

FEDERAL TRADE COMMISSION DECISIONS

FINDINGS, OPINIONS, AND ORDERS
JULY 1, 2021, TO DECEMBER 31, 2021

IN THE MATTER OF

**MOVIEPASS, INC.,
HELIOS AND MATHESON ANALYTICS, INC.,
MITCHELL LOWE,
AND
THEODORE FARNSWORTH**

CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT AND SECTION 4 OF THE RESTORE ONLINE SHOPPERS' CONFIDENCE ACT.

*Docket No. C-4751; File No. 192 3000
Complaint, October 1, 2021 – Decision, October 1, 2021*

This consent order addresses MoviePass, Inc.'s representation of their movie subscription service. The complaint alleges that Respondents violated Section 5(a) of the Federal Trade Commission Act by deceptively preventing subscribers from using the subscription service as advertised and failing to take reasonable measures to secure consumers' data. The complaint also alleges that respondents violated Section 4 of the Restore Online Shoppers' Confidence Act by failing to clearly and conspicuously disclose all material terms of the transaction before billing through a negative option feature. The consent order prohibits Respondents from misrepresenting their service and data practices and stipulates that any businesses controlled by the Respondents must implement information security programs.

Participants

For the *Commission*: Thomas B. Carter and Zachary A. Keller.

For the *Respondents*: Alan Nisselson and Leslie S. Barr [*Windels Marx Lane & Mittendorf, LLP.*] and Jason Gonzalez, Neal Gauger and Tina Sciocchetti [*Nixon Peabody, LLP.*].

COMPLAINT

The Federal Trade Commission, having reason to believe that MoviePass, Inc., a corporation, Helios and Matheson Analytics, Inc., a corporation, Mitchell Lowe, individually and as an officer of MoviePass, Inc., and Theodore Farnsworth, individually and as an officer of Helios and Matheson Analytics, Inc. (collectively, "Respondents"), have violated the provisions of the Federal Trade Commission Act, 15 U.S.C. § 45, and the Restore Online Shoppers' Confidence Act

Complaint

(“ROSCA”), 15 U.S.C. § 8403, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent MoviePass, Inc. is a Delaware corporation with its principal place of business at 350 Fifth Avenue, Suite 5330, New York, New York 10118. Respondent MoviePass is a subsidiary of Helios and Matheson Analytics, Inc., which acquired a controlling interest in August 2017 and more than 90 percent of the company by April 2018.

2. Respondent Helios and Matheson Analytics, Inc. (“Helios”) is a Delaware corporation with its principal place of business also at 350 Fifth Avenue, Suite 5330, New York, New York 10118.

3. Respondent Mitchell Lowe (“Lowe”) is the Chief Executive Officer of Respondent MoviePass. Individually or in concert with others, he controlled or had the authority to control, or participated in the acts and practices of Respondent MoviePass, including those relating to its advertising, marketing, public relations, data security, customer service, and the acts and practices alleged in this complaint. At all times material to this complaint, his principal office or place of business was the same as that of Respondents MoviePass and Helios.

4. Respondent Theodore Farnsworth (“Farnsworth”) was the Chief Executive Officer of Helios until September 2019. Individually or in concert with others, he controlled or had the authority to control, or participated in the acts and practices of Respondents MoviePass and Helios, including those relating to Respondent MoviePass’s advertising, marketing, public relations, customer service, and the acts and practices alleged in this complaint. At all times material to this complaint, his principal office or place of business was the same as that of Respondents MoviePass and Helios.

5. Respondents MoviePass and Helios (collectively, “Corporate Respondents”) have operated as a common enterprise while engaging in the unlawful acts and practices alleged below. Corporate Respondents have conducted the business practices described below through interrelated companies that have common ownership, managers, employees, and office locations. Because these Corporate Respondents have operated as a common enterprise, each of them is jointly and severally liable for the acts and practices alleged below. Lowe and Farnsworth have formulated, directed, controlled, or had the authority to control, or participated in the acts and practices of the common enterprise alleged in this complaint.

6. Respondents have advertised, offered for sale, sold, and distributed services to consumers, including the MoviePass movie viewing subscription service.

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

Complaint

RESPONDENTS' BUSINESS PRACTICES

8. In 2011, Respondent MoviePass launched a “MoviePass” subscription service that allowed consumers to view movies at their local theaters for a monthly fee. Between 2011 and 2017, Respondent MoviePass offered a variety of subscription plans at different price points, which were generally sold through a negative option in which consumers continued to pay a monthly fee for the service unless they affirmatively canceled their subscriptions.

9. In August 2017, Respondents re-launched the MoviePass service nationwide, offering consumers “unlimited” movie viewings at theaters for \$9.95 per month, again sold as a negative option. Respondents expressly marketed the service (a) as offering “Unlimited movies for only \$9.95/month”; (b) as providing access to “ANY MOVIE ANY THEATER ANY DAY,” including “ALL MAJOR MOVIES” in “ALL MAJOR THEATERS”; and (c) as allowing consumers to “[e]njoy a new movie every day.” The following marketing materials were representative of its advertisements during the period material to this complaint:

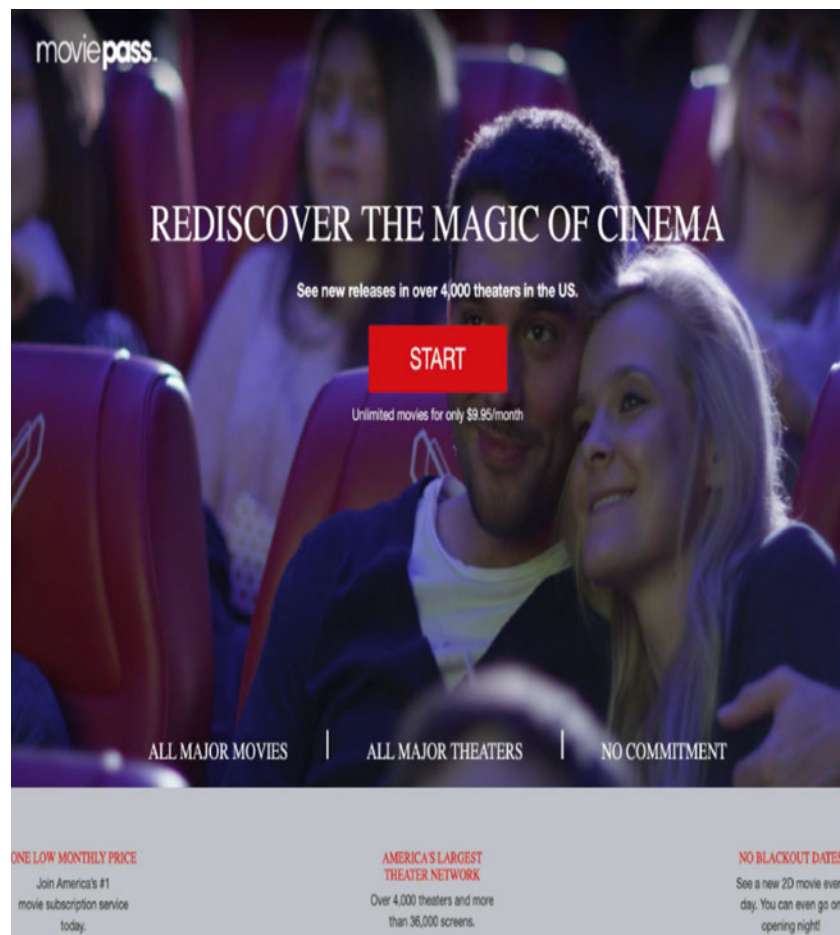


Figure 1 (image produced to the FTC by Respondent MoviePass on June 14, 2019).

