

Complaint

IN THE MATTER OF

LOOKOUT SERVICES, INC.CONSENT ORDER, ETC., IN REGARD TO ALLEGED VIOLATIONS OF
SEC. 5(A) OF THE FEDERAL TRADE COMMISSION ACT

*Docket No. C-4326; File No. 102 3076
Filed June 15, 2011 – Decision June 15, 2011*

This consent order addresses a security breach by Lookout Services, Inc. (“Lookout”), in which an employee gained unauthorized access to sensitive personal information, including Social Security numbers, of more than 37,000 consumers. Lookout provides a web-based computer product, known as I-9 Solution, that uses an employee’s sensitive personal information, including Social Security number, date of birth, address, and passport number, to verify that employee’s eligibility to work in the United States. The complaint alleges that Lookout misrepresented that it had implemented reasonable and appropriate security measures to protect the sensitive personal information it collected and maintained. This misrepresentation, combined with Lookout’s failure to implement such measures, constituted an unfair act or practice in violation of Section 5 of the FTC Act. The consent order prohibits Lookout from misrepresenting the privacy, confidentiality, or integrity of the personal information it collects from or about consumers. The consent order further requires Lookout to establish and maintain a comprehensive information security program. The consent order requires that Lookout retain an independent third party professional to assess this program on a biennial basis for the next 20 years.

Participants

For the *Commission*: Kristin Krause Cohen and Kandi Parsons.

For the *Respondent*: Rufus Oliver, Baker Botts L.L.P.

COMPLAINT

The Federal Trade Commission, having reason to believe that Lookout Services, Inc. (“respondent” or “Lookout”) has violated the

Complaint

provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Lookout is a Texas corporation, with its principal office or place of business at 5909 West Loop South, Suite 300, Bellaire, Texas 77401.

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 FTC Act, 15 U.S.C. § 44.

3. At all relevant times, Lookout has been in the business of selling a web-based computer product known as the I-9 Solution. This product is designed to help employers comply with their obligations under federal law to complete and maintain a U.S. Citizenship and Immigration Services Form I-9 about each employee in order to verify that the employee is eligible to work in the United States.

4. The I-9 Solution routinely collects and stores information from or about its customers’ employees, including, but not limited to, names; addresses; dates of birth; Social Security numbers; passport numbers; alien registration numbers; driver’s license numbers; and military identification numbers. This highly sensitive information is maintained in Lookout’s database (the “I-9 database”). The misuse of such information – particularly Social Security numbers – can facilitate identity theft and related consumer harms.

5. Since at least April 2009, Lookout has disseminated or caused to be disseminated statements in its marketing materials, including, but not limited to, the following statement regarding the security of data it maintains:

Secure Your Data

Although the data is entered via the web,
your data will be encoded and transmitted
over secured lines to Lookout Services

Complaint

server. This FTP interface will protect your data from interception, as well as, keep the data secure from unauthorized access.

6. Since at least 2006, Lookout's website has made the following claim:

Perimeter Defense – Our servers are continuously monitoring attempted network attacks on a 24 x 7 basis, using sophisticated software tools.

7. Since at least 2006 and continuing through at least the Fall of 2009, respondent engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on Lookout's networks. Among other things, respondent:

- a. failed to implement reasonable policies and procedures for the security of sensitive consumer information collected and maintained by Lookout;
- b. failed to establish or enforce rules sufficient to make user credentials (i.e., user ID and password) hard to guess. For example, respondent did not require its customers or employees to use complex passwords to access the I-9 database. Accordingly, users could select the same word, including common dictionary words, as both the password and user ID, or a close variant of the user ID as the password;
- c. failed to require periodic changes of user credentials, such as every 90 days, for customers and employees with access to sensitive personal information;
- d. failed to suspend user credentials after a certain number of unsuccessful login attempts;

Complaint

- e. did not adequately assess and address the vulnerability of Lookout's web application to widely-known security flaws, such as "predictable resource location," which enables users to easily predict patterns and manipulate the uniform resource locators ("URLs") to gain access to secure web pages;
- f. allowed users to bypass the authentication procedures on Lookout's website when they typed in a specific URL;
- g. failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as by employing an intrusion detection system and monitoring system logs; and
- h. created an unnecessary risk to personal information by storing passwords used to access the I-9 database in clear text.

8. In October 2009, and again in December 2009, Lookout's weak authentication practices and web application vulnerabilities enabled an employee of a Lookout customer to gain access to the personal information of over 37,000 consumers.

