constructively or actually controls the entities.

³⁰ Petition at 8.

³¹ *FTC v. Invention Submission Corp.*, 1991-1 Trade Cas. (CCH) ¶ 69,338, at 65,353 (D.D.C. 1991), *aff'd*, 965 F.2d 1086, 1089 (D.C. Cir. 1992).

Responses to Petitions to Quash

constitutes a trade secret does not limit the Commission's power to obtain it. The only issue is whether the data which the Commission seeks is reasonably relevant to its investigation[.]”³²

The courts have acknowledged that an agency's confidentiality rules and practices provide ample protection for confidential information, and, therefore, the status of the responsive materials as trade secrets or confidential commercial information is not a proper basis for a motion to quash.³³ The Commission's Rules of Practice and Procedure provide CCL with adequate protections. Indeed, in its petition, CCL acknowledged that it was advised during its conference with Commission counsel that it could mark all trade secret information produced as “confidential.”³⁴ Commission rules specify that “no material that is marked or otherwise identified as confidential . . . will be made available without the consent of the person who produced the material, to any individual other than a duly authorized officer or employee of the Commission or a consultant or contractor retained by the Commission who has agreed in writing not to disclose the information.”³⁵ Moreover, material obtained by the Commission:

[t]hrough compulsory process and protected by section 21(b) of the Federal Trade Commission Act, 15 U.S.C. 57b-2(b) . . . and designated by the submitter as confidential and protected by . . . 15 U.S.C. 57b-2(f) [] and

³² *FTC v. Green*, 252 F. Supp. 153, 157 (S.D.N.Y. 1966).

³³ See, e.g., *FTC v. Rockefeller*, 441 F. Supp. 234, 242 (S.D.N.Y. 1977) (citations omitted) (“Respondents contend that the subpoenas should not be enforced because they seek confidential information. Such an objection poses no obstacles to enforcement. Even if it did, the impediment would be overcome by the protective provisions [implemented by the FTC], which are more than adequate for the purpose of guaranteeing confidentiality.”); *Texaco*, 555 F.2d 862, 884 n.2 (D.C. Cir. 1977) (“It is the agencies, not the courts, which should, in the first instance, establish the procedures for safeguarding confidentiality,” citing *FCC v. Schreiber*, 381 U.S. 279, 290-91, 295-96 (1965)).

³⁴ Petition at 8 n.24.

³⁵ 16 C.F.R. §4.10 (d).

Responses to Petitions to Quash

§ 4.10(d) of [Commission rules] . . . may be disclosed in Commission administrative or court proceedings subject to Commission or court protective or in camera orders as appropriate. . . . Prior to disclosure of such material in a proceeding, the submitter will be afforded an opportunity to seek an appropriate protective or in camera order.³⁶

These procedures provide ample protection for CCL for any responsive trade secrets or proprietary information that might be produced.³⁷ Consequently, there is no basis to limit or quash the CID merely because the documents may include confidential information.

III. CONCLUSION

For the foregoing reasons,

IT IS HEREBY ORDERED THAT the Petition of Caribbean Cruise Line, Inc. to Limit or Quash the Civil Investigation Demand be, and it hereby is, **DENIED**.

IT IS FURTHER ORDERED THAT all responses to the specifications in the Civil Investigative Demand to Caribbean Cruise Line, Inc. must be produced on or before May 24, 2013.

By the Commission.

³⁶ 16 C.F.R. § 4.10 (g).

³⁷ See *U.S. Int'l Trade Comm'n v. Tenneco West*, 822 F.2d 73, 79 (D.C. Cir. 1987) (“deference is due an agency in choosing its own procedures for guarding confidentiality”).