Complaint

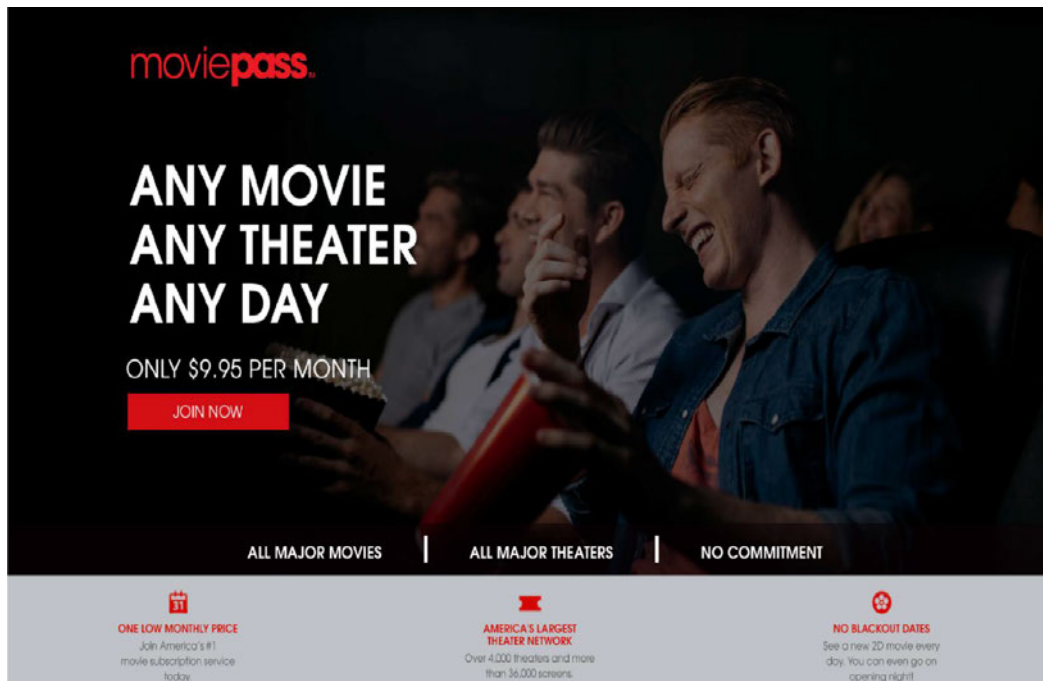


Figure 2 (image produced to the FTC by Respondent MoviePass on June 14, 2019).

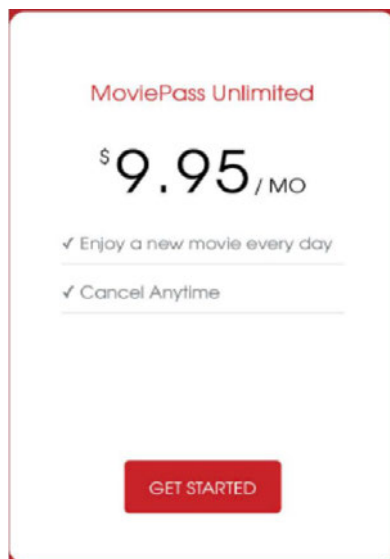


Figure 3 (image produced to the FTC by Respondent MoviePass on June 14, 2019).

10. Respondents had attracted approximately 3.2 million subscribers to MoviePass by early 2018. By this time, however, Corporate Respondents were already incurring financial losses due to the cost of the movie tickets subscribers acquired through the service.

Complaint

- a. In Respondent Helios's April 2018 Form 10-K filing, its auditors "expressed substantial doubt about [Respondent Helios's] ability to continue as a going concern."
- b. In a May 2018 SEC filing, Respondent Helios provided a "Financial Update" in which it disclosed that it ran an average cash deficit of \$21.7 million per month from September 30, 2017 to April 30, 2018.

**RESPONDENTS DECEPTIVELY PREVENTED SUBSCRIBERS FROM USING
MOVIEPASS AS ADVERTISED**

11. In April 2018, Respondents devised and implemented "password disruption" and "ticket verification" programs in tandem to limit frequent MoviePass users' ability to view movies through the service as advertised.

12. Password Disruption. Under Respondents' password disruption program, Respondents invalidated the passwords of the 75,000 subscribers who used the service most frequently while claiming that "we have detected suspicious activity or potential fraud" on the affected subscribers' accounts.

13. This representation regarding purported "suspicious activity" caused one MoviePass executive to advise that it "**could insinuate there may have been a data breach**" (emphasis in original) and another to advise that "[i]t will go on [an online forum] and suspicions will arise ... 'were they hacked?' 'Is our data really safe?'"

14. The password disruption program impeded subscribers' ability to view movies because MoviePass's password reset process often failed.

- a. To reset their passwords, subscribers generally had to complete four steps: (i) enter their email addresses into the MoviePass app's "Reset Password" tool; (ii) wait for Respondent MoviePass to send an email with a password reset hyperlink; (iii) respond to the email by clicking on a hyperlink in the email; and (iv) fill out password reset information on a webpage accessed by the hyperlink.
- b. Subscribers were often unable to reset their passwords because (i) the app would not accept their email address; (ii) the subscriber would never receive a password reset email; or (iii) the email's hyperlink would lead to a "Page Not Found" notification.
- c. Indeed, when discussing the password disruption program, a MoviePass executive acknowledged that subscribers using a common smartphone operating system would encounter technical difficulty in resetting their passwords.

Complaint

- d. When subscribers attempted to contact MoviePass's customer service about their inability to reset their MoviePass passwords, Respondents often responded weeks later or not at all.
- e. As a result of password reset failures and related poor customer service, subscribers who were required to reset their passwords were often unable to reset their passwords or to reset their passwords in a timely manner.

15. Both Lowe and Farnsworth knew of, ordered, or helped execute the password disruption program.

- a. On April 11, 2018, an employee of Respondent Helios, writing from Farnsworth's personal email address and expressly "on behalf of Ted [Farnsworth]" to Lowe and others, proposed a notice that informed subscribers that their account passwords were required to be reset due to "suspicious activity or potential fraud."
- b. Lowe circulated the proposed notice to MoviePass executives for comment and personally ordered subscribers' passwords to be disrupted in accordance with this plan. Lowe also personally chose the number of consumers who would be affected by the program.

16. Both Lowe and Farnsworth were aware of the deceptive nature of the password disruption program even at the time they were formulating it and understood its negative effect on consumers.

- a. When Lowe and Farnsworth presented the disruption program to other executives of Respondent MoviePass, one executive warned that the password disruption program "would be targeting all of our heavy users" and that "**there is a high risk this would catch the FTC's attention (and State AG's attention)** and could reinvigorate their questioning of MoviePass, this time from a Consumer Protection standpoint." (Emphasis in original).
- b. Another executive agreed, warning of "**FTC Fears:** All [the other MoviePass executive's] notes about FTC and PR [public relations] fire are my main concerns as I think the PR backlash will flame the FTC stuff." (Emphasis in original).
- c. In response to these concerns, Lowe responded, "Ok I get it. So let[']s try this with a small group. Let[']s say 2% of our highest volume users."

Complaint

- d. Respondents MoviePass and Lowe tracked the effect of password disruption on subscribers' use of the service. For example, Respondents MoviePass and Lowe found that only one-half of affected subscribers had successfully reset their passwords one week after they executed their plan.

17. Respondents' password disruption program prevented many subscribers who were using MoviePass in compliance with its terms of use from viewing movies with their MoviePass subscriptions.

18. Ticket Verification. Also in April 2018, Respondents imposed a ticket verification program to prevent certain subscribers from using the service.

19. The ticket verification program required subscribers to take and submit pictures of their physical movie ticket stubs for approval through the MoviePass app within a certain timeframe. Only tickets accepted by Respondent MoviePass's automated system qualified as properly submitted, and the program terms warned: (a) that subscribers whose pictures were not verified by the automated system would not be able to view future films until they uploaded a photo; and (b) that subscribers whose pictures were not verified by the automated system more than once would have their subscriptions canceled.

20. Respondents imposed this ticket verification requirement on the 20 percent of subscribers who used the MoviePass service most frequently while representing to these approximately 450,000 consumers that they had been "randomly selected" for the program and that it was intended to ensure compliance with MoviePass's terms of use.

21. The ticket verification program obstructed thousands of subscribers' ability to use MoviePass because: (a) the automated ticket verification program often did not function on certain common smartphone operating systems; (b) the program's software often failed to recognize pictures of the ticket stubs subscribers submitted; and (c) Respondents were unable to handle the volume of customer service complaints relating to the program, which left subscribers' complaints unresolved.