9. Specifically, in October 2009, the employee obtained a URL for a secure web page during a webinar for the I-9 Solution. She later typed that URL into her browser and gained access to a portion of the I-9 database. By typing the precise URL into the browser, she bypassed the Lookout login page, and was never prompted to provide a valid user credential. The employee then made minimal and easy-to-guess changes to the URL and gained access to the entire I-9 database.

10. In December 2009, the employee visited Lookout's public-facing login web page for the I-9 Solution where she guessed and entered several different user IDs and passwords, including the user ID "test" and the password "test." Because this was a valid user

Complaint

credential for one of Lookout's customers, entering "test" and "test" gave her access to the personal information of the more than 11,000 consumers employed by that customer. Then, by making minimal and easy-to-guess changes to the URL, the employee again gained access to the entire I-9 database, which included the personal information of more than 37,000 consumers.

11. Because Lookout did not employ an intrusion detection system until October 2009, or adequately monitor system logs until December 2009, it is unknown if other unauthorized persons accessed the personal information in the I-9 database before that time.

12. Following the October and December 2009 breaches, Lookout took steps to prevent additional unauthorized access to the I-9 database, including disabling the "test" account and instituting certain code patches to its application. In January 2010, Lookout mailed breach notification letters to customers whose accounts the employee may have viewed.

VIOLATIONS OF THE FTC ACT

13. Through the means described in Paragraphs 5 and 6, respondent represented, expressly or by implication, that it implemented reasonable and appropriate measures to protect personal information against unauthorized access.

14. In truth and in fact, as described in Paragraph 7, respondent did not implement reasonable and appropriate measures to protect personal information against unauthorized access. Therefore, the representations set forth in Paragraph 13 were, and are, false and misleading, and constitute a deceptive act or practice.

15. As set forth in Paragraph 7, respondent failed to employ reasonable and appropriate measures to prevent unauthorized access to sensitive personal information. Respondent'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

Complaint

reasonably avoidable by consumers. This practice was, and is, an unfair act or practice.

16. 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 fifteenth day of June, 2011, has issued this complaint against respondent.

By the Commission.

DECISION AND ORDER

The Federal Trade Commission having initiated an investigation of certain acts and practices of the Respondent named in the caption hereof, and the Respondent having been furnished thereafter with a copy of a draft 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 the Respondent with violation of the Federal Trade Commission 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"), an admission by the Respondent of all the jurisdictional facts set forth in the aforesaid draft Complaint, a statement that the signing of said Consent Agreement is for settlement purposes only and does not constitute an admission by Respondent that the law has been violated as alleged in such Complaint, or that the facts as alleged in such Complaint, other than

Decision and Order

jurisdictional facts, are true, and waivers and other provisions as required by the Commission's Rules; and

The Commission having thereafter considered the matter and having determined that it has reason to believe that the Respondent has violated the said Act, and that a Complaint should issue stating its charges in that respect, and having thereupon accepted the executed Consent Agreement and placed such Consent Agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comments, now in further conformity with the procedure described 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 is a Texas corporation with its principal office or place of business at 5909 West Loop South, Suite 300, Bellaire, Texas 77401.
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 Lookout Services, Inc., its subsidiaries, divisions, affiliates, successors and assigns.
2. “Personal information” shall mean individually identifiable information from or about an individual consumer 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

Decision and Order

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 number or other government-issued identification number; (g) a bank account, debit card, or credit card account number; (h) a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is combined with other available data that identifies an individual consumer; (i) a biometric record; or (j) any information that is combined with any of (a) through (i) above. For the purpose of this provision, a "consumer" shall mean any person, including, but not limited to, any user of respondent's services, any employee of respondent, or any individual seeking to become an employee, where "employee" shall mean an agent, servant, salesperson, associate, independent contractor, or other person directly or indirectly under the control of respondent.

3. "Commerce" shall mean as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

I.

IT IS ORDERED that respondent, directly or through any corporation, subsidiary, division, website, or other device, shall not misrepresent in any manner, expressly or by implication, the extent to which it maintains and protects the privacy, confidentiality, security, or integrity of personal information collected from or about consumers.

II.

IT IS FURTHER ORDERED that respondent and its officers, agents, representatives, and employees, directly or through any corporation, subsidiary, division, website, or other device, shall, no later than the date of service of this order, establish and implement,

Decision and Order

and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers, including:

- A. the designation of an employee or employees to coordinate and be accountable for the information security program.
- B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures.
- C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures.
- D. the development and use of reasonable steps to select and retain service providers capable of appropriately

Decision and Order

safeguarding personal information they receive from respondent, and requiring service providers by contract to implement and maintain appropriate safeguards.