22. Both Lowe and Farnsworth knew of, ordered, or helped execute the ticket verification program.

- a. Lowe was aware of the ticket verification program and personally chose the number of consumers who would be subject to the program.
- b. Farnsworth was aware of the ticket verification program and received at least one report about the program's effect on consumers.

Complaint

23. Lowe was aware that the ticket verification program was deceptive and understood its negative effect on consumers.

- a. Respondents MoviePass and Lowe used the program to limit consumers' viewing of a major motion picture. When a MoviePass executive suggested that they delay an increase of ticket verification as "dry powder" to reduce ticket purchases for an upcoming major film release, Lowe responded, "Yes i [sic] agree to hold our powder for [the film]."
- b. When Lowe was advised by a MoviePass executive that the ticket verification and password disruption programs would render Respondent MoviePass "not [] able to keep up in incoming [consumer complaint] volume this weekend," Lowe responded, "Yep we understand."
- c. Respondents MoviePass and Lowe tracked the program's effect on subscribers and the anticipated reduction in usage the program would cause.

24. Respondents' ticket verification program prevented many subscribers who were using MoviePass in compliance with its terms of use from viewing movies with their MoviePass subscriptions.

25. Trip Wires. By approximately August 2018, Respondents devised another program to prevent frequent users from viewing one movie per day with MoviePass as Respondents had advertised: undisclosed financial thresholds that Respondents referred to as "trip wires."

26. To implement trip wires, Respondents placed subscribers into groups based upon how frequently they used MoviePass. Respondents assigned a dollar allotment to each group so that subscribers in the same group would collectively only be able to purchase a limited number of tickets using the MoviePass service.

27. Respondents typically imposed their trip wire financial thresholds on subscribers who viewed more than three movies per month using MoviePass—far fewer than the "one movie per day" limit that MoviePass represented when marketing MoviePass.

28. Subscribers were unaware that they had been placed in these groups or that they were subject to these financial trip wires: the practice was not disclosed in Respondents' advertising or terms of use, and MoviePass customer service did not tell affected subscribers who had lost access to MoviePass that they were subject to them.

29. Once a given group hit its "trip wire" threshold, Respondents denied access to the MoviePass service to all subscribers in that group. Subscribers affected by the trip wire would be unable to use the MoviePass service when they attempted to use it, often after having already traveled to a movie theater intending to use the service.

Complaint

30. Both Lowe and Farnsworth knew of, ordered, or helped execute the trip wire program.

- a. Lowe was aware of the trip wire program and personally set the trip wire thresholds.
- b. Farnsworth was aware of the trip wire program and received at least one report about its implementation and effect on consumers.

31. Lowe was aware that trip wire program was deceptive and understood its negative effect on consumers.

- a. On April 4, 2019, Lowe explained in an email that the “beauty of the cap [i.e. trip wire financial threshold]” was that “heavy users compete against other heavy users for tickets.”
- b. The following week, Lowe participated in correspondence regarding trip wire-related consumer complaints where a senior manager noted that “[w]e do have our hands tied as far as an explanation goes as we do not want to tell them they’ve consumed too much . . . These users are under the assumption that they’re uncapped, so it’s going to be tricky coming up with the right wording.”

32. Respondents’ trip wire program prevented many subscribers who were using MoviePass in compliance with its terms of use from viewing movies with their MoviePass subscriptions.

RESTORE ONLINE SHOPPERS’ CONFIDENCE ACT

33. In 2010, Congress passed the Restore Online Shoppers’ Confidence Act, 15 U.S.C. § 8401 *et seq.*, which became effective on December 29, 2010. Congress passed ROSCA because “[c]onsumer confidence is essential to the growth of online commerce. To continue its development as a marketplace, the Internet must provide consumers with clear, accurate information and give sellers an opportunity to fairly compete with one another for consumers’ business.” Section 2 of ROSCA, 15 U.S.C. § 8401.

34. Section 4 of ROSCA, 15 U.S.C. § 8403, generally prohibits charging consumers for goods or services sold in transactions effected on the Internet through a negative option feature, as that term is defined in the Commission’s Telemarketing Sales Rule (“TSR”), 16 C.F.R. § 310.2(w), unless the seller (1) clearly and conspicuously discloses all material terms of the transaction before obtaining the consumer’s billing information, (2) obtains the consumer’s express informed consent before making the charge, and (3) provides a simple mechanism to stop recurring charges. See 15 U.S.C. § 8403.

Complaint

35. The TSR defines a negative option feature as: “in an offer or agreement to sell or provide any goods or services, a provision under which the consumer’s silence or failure to take an affirmative action to reject goods or services or to cancel the agreement is interpreted by the seller as acceptance of the offer.” 16 C.F.R. § 310.2(w).

36. As described in Paragraphs 8 to 10, above, Respondents have advertised and sold subscriptions to the MoviePass service to consumers through a negative option feature as defined by the TSR. See 16 C.F.R. § 310.2(w).

37. Pursuant to Section 5 of ROSCA, 15 U.S.C. § 8404, a violation of ROSCA is a violation of a rule promulgated under Section 18 of the FTC Act, 15 U.S.C. § 57a.

VIOLATIONS OF THE FTC ACT**Count I – All Respondents
Misrepresenting MoviePass**

38. In connection with the advertising, promotion, offering for sale, or sale of the MoviePass subscription service, Respondents have represented, directly or indirectly, expressly or by implication, that consumers who purchase a MoviePass subscription:

- a. could use MoviePass to view one movie per day at their local movie theaters; and
- b. could use MoviePass to view any movie, in any theater, at any time.

39. In numerous instances in which Respondents made these representations, consumers who purchased a MoviePass subscription:

- a. could not use MoviePass to view one movie per day at their local movie theaters; and
- b. could not use MoviePass to view any movie, in any theater, at any time.

Therefore, the representations set forth in Paragraph 38 are false or misleading.

VIOLATIONS OF ROSCA**Count II – All Respondents
Violations of ROSCA**

40. In numerous instances, in connection with charging consumers for goods or services sold in transactions effected on the Internet through a negative option feature, as described in Paragraphs 11—32 above, Respondents have failed to:

Complaint

- a. clearly and conspicuously disclose all material terms of the transaction before obtaining the consumer's billing information; or
- b. obtain the consumer's express informed consent before charging the consumer's credit card, debit card, bank account, or other financial account for the transaction.

41. Respondents' practices as set forth in Paragraph 40 are a violation of Section 4 of ROSCA, 15 U.S.C. § 8403, and are therefore a violation of a rule promulgated under Section 18 of the FTC Act, 15 U.S.C. § 57a, 15 U.S.C. § 8404(a), and therefore constitute an unfair or deceptive act or practice in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

**RESPONDENTS' FAILURE TO TAKE REASONABLE MEASURES
TO SECURE CONSUMERS' DATA**

42. Respondent MoviePass collected significant amounts of personal information from consumers in connection with its subscriptions, including first name, last name, postal address, email address, birth date, gender, credit card number, CVV, expiration date, billing address, card type, geolocation information, user reviews, and movies attended.

43. In MoviePass's privacy policy, Respondent MoviePass made representations about its data security practices concerning personal information collected from consumers.

44. Respondent MoviePass represented, in relevant part, that it "takes information security very seriously" and "uses reasonable administrative technical, physical, and managerial measures to protect [consumers'] personal details from unauthorized access."

45. Respondent MoviePass further represented that it stored consumers' email addresses and payment information in "an encrypted form."

46. Lowe was responsible for Respondent MoviePass's consumer response and communication policies, practices, and procedures. These responsibilities include oversight of the representations Respondent MoviePass has made to consumers regarding data security.

47. Lowe was also responsible for the oversight of Respondent MoviePass's data security practices.

48. On August 20, 2019, media outlets reported that a security researcher had allegedly breached an exposed Respondent MoviePass database containing large amounts of consumers' personal information.

49. Respondent MoviePass confirmed the data breach on August 22, 2019 through a prepared statement, acknowledging "a security vulnerability that may have exposed subscriber records" and promising to "diligently [] investigate the scope of [the] incident and its potential impact on [MoviePass's] subscribers."

Complaint

50. Following an investigation into the breach, Respondent MoviePass found that certain personal information of consumers had been exposed between April 25, 2019, and August 20, 2019.

51. According to Respondent MoviePass's analysis, the breach exposed a server containing unencrypted personal information. The unencrypted information contained approximately 28,191 consumers' financial information—i.e., the name on the credit card, the credit card number, the expiration date of credit card, the billing address, and the type of card—and other personal information, including first name, last name, postal address, email address, birth date, gender, geolocation, user reviews, and movies attended.

52. Respondent MoviePass's analysis also indicated that the exposed server was accessed several times from countries where the company does not operate or otherwise have any relationships.

53. This breach was made possible by the failure of Respondents MoviePass and Lowe to take reasonable steps to protect consumers' personal information stored on its network from unauthorized access. In fact, Respondents MoviePass and Lowe engaged in a number of practices that failed to provide reasonable security for consumers' personal information stored on its network. Among other things, Respondents MoviePass and Lowe:

- a. Stored consumers' personal information, including financial information and email addresses in clear text;
- b. Failed to assess the risks to the personal information stored on its network, such as by conducting periodic risk assessments or performing vulnerability and penetration testing of the network;
- c. Failed to maintain and manage security controls that protect and restrict access to consumers' personal information. For example, Respondent MoviePass disabled its firewall and loaded consumers' personal information onto a server in April 2019 in a manner that left the information accessible to any parties with an internet connection;
- d. Failed to provide adequate security training to its employees; and
- e. Failed to implement safeguards to detect anomalous activity and/or cybersecurity events, such as an adequate intrusion prevention or detection system to alert of potentially unauthorized access to Respondent MoviePass's network or servers.

Decision and Order

VIOLATIONS OF THE FTC ACT**Count III – Respondents MoviePass, Helios, and Lowe
Deceptive Failure to Take Reasonable Measures to Protect Consumer Data**

54. As described in Paragraphs 43—45, Respondents MoviePass, Helios, and Lowe have represented, directly or indirectly, expressly or by implication, that they used reasonable administrative, technical, physical, and managerial measures to protect consumers' personal information from unauthorized access.

55. In fact, as set forth in Paragraphs 48—53, Respondents MoviePass, Helios, and Lowe have failed to use reasonable administrative, technical, physical, and managerial measures to protect consumers' personal data from unauthorized access. Therefore, the representations set forth in Paragraph 54 are false or misleading.

VIOLATIONS OF SECTION 5 AND ROSCA

56. The acts and practices of Respondents as alleged in this complaint constitute unfair or deceptive acts or practices, and the making of false advertisements, in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act and Section 4 of the Restore Online Shoppers' Confidence Act.

By the Commission, Commissioner Phillips dissenting.

DECISION

The Federal Trade Commission ("Commission") initiated an investigation of certain acts and practices of the Respondents named in the caption. The Commission's Bureau of Consumer Protection ("BCP") prepared and furnished to Respondents a draft Complaint. BCP proposed to present the draft Complaint to the Commission for its consideration. If issued by the Commission, the draft Complaint would charge the Respondents with violations of the Federal Trade Commission Act.

Respondents and BCP thereafter executed an Agreement Containing Consent Order ("Consent Agreement"). The Consent Agreement includes: 1) statements by Respondents that they neither admit nor deny any of the allegations in the Complaint, except as specifically stated in this Decision and Order, and that only for purposes of this action, they admit the facts necessary to establish jurisdiction; and 2) waivers and other provisions as required by the Commission's Rules.

Decision and Order

The Commission considered the matter and determined that it had reason to believe that Respondents have violated the Federal Trade Commission Act, and that a Complaint should issue stating its charges in that respect. The Commission accepted the executed Consent Agreement and placed it on the public record for a period of 30 days for the receipt and consideration of public comments. The Commission duly considered any comments received from interested persons pursuant to Section 2.34 of its Rules, 16 C.F.R. § 2.34. Now, in further conformity with the procedure prescribed in Rule 2.34, the Commission issues its Complaint, makes the following Findings, and issues the following Order:

Findings

1. The Respondents are:
 - a. Respondent MoviePass, Inc. is a Delaware corporation with its principal place of business at 350 Fifth Avenue, Suite 5330, New York, New York 10118. Respondent MoviePass is a subsidiary of Helios and Matheson Analytics, Inc., which acquired a controlling interest in August 2017 and more than 90 percent of the company by April 2018.
 - b. Respondent Helios and Matheson Analytics, Inc. is a Delaware corporation with its principal place of business also at 350 Fifth Avenue, Suite 5330, New York, New York 10118.
 - c. Respondent Mitchell Lowe is the Chief Executive Officer of Respondent MoviePass. Individually or in concert with others, he controlled or had the authority to control, or participated in the acts and practices of Respondent MoviePass, including those relating to its advertising, marketing, public relations, data security, customer service, and the acts and practices alleged in this complaint. At all times material to this complaint, his principal office or place of business was the same as that of Respondents MoviePass and Helios.
 - d. Respondent Theodore Farnsworth was the Chief Executive Officer of Helios until September 2019. Individually or in concert with others, he controlled or had the authority to control, or participated in the acts and practices of Respondents MoviePass and Helios, including those relating to Respondent MoviePass's advertising, marketing, public relations, customer service, and the acts and practices alleged in this complaint. At all times material to this complaint, his principal office or place of business was the same as that of Respondents MoviePass and Helios.
2. On January 28, 2020, Respondents MoviePass, Inc. and Helios and Matheson Analytics, Inc. filed voluntary petitions for relief under Chapter 7 of the Bankruptcy Code, 11 U.S.C. 701 *et seq.*, in the United States Bankruptcy Court for the Southern District of New York ("Bankruptcy Court"). *See In re MoviePass, Inc.*, Case No.

Decision and Order

20-10244-smb (Bankr. S.D.N.Y. Jan. 28, 2020); *In re Helios and Matheson Analytics, Inc.*, Case No. 20-10242-smb (Bankr. S.D.N.Y. Jan. 28, 2020) (“Bankruptcy Cases”). Alan Nisselson of the firm Windels, Marx, Lane & Mittendorf, LLP was appointed as the trustee (“Bankruptcy Trustee”).

3. If the Bankruptcy Cases are pending as of the date of entry of this Order, then this action against Respondents MoviePass, Inc. and Helios and Matheson Analytics, Inc., including the entry of judgment and enforcement of a judgment other than a money judgment, is not stayed by 11 U.S.C. § 362(a)(1), (2), (3), or (6) because it is an action brought by the Commission to enforce its police and regulatory power as a governmental unit pursuant to 11 U.S.C. § 362(b)(4) and thus falls within an exemption to the automatic stay.
4. The Bankruptcy Trustee is not a Respondent or a party to this Order and is acting solely in his fiduciary capacity as Chapter 7 trustee in the Bankruptcy Cases to bind Respondents MoviePass, Inc. and Helios and Matheson Analytics, Inc. to this Consent Agreement. The Bankruptcy Trustee’s obligations arise, if at all, only if the Bankruptcy Trustee obtains authorization from the Bankruptcy Court to operate the business of such entity pursuant to 11 U.S.C. § 721, or abandons property of the estate of such entity pursuant to 11 U.S.C. § 554, before the Bankruptcy Case is closed. In the event that any obligations arise hereunder, the Bankruptcy Trustee shall have no further obligations under this Order after the Bankruptcy Case is closed, including with respect to any property the Bankruptcy Trustee abandons to effectuate the closing of any such Bankruptcy Case.
5. Notwithstanding the above, no obligations under this Consent Agreement arose by virtue of the Bankruptcy Trustee’s limited operation of the MovieFone business pursuant to that certain Order of the Bankruptcy Court entered on February 26, 2020, which authorized the Bankruptcy Trustee, effective as of January 28, 2020, to continue the operation of the MovieFone business for a limited period until March 31, 2020, pursuant to 11 U.S.C. § 721.
6. The Bankruptcy Trustee has obtained approval from the Bankruptcy Court to enter into this Order and take any and all actions necessary to implement the terms and conditions of this Order applicable to Respondents MoviePass, Inc. and Helios and Matheson Analytics, Inc.
7. The Commission has jurisdiction over the subject matter of this proceeding and over the Respondents, and the proceeding is in the public interest.