- E. the evaluation and adjustment of respondent's information security program in light of the results of the testing and monitoring required by subpart C, 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 the information security program.

III.

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 uses procedures and standards generally accepted in the profession. Professionals qualified to prepare such assessments shall be: a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a 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 and 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;

Decision and Order

- 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 personal information collected from or about consumers;
- 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, confidentiality, and integrity of personal 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 completed. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director for 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 Lookout Services, Inc.*, FTC File No.1023076. *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.

Decision and Order

IV.

IT IS FURTHER ORDERED that respondent shall maintain and, upon request, make available to the Federal Trade Commission for inspection and copying:

- A. for a period of three (3) years after the date of preparation of each Assessment required under Part III of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of 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 IV.A, for a period of five (5) years from the date of preparation or dissemination, whichever is later, a print or electronic copy of each document relating to compliance with this order, including but not limited to:
 - 1. all advertisements and promotional materials containing any representations covered by this order, with 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 compliance with this order.

V.

IT IS FURTHER ORDERED that respondent shall deliver copies of the order as directed below:

Decision and Order

- A. Respondent must deliver a copy of this order to (1) all current and future principals, officers, directors, and managers, (2) all current and future employees, agents, and representatives having responsibilities relating to the subject matter of this order, and (3) any business entity resulting from any change in structure set forth in Part VI. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities. For any business entity resulting from any change in structure set forth in Part VI, delivery shall be at least ten (10) days prior to the change in structure.
- B. Respondent must secure a signed and dated statement acknowledging receipt of this order, within thirty (30) days of delivery, from all persons receiving a copy of the order pursuant to this section.

VI.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in respondent 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 company; 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 either corporate name or address. *Provided, however,* that, with respect to any proposed change in the corporation about which respondent learns less 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

Decision and Order

Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the matter of Lookout Services, Inc.*, FTC File No.1023076. *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.

VII.

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 additional true and accurate written reports.

VIII.

This order will terminate on June 15, 2031, or twenty (20) years from the most recent date that the United States or the Federal Trade 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 less 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.

Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order,

Decision and Order

and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

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

The Federal Trade Commission has accepted, subject to final approval, a consent order applicable to Lookout Services, Inc.

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.

The Commission's complaint alleges that Lookout sells a web-based computer product known as the I-9 Solution. This product is designed to help employers comply with their obligations under federal law to complete and maintain a U.S. Citizenship and Immigration Services Form I-9 about each employee in order to verify that the employee is eligible to work in the United States. The complaint alleges that the I-9 Solution routinely collects and stores information about Lookout's customers' employees, including, but not limited to: names; addresses; dates of birth; Social Security

Analysis to Aid Public Comment

numbers; passport numbers; alien registration numbers; driver's license numbers; and military identification numbers. This highly sensitive information is maintained in Lookout's database (the "I-9 database"). The misuse of such information – particularly Social Security numbers, which do not expire – can facilitate identity theft, including existing and new account fraud, and related consumer harms.

The complaint alleges that, since at least 2006, Lookout engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for the personal information it collected and maintained. The challenged practices are fundamental security failures, most of which have been challenged in prior FTC data security cases. Among other things, Lookout:

- a. failed to implement reasonable policies and procedures for the security of sensitive consumer information it collected and maintained;
- b. failed to establish or enforce rules sufficient to make user credentials (*i.e.*, user ID and password) hard to guess;
- c. failed to require periodic changes of user credentials, such as every 90 days, for customers and employees with access to sensitive personal information;
- d. failed to suspend user credentials after a certain number of unsuccessful login attempts;
- e. did not adequately assess and address the vulnerability of its web application to widely-known security flaws, such as "predictable resource location," which enables users to easily predict patterns and manipulate the uniform resource locators ("URL") to gain access to secure web pages;
- f. allowed users to bypass the authentication procedures on Lookout's website when they typed in a specific URL;

Analysis to Aid Public Comment

- g. failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as by employing an intrusion detection system and monitoring system logs; and
- h. created an unnecessary risk to personal information by storing passwords used to access the I-9 database in clear text.

Each of these failures could have been remedied using well-known, readily available, and/or free or low-cost data security measures.