Decision and Order

ORDER**Definitions**

For purposes of this Order, the following definitions apply:

- A. “Covered Business” means (1) Corporate Respondents; (2) any business that Corporate Respondents control, directly or indirectly; and (3) any business that Respondent Lowe controls, directly or indirectly, that collects or maintains consumers’ Personal Information.
- B. “Covered Incident” means any instance in which any U.S. federal, state, or local law or regulation requires Respondents to notify any U.S. federal, state, or local government entity that information collected or received, directly or indirectly, by Respondents from or about an individual consumer was, or is reasonably believed to have been, accessed or acquired without authorization.
- C. “Respondents” means all of the Individual Respondents and the Corporate Respondents, individually, collectively, or in any combination.
 - 1. “Corporate Respondents” means MoviePass, Inc., Helios and Matheson Analytics, Inc., and their successors and assigns, *provided that*, for the purposes of Sections II-X of this Order, each of MoviePass, Inc. and Helios and Matheson Analytics, Inc., including their bankruptcy estates, are excluded from the definition of “Respondents” and “Corporate Respondents” for the period from the date of entry of this Order (at which time obligations under this Order arise) until the date the Bankruptcy Case for each such entity is closed, unless the Bankruptcy Trustee obtains authorization from the Bankruptcy Court to operate the business of such entity pursuant to 11 U.S.C. § 721 or abandons property of the estate of such entity pursuant to 11 U.S.C. § 554 before the Bankruptcy Case is closed, in which case Sections II-X of this Order shall apply to such entity as of the date such an event occurs.
 - 2. “Individual Respondents” means Mitchell Lowe and Theodore Farnsworth.
- D. “Personal Information” means individually identifiable information from or about an individual consumer, including:
 - 1. First and last name.
 - 2. Home or other physical address, including street name and name of city or town, or other information about the location of the individual, including but not limited to fine or coarse location or GPS coordinates;

Decision and Order

3. Email address;
4. Telephone number;
5. Date of birth;
6. Social Security number;
7. Other government-issued identification numbers, such as a driver's license number, military identification number, passport number, or other personal identification number;
8. Financial institution account number;
9. Credit or debit card information; or
10. Authentication credentials, such as a username and password.

I. PROHIBITION AGAINST MISREPRESENTATIONS

IT IS ORDERED that Respondents, Respondents' officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with advertising, promotion, offering for sale, or sale of any product or service, are permanently restrained and enjoined from misrepresenting or assisting others in misrepresenting, expressly or by implication:

- A. That the service will allow consumers to view one movie per day at their local movie theaters;
- B. That the service will allow consumers to view any movie, in any theater, at any time;
- C. The total costs to purchase, receive, or use, and the quantity of, any good or service that is the subject of the sales offer;
- D. All material restrictions, limitations, or conditions to purchase, receive, or use the product or service that is subject of the sales offer;
- E. That Respondents will take reasonable administrative technical, physical, or managerial measures to protect consumers' Personal Information from unauthorized access;
- F. The extent to which Respondents otherwise protect the privacy, security, availability, confidentiality, or integrity of Personal Information; or

Decision and Order

- G. Any material fact.

II. MANDATED INFORMATION SECURITY PROGRAM

IT IS FURTHER ORDERED that each Covered Business shall not transfer, sell, share, collect, maintain, or store Personal Information unless it establishes and implements, and thereafter maintains, a comprehensive information security program (“Information Security Program”) that protects the security, confidentiality, and integrity of Personal Information. To satisfy this requirement, each Covered Business must, at a minimum:

- A. Document in writing the content, implementation, and maintenance of the Information Security Program;
- B. Provide the written program and any evaluations thereof or updates thereto to its board of directors or equivalent governing body or, if no such board or equivalent governing body exists, to a senior officer responsible for its Information Security Program at least once every twelve (12) months and promptly (not to exceed thirty (30) days) after a Covered Incident;
- C. Designate a qualified employee or employees to coordinate, oversee, and be responsible for the Information Security Program;
- D. Assess and document, at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following a Covered Incident, internal and external risks to the security, confidentiality, or integrity of Personal Information that could result in the (1) unauthorized collection, maintenance, use, or disclosure of, or provision of access to, Personal Information; or the (2) misuse, loss, theft, alteration, destruction, or other compromise of such information;
- E. Design, implement, maintain, and document safeguards each Covered Business identifies that control for the internal and external risks to the security, confidentiality, or integrity of Personal Information identified in response to sub-Provision II.D. Each safeguard must be based on the volume and sensitivity of the Personal Information that is at risk, and the likelihood that the risk could be realized and result in the (1) unauthorized collection, maintenance, use, or disclosure of, or provision of access to, Personal Information; or the (2) misuse, loss, theft, alteration, destruction, or other compromise of such information. Such safeguards must also include:
 - 1. Training of all its employees, at least once every twelve (12) months, on how to safeguard Personal Information;

Decision and Order

2. Technical measures to monitor of all of its networks and all systems and assets within those networks to identify data security events, including unauthorized attempts to exfiltrate Personal Information from those networks; and
 3. Data access controls for all databases storing Personal Information, including by, at a minimum, (a) restricting inbound connections to approved IP addresses, (b) requiring authentication to access them, and (c) limiting employee access to what is needed to perform that employee's job function;
- F. Assess, at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following a Covered Incident, the sufficiency of any safeguards in place to address the internal and external risks to the security, confidentiality, or integrity of Personal Information, and modify the Information Security Program based on the results;
- G. Test and monitor the effectiveness of the safeguards at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following a Covered Incident, and modify the Information Security Program based on the results. Such testing and monitoring must include vulnerability testing of each of the Covered Business's networks once every four months and promptly (not to exceed thirty (30) days) after a Covered Incident, and penetration testing of each of the Covered Business's networks at least once every twelve (12) months and promptly (not to exceed thirty (30) days) after a Covered Incident;
- H. Select and retain service providers capable of safeguarding Personal Information they access through or receive from each Covered Business, and contractually require service providers to implement and maintain safeguards sufficient to address the internal and external risks to the security, confidentiality, or integrity of Personal Information; and
- I. Evaluate and adjust the Information Security Program in light of any changes to its operations or business arrangements, a Covered Incident, new or more efficient technological or operational methods to control for the risks identified in Provision III.D of this Order, or any other circumstances that any such Covered Business knows or has reason to know may have an impact on the effectiveness of the Information Security Program or any of its individual safeguards. At a minimum, each Covered Business must evaluate the Information Security Program at least once every twelve (12) months and modify the Information Security Program based on the results.

Decision and Order

III. INFORMATION SECURITY ASSESSMENTS BY A THIRD PARTY

IT IS FURTHER ORDERED that, in connection with compliance with Provision II.B of this Order titled Mandated Information Security Program, Respondents must obtain initial and biennial assessments (“Assessments”):

- A. The Assessments must be obtained from a qualified, objective, independent third party professional (“Assessor”), who: (1) uses procedures and standards generally accepted in the profession; (2) conducts an independent review of the Information Security Program; (3) retains all documents relevant to each Assessment for five years after completion of such Assessment, and (4) will provide such documents to the Commission within ten (10) days of receipt of a written request from a representative of the Commission. No documents may be withheld on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney client privilege, statutory exemption, or any similar claim.
- B. For each Assessment, any such Respondent must provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the name, affiliation, and qualifications of the proposed Assessor, whom the Associate Director shall have the authority to approve in her or his sole discretion.
- C. The reporting period for the Assessments must cover: (1) the first 180 days after the issuance date of the Order for the initial Assessment; and (2) each two-year period thereafter for twenty (20) years after issuance of the Order for the biennial Assessments.
- D. Each Assessment must, for the entire assessment period: (1) determine whether such Covered Business has implemented and maintained the Information Security Program required by Provision II of this Order, titled Mandated Information Security Program; (2) assess the effectiveness of such Covered Business’s implementation and maintenance of sub-Provisions II.A—I; (3) identify any gaps or weaknesses in, or instances of material noncompliance with, the Information Security Program; (4) address the status of gaps or weaknesses in, or instances of material non-compliance with, the Information Security Program that were identified in any prior Assessment required by this Order; and (5) identify specific evidence (including, but not limited to, documents reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Assessor examined is (a) appropriate for assessing an enterprise of the Covered Business’s size, complexity, and risk profile; and (b) sufficient to justify the Assessor’s findings. No finding of any Assessment shall rely primarily on assertions or attestations by such Covered Business’s management. The Assessment must be signed by the Assessor, state that the Assessor conducted an independent review of the Information Security Program and did not rely primarily on assertions or

Decision and Order

attestations by such Covered Business's management, and state the number of hours that each member of the assessment team worked on the Assessment. To the extent that such Covered Business revises, updates, or adds one or more safeguards required under Provision II of this Order during an Assessment period, the Assessment must assess the effectiveness of the revised, updated, or added safeguard(s) for the time period in which it was in effect, and provide a separate statement detailing the basis for each revised, updated, or additional safeguard.

- E. Each Assessment must be completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Commission representative in writing, such Respondent must submit the initial Assessment to the Commission within ten (10) days after the Assessment has been completed via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "In re MoviePass, Inc., FTC File No. 1923000." All subsequent biennial Assessments must be retained by Respondents until the order is terminated and provided to the Associate Director for Enforcement within ten days of request.

IV. COOPERATION WITH THIRD-PARTY INFORMATION SECURITY ASSESSOR

IT IS FURTHER ORDERED that each Covered Business, whether acting directly or indirectly, in connection with any Assessment required by Provision III of this Order titled Information Security Assessments by a Third Party, must:

- A. Provide or otherwise make available to the Assessor all information and material in its possession, custody, or control that is relevant to the Assessment for which there is no reasonable claim of privilege;
- B. Provide or otherwise make available to the Assessor information about its network(s) and all of its IT assets so that the Assessor can determine the scope of the Assessment, and visibility to those portions of the network(s) and IT assets deemed in scope; and
- C. Disclose all material facts to the Assessor, and not misrepresent in any manner, expressly or by implication, any fact material to the Assessor's: (1) determination of whether each Covered Business subject to Provisions II and III of this Order has implemented and maintained the Information Security Program required by Provision II of this Order, titled Mandated Information Security Program; (2) assessment of the effectiveness of the implementation and maintenance of sub-Provisions II.A—I; or (3) identification of any gaps or weaknesses in, or instances of material non-compliance with, the Information Security Program.

Decision and Order

V. COVERED INCIDENT REPORTS

IT IS FURTHER ORDERED that Respondents, for any Covered Business, within thirty (30) days after discovery of a Covered Incident must submit a report to the Commission. The report must include, to the extent possible:

- A. The date, estimated date, or estimated date range when the Covered Incident occurred;
- B. A description of the facts relating to the Covered Incident, including the causes of the Covered Incident, if known;
- C. A description of each type of information that triggered the notification obligation to the U.S. federal, state, or local government entity;
- D. The number of consumers whose information triggered the notification obligation to the U.S. federal, state, or local government entity;
- E. The acts that the Covered Business has taken to date to remediate the Covered Incident and protect Personal Information from further exposure or access, and protect affected individuals from identity theft or other harm that may result from the Covered Incident; and
- F. A representative copy of any materially different notice sent by the Covered Business to consumers or to any U.S. federal, state, or local government entity. Unless otherwise directed by a Commission representative in writing, all Covered Incident reports to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "*In re MoviePass, Inc., et al.*, FTC File No. 1923000."

VI. ANNUAL CERTIFICATION

IT IS FURTHER ORDERED that each Covered Business must:

- A. One year after the issuance date of this Order, and each year thereafter, provide the Commission with a certification from a senior corporate manager, or if no such senior corporate manager exists, a senior officer, of each Covered Business responsible for such Covered Business's Information Security Program that: (1) the Covered Business has established, implemented, and maintained the requirements of this Order; (2) the Covered Business is not aware of any material non-compliance that has not been (a) corrected or (b) disclosed to the Commission; and (3) includes a brief description of all Covered Incidents during the certified period. The certification must be based on the personal knowledge of the senior corporate

Decision and Order

manager, senior officer, or subject matter experts upon whom the senior corporate manager or senior officer reasonably relies in making the certification.

- B. Unless otherwise directed by a Commission representative in writing, submit all annual certifications to the Commission pursuant to this Order via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, “In re *MoviePass, Inc., et al.*, FTC File No. 1923000.”

VII. ACKNOWLEDGMENTS OF THE ORDER

IT IS FURTHER ORDERED that Respondents obtain acknowledgments of receipt of this Order:

- A. Each Respondent, within 10 days after the effective date of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.
- B. For 20 years after the issuance date of this Order, each Individual Respondent for any business that such Respondent, individually or collectively with any other Respondents, is the majority owner or controls directly or indirectly, and each Corporate Respondent, must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees having managerial responsibilities for conduct related to the subject matter of the Order and all agents and representatives who participate in conduct related to the subject matter of the Order; and (3) any business entity resulting from any change in structure as set forth in the Provision titled Compliance Reports and Notices. Delivery must occur within 10 days after the effective date of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.
- C. From each individual or entity to which a Respondent delivered a copy of this Order, that Respondent must obtain, within 30 days, a signed and dated acknowledgment of receipt of this Order.

VIII. COMPLIANCE REPORTS AND NOTICES

IT IS FURTHER ORDERED that Respondents make timely submissions to the Commission:

- A. One year after the issuance date of this Order, each Respondent must submit a compliance report, sworn under penalty of perjury, in which:

Decision and Order

1. Each Respondent must: (a) identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission, may use to communicate with Respondent; (b) identify all of that Respondent's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (c) describe the activities of each business, including the goods and services offered, the means of advertising, marketing, and sales, and the involvement of any other Respondent (which Individual Respondents must describe if they know or should know due to their own involvement); (d) describe in detail whether and how that Respondent is in compliance with each Provision of this Order, including a discussion of all of the changes the Respondent made to comply with the Order; and (e) provide a copy of each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.
 2. Additionally, each Individual Respondent must: (a) identify all his telephone numbers and all his physical, postal, email and Internet addresses, including all residences; (b) identify all his business activities, including any business for which such Respondent performs services whether as an employee or otherwise and any entity in which such Respondent has any ownership interest; and (c) describe in detail such Respondent's involvement in each such business activity, including title, role, responsibilities, participation, authority, control, and any ownership.
- B. Each Respondent must submit a compliance notice, sworn under penalty of perjury, within 14 days of any change in the following:
1. Each Respondent must submit notice of any change in: (a) any designated point of contact; or (b) the structure of any Corporate Respondent or any entity that Respondent has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.
 2. Additionally, each Individual Respondent must submit notice of any change in: (a) name, including alias or fictitious name, or residence address; or (b) title or role in any business activity, including (i) any business for which such Respondent performs services whether as an employee or otherwise and (ii) any entity in which such Respondent has any ownership interest and over which Respondents have direct or indirect control. For each such business activity, also identify its name, physical address, and any Internet address.

Decision and Order

- C. Each Respondent must submit notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against such Respondent within 14 days of its filing.
- D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: “I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: “_____” and supplying the date, signatory’s full name, title (if applicable), and signature.
- E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: *In re MoviePass, Inc., et al.*, FTC File No. 1923000.