The complaint further alleges that, as a result of these failures, an employee of a Lookout customer was able to obtain unauthorized access to Lookout's I-9 database on two separate occasions between October and December 2009. In both instances, the employee gained unauthorized access to the personal information, including Social Security numbers, of more than 37,000 consumers. Given the sensitive nature of the personal information exposed, the company's failure to provide reasonable and appropriate security for this information is likely to cause consumers substantial injury as described above. That substantial injury is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. The complaint alleges that Lookout's failure to employ reasonable and appropriate measures to prevent unauthorized access to sensitive personal information is an unfair act or practice and that the company misrepresented that it had implemented such measures, in violation of Section 5 of the Federal Trade Commission Act.

The proposed order applies to personal information that Lookout collects from or about consumers and employees. It contains provisions designed to prevent Lookout from engaging in the future in practices similar to those alleged in the complaint.

Part I of the proposed order prohibits misrepresentations about the privacy, confidentiality, or integrity of personal information

Analysis to Aid Public Comment

collected from or about consumers. Part II of the proposed order requires Lookout to establish and maintain a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. The security program must contain administrative, technical, and physical safeguards appropriate to Lookout's size and complexity, the nature and scope of its activities, and the sensitivity of the information collected from or about consumers and employees. Specifically, the proposed order requires Lookout to:

- designate an employee or employees to coordinate and be accountable for the information security program;
- identify material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks;
- design and implement reasonable safeguards to control the risks identified through risk assessment, and regularly test or monitor the effectiveness of the safeguards' key controls, systems, and procedures;
- develop and use reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from Lookout, and require service providers by contract to implement and maintain appropriate safeguards; and
- evaluate and adjust its information security programs in light of the results of testing and monitoring, any material changes to operations or business arrangements, or any other circumstances that it knows or has reason to know may have a material impact on its information security program.

Analysis to Aid Public Comment

Part III of the proposed order requires Lookout 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, confidentiality, and integrity of sensitive consumer, employee, and job applicant information has been protected.

Parts IV through VIII of the proposed order are reporting and compliance provisions. Part IV requires Lookout to retain documents relating to its compliance with the order. For most records, the order requires that the documents be retained for a five-year period. For the third-party assessments and supporting documents, Lookout must retain the documents for a period of three years after the date that each assessment is prepared. Part V requires dissemination of the order now and in the future to all current and future subsidiaries, current and future principals, officers, directors, and managers, and to persons with responsibilities relating to the subject matter of the order. Part VI ensures notification to the FTC of changes in corporate status. Part VII mandates that Lookout submit a compliance report to the FTC within 60 days, and periodically thereafter as requested. Part VIII 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 order or to modify its terms in any way.

Complaint

**IN THE MATTER OF
TOPS MARKETS LLC, MORGAN STANLEY CAPITAL
PARTNERS V U.S. HOLDCO LLC, AND THE PENN
TRAFFIC COMPANY**

CONSENT ORDER, ETC., IN REGARD TO ALLEGED VIOLATIONS OF
SEC. 5 OF THE FEDERAL TRADE COMMISSION ACT AND SEC. 7 OF
THE CLAYTON ACT

*Docket No. C-4295; File No. 101 0074
Filed August 4, 2010 – Decision June 30, 2011*

This consent order addresses the allegations regarding the proposed \$85 million acquisition by Tops Markets LLC (“Tops”) of substantially all supermarkets owned by The Penn Traffic Company (“Penn”), as part of Penn’s petition for bankruptcy pursuant to Chapter 11 of the Bankruptcy Code, 11 U.S.C. § 301, *et seq.* The complaint alleges that the acquisition of Penn’s supermarkets by Tops would eliminate direct competition in parts of New York and Pennsylvania, resulting in higher grocery prices for consumers. The consent order requires the parties to divest seven Penn supermarkets, together with their related assets, to a Commission-approved buyer and to allow the Commission-approved buyer to operate these supermarkets at their respective locations. The consent order further requires the parties to maintain the competitive viability of these assets pending divestiture. In the event the parties fail to divest the assets within the time period prescribed by the Commission, the consent order permits the Commission to appoint a divestiture trustee to effectuate the divestiture.

Participants

For the *Commission*: Michelle Fetterman, Jeanne Liu, David von Nirschl, and Anthony Saunders.

For the *Respondents*: Kathleen Beasley and Jim Wade, Haynes & Boone LLP; and Kevin Arquit, Evan Cohen, Aimee Goldstein, and Jayma Meyer, Simpson Thacher & Bartlett LLP.