IX. RECORDKEEPING

IT IS FURTHER ORDERED that Respondents must create certain records for 20 years after the issuance date of the Order, and retain each such record for 5 years. Specifically, each Corporate Respondent, in connection with any conduct related to the subject matter of the Order, and each Individual Respondent for any business that such Respondent, individually or collectively with any other Respondents, is a majority owner or controls directly or indirectly, must create and retain the following records:

- A. Accounting records showing the revenues from all goods or services sold, the costs incurred in generating those revenues, and resulting net profit or loss;
- B. Personnel records showing, for each person providing services in relation to any aspect of the Order, whether as an employee or otherwise, that person’s: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;
- C. Copies or records of all consumer complaints and refund requests, whether received directly or indirectly, such as through a third party, and any response;
- D. All records necessary to demonstrate full compliance with each provision of this Order, including all submissions to the Commission; and
- E. A copy of each unique advertisement or other marketing material making a representation subject to this Order.

Decision and Order

X. COMPLIANCE MONITORING

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondents' compliance with this Order:

- A. Within 10 days of receipt of a written request from a representative of the Commission, each Respondent must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury, and produce records for inspection and copying.
- B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with each Respondent. Respondents must permit representatives of the Commission to interview anyone affiliated with any Respondent who has agreed to such an interview. The interviewee may have counsel present.
- C. The Commission may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Respondents or any individual or entity affiliated with Respondents, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.
- D. Upon written request from a representative of the Commission, any consumer reporting agency must furnish consumer reports concerning Individual Respondents, pursuant to Section 604(2) of the Fair Credit Reporting Act, 15 U.S.C. § 1681b(a)(2).

XI. ORDER EFFECTIVE DATES

IT IS FURTHER ORDERED that this Order is final and effective upon the date of its publication on the Commission's website (ftc.gov) as a final order. This Order will terminate 20 years from the date of its issuance (which date may be stated at the end of this Order, near the Commission's seal), or 20 years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

- A. Any Provision in this Order that terminates in less than 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 Provision.

Concurring Statement

Provided, further, that if such complaint is dismissed or a federal court rules that the 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 will terminate according to this Provision 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 Phillips dissenting.

CONCURRING STATEMENT OF COMMISSIONER CHRISTINE S. WILSON

I support the complaint and consent in this matter challenging the respondents' marketing of its movie subscription product. Specifically, the respondents offered subscribers "unlimited movies" but deployed a variety of tactics to prevent consumers from enjoying unlimited benefits, as recounted in the complaint, rendering the representations deceptive. I also concur with the inclusion of a count challenging violations of the Restore Online Shoppers' Confidence Act, 15 U.S.C. § 8403 (ROSCA). The conduct alleged in this case, in my view, violates the plain language of the statute.

Section 8403 of ROSCA states that:

It shall be unlawful for any person to charge or attempt to charge any consumer for any goods or services sold in a transaction effected on the Internet through a negative option feature (as defined in the Federal Trade Commission's Telemarketing Sales Rule in part 310 of title 16, Code of Federal Regulations), unless the person—

- (1) provides text that clearly and conspicuously discloses all material terms of the transaction before obtaining the consumer's billing information;
- (2) obtains a consumer's express informed consent before charging the consumer's credit card, debit card, bank account, or other financial account for products or services through such transaction; and
- (3) provides simple mechanisms for a consumer to stop recurring charges from being placed on the consumer's credit card, debit card, bank account, or other financial account.

Concurring Statement

The TSR defines “negative option feature” as “an offer or agreement to sell or provide any goods or services, a provision under which the customer’s silence or failure to take an affirmative action to reject goods or service or to cancel the agreement is interpreted by the seller as acceptance of the offer.” 16 C.F.R. §310.2(w).

MoviePass Unlimited was a month-to-month arrangement that consumers could cancel at any time. The FTC for decades has interpreted these types of recurring agreements as negative option plans. Each month, the consumer’s failure to cancel implies consent to be charged for an additional month. In other words, the seller obtains consent for the recurring charge using a negative option.

The “unlimited” aspect of the MoviePass subscription constituted a material term of the pass that the company marketed and sold. Notably, as alleged in the complaint, MoviePass highlighted this term as a primary selling point – touting “MoviePass Unlimited” and stating “Enjoy a new movie every day.” MoviePass did not disclose that it would prevent consumers from actually viewing one movie per day or that it would implement ticket verification procedures to frustrate consumers’ attempts to use their passes, as described in the Commission’s complaint. In essence, MoviePass throttled subscribers’ movie consumption. The terms or limits to the purportedly unlimited subscription that were employed to achieve this throttling effect almost certainly would be considered material to consumers’ decisions to purchase the subscription.

ROSCA Section 8403 plainly states that for goods or services sold through a negative option feature, the seller must “clearly and conspicuously disclose all material terms of the transaction.” The respondents here did not disclose all material terms. Therefore, these facts, as alleged, in my view support a violation of ROSCA.

I am mindful that this settlement marks the first time the Commission has alleged a violation of ROSCA where the undisclosed material terms do not relate specifically to the negative option feature but instead to the underlying good or service marketed through that feature. But I believe that the facts of this case fall well within the bounds of the conduct that Congress contemplated challenging when promulgating the statute. In fact, the conduct described in the complaint fits neatly within the plain language of the statute.

Given the inaugural use of ROSCA for this purpose, it is appropriate that the Commission is foregoing civil penalties. Businesses need predictability about the manner in which laws will be enforced and should be afforded the ability to contest new uses of authority. This case will serve as notice to the market, and future violations of this type may well warrant civil penalties.

The Supreme Court’s recent decision in *AMG*¹ has eliminated the FTC’s ability to seek equitable monetary relief under Section 13(b) of the FTC Act to compensate consumers. The temptation to test the limits of our remaining sources of authority is likely to be strong. On numerous occasions, I have expressed concern about novel interpretations of our authority that

¹ *AMG v. FTC*, slip op No. 19-508 (Apr. 22, 2021), https://www.supremecourt.gov/opinions/20pdf/19-508_l6gn.pdf.

Dissenting Statement

exceed the boundaries of underlying statutes and corresponding Congressional intent.² And I will scrutinize carefully any future attempts to expand ROSCA, or any other authority entrusted to the Commission, beyond the plain language. Here, however, I am satisfied that the challenged conduct falls well within the four corners of the statute and therefore conclude that, under the facts alleged, including a ROSCA count is not an overreach.

DISSENTING STATEMENT OF COMMISSIONER NOAH JOSHUA PHILLIPS

The Commission's decision in this case to plead a novel theory of liability under the Restore Online Shoppers' Confidence Act of 2010 ("ROSCA") accomplishes nothing for consumers and reduces clarity for businesses seeking to follow the law. I respectfully dissent.

Congress enacted ROSCA to protect consumers from aggressive sales tactics on the Internet. In so doing, it expressed particular concern about the practice of reputable online retailers sharing their customers' information with third party sellers ("post-transaction third party sellers"), who in turn "used aggressive, misleading sales tactics" to charge millions of unwitting American consumers for goods and services.¹ Consumers didn't know what they were being charged for and had no way to stop recurring charges. Congress found that these sales tactics undermined consumer confidence in the Internet and harmed the American economy.²

The crux of the statutory regime set forth in ROSCA is to require disclosures in two particular circumstances. The first deals specifically with post-transaction third party sellers that, unbeknownst to consumers, receive consumers' financial information and charge them for goods or services, making it impossible for consumers to figure out what they were being charged for or

² Statement of Commissioner Christine S. Wilson Concurring in Part, Dissenting in Part, Notice of Proposed Rulemaking related to Made in USA Claims (June 22, 2020) (expressing concern that the proposed rule exceeds the scope of authority Congress granted the FTC), https://www.ftc.gov/system/files/documents/public_statements/1577099/p074204musawilsonstatementrev.pdf; Separate Statement of Commissioner Christine S. Wilson Concurring in Part, Dissenting in Part, *FTC v. Avant, LLC* (Apr. 15, 2019) (dissenting with respect to the maiden use of the Telemarketing Sales Rule (TSR) provision related to novel payments (specifically remotely created checks) in a non-fraud case), https://www.ftc.gov/system/files/documents/public_statements/1514073/avant_inc_1623090_separate_statement_of_christine_s_wilson_4-15-19.pdf. In the *Avant* matter, the Commission sought to impose liability under the TSR against a legitimate company, selling legitimate products, in circumstances not contemplated when the Rule was promulgated to address fraudulent businesses abusing these types of payments. *Id.*

¹ 15 U.S.C. § 8401(4).

² 15 U.S.C. § 8401(3).

Dissenting Statement

how to stop it.³ Accordingly, under Section 8402, these post-transaction third party sellers cannot charge or attempt to charge a consumer's financial account for any good or service sold in an Internet transaction unless, before obtaining the consumer's billing information, they clearly and conspicuously disclose all material terms of the transaction. The statute defines these terms to include: a description of the goods or services being offered; the fact that such seller is not affiliated with the initial merchant; and the cost of such goods or services.⁴ The post-transaction third party seller must also obtain express informed consent from the consumer. That scenario is not at issue here.

The second circumstance is when *any* seller uses a negative option feature, one of the aggressive tactics that Congress found third-party sellers employed. Here ROSCA also requires specific upfront disclosures. Under Section 8403, before charging a consumer for goods or services sold through a negative option feature,⁵ the seller must: (i) clearly and conspicuously disclose "all material terms of the transaction" before obtaining the consumer's billing information; (ii) obtain express informed consent from the consumer before charging the consumer's financial account; and (iii) provide a simple mechanism for the consumer to stop the recurring charges.⁶ Section 8403 does not define which terms must be disclosed, or make clear whether the disclosure obligation applies to the negative option feature or that feature as well as the underlying product.

In selling its services to consumers, MoviePass used a negative option feature. Consumers interacted directly with MoviePass and were aware that they were purchasing a service from MoviePass and were agreeing to recurring charges. The complaint does not allege that MoviePass failed to provide a simple mechanism to cancel the recurring charge or that any ROSCA violation took place for the majority of its consumers.

Liability here is instead predicated on the fact that, when it became apparent its business model was not working because some customers were going to too many movies, MoviePass began throttling high-volume users of its service and potentially reducing their ability to screen movies on a truly "unlimited" basis and failed to disclose this to new consumers. This is deception, and it violates Section 5 of the FTC Act. But the complaint also fashions MoviePass's failure to disclose affirmatively that it would throttle certain high-volume users of its service as a failure to clearly and conspicuously disclose all material terms of the transaction before obtaining the consumer's billing information under ROSCA.⁷

³ As set forth in ROSCA's Findings and Declaration of Policy section, in exchange for "bounties" and other payments, hundreds of reputable online retailers and websites shared their customers' billing information, including credit card and debit card numbers, with third party sellers through a process known as "data pass". 15 U.S.C. § 8401. This practice is not at issue here.

⁴ 15 U.S.C. § 8402(a).

⁵ ROSCA incorporates the definition of negative option feature from the Telemarketing Sales Rule, 16 C.F.R. § 310.2(w): Negative option feature means, in an offer or agreement to sell or provide any goods or services, a provision under which the customer's silence or failure to take an affirmative action to reject goods or services or to cancel the agreement is interpreted by the seller as acceptance of the offer.

⁶ 15 U.S.C. § 8403.

⁷ Likewise, this means that MoviePass did not obtain express informed consent.

Dissenting Statement

The novelty here is that, for the first time, the Commission is treating a deception about the characteristics of the underlying product—not the negative option feature—as a violation of ROSCA. To date, all the complaints filed by the Commission that allege ROSCA violations in the negative option context with a first party seller have involved defendants hiding a negative option feature, not obtaining express informed consent before charging the consumer, or failing to provide a simple mechanism for cancelling the recurring charge.⁸ Instead of examining whether consumers understood the negative option feature, had given consent to that, or were able to cancel in a simple way, this complaint instead looks to the characteristics of the product that MoviePass sold to its some of its consumers.

The Commission is thus announcing that it may seek civil penalties against all businesses that online negative option features where the Commission determines that there has been any material deception, whether relating to the negative option feature or a characteristic of the underlying product. I have several concerns with this approach.

First, pleading this new theory accomplishes nothing here. One benefit of establishing liability for rule violations is to obtain a penalty. But the corporate respondents are in bankruptcy and the individual respondents are settling these allegations in a no-money order. The relief we obtain today is no different than if we proceeded without a ROSCA count. Including a ROSCA count does nothing for consumers in terms of monetary or injunctive relief. That makes our announcement of sweeping new liability and introduction of a lack of clarity to the market about required disclosures, discussed below, ill-advised.

Second, while not facially-implausible, the statutory interpretation pushed by the Commission in this case is far from obvious. Section 8403 concerns “negative option marketing” and speaks specifically to, *inter alia*, “goods or services sold in a transaction effected on the Internet through a negative option feature”. The negative option is the aggressive tactic that Congress was concerned about, and the statutory requirements of disclosure of terms, consent to collection of financial information, and simple cancellation protect specifically against its abuse. But there is nothing in the statute—and little, for that matter, in the legislative history—to suggest congressional intent to regulate disclosures about the products or services being sold, as opposed to disclosures about the negative option.

Section 8402, concerning third-party post-transaction sellers, provides an important contrast. There, Congress specifically delineated the terms that sellers were obligated to disclose, including defining “material terms” to include “a description of the goods or services”. Section 8403, addressing negative options, does not include that language. (So the Commission reads the words into the statute.) A heightened requirement for post-transaction third party sellers makes

⁸ For example, in *FTC v. Triangle Media Corporation*, consumers were offered a free trial but were charged as much as \$98.71 for the trial shipment, and also were enrolled in a negative-option continuity plan without their consent. Defendants also used deceptive order confirmation pages to trick consumers into ordering additional products, for which the defendants similarly charged consumers full price and enrolled them in negative-option plans. The defendants then made it difficult to cancel the continuity plan, stop or avoid the recurring charges, or obtain a refund. *FTC v. Triangle Media Corp.*, No. 18cv1388-MMA (NLS), 2018 WL 4051701 (S.D. Cal. Aug. 24, 2018).

Dissenting Statement

sense. Where the consumer is not aware of the transaction at all, disclosures about the product are essential. But where the consumer is aware they are buying the product—but not the negative option that will continue charging them over time—the justification for compelling disclosure about the product is less clear.⁹ What is more, because Congress specifies certain material terms in Section 8402 but not Section 8403, the scope of the obligation the Commission adopts—regarding “all material terms”, whatever a majority of FTC Commissioners might deem those to be—would impose fewer disclosure obligations on post-transaction third party sellers than on businesses that use negative options. There is simply no justification for that.

Third, the Commission fails to announce today precisely what it believes are the “material terms”, reducing clarity for businesses about their disclosure obligations. ROSCA creates affirmative disclosure obligations, but we have given no guidance to businesses about what to disclose.¹⁰ Instead, the Commission now declares—in a settlement with two bankrupt companies and two individuals, none of whom will pay anything—that failing to disclose a product characteristic that the Commission later deems material exposes a business to substantial civil penalties. At the very least, before putting this new theory into action, the Commission should issue guidance to companies as to their disclosure obligations.

The Commission’s decision dramatically to re-interpret ROSCA and expand liability comes just weeks after the Supreme Court’s decision in *AMG Capital Management, LLC v. FTC*, which held that equitable monetary relief is not available under Section 13(b) of the FTC Act.¹¹ I believe Congress should amend the statute. But I do not agree that our loss of authority under one statute somehow creates authority elsewhere. While equitable relief is not intended to be penal, my colleagues have touted the triggering of rule penalties as an alternative because they deprive the defendant of money.¹² But even to the extent one takes the view that a rule violation occurred here, and leaving aside the lack of clarity the Commission today creates, the reader should keep in mind that the respondents are not paying any money here at all.

I therefore dissent.

⁹ Other than in specific congressionally-delineated contexts, the FTC does not have civil penalty authority in the first instance for deception in the sale of products or services.

¹⁰ In fact, the Commission did not even raise this issue in its recent rulemaking proposal concerning negative options. See Rules Concerning the Use of Prenotification Negative Option Plans, Advance Notice of Proposed Rulemaking and Request for Public Comment, 84 Fed. Reg. 52393, Oct. 2, 2019.

¹¹ See *AMG Capital Mgmt., LLC v. FTC*, No. 19-508, 593 U.S. ___, slip op. (Apr. 22, 2021), https://www.supremecourt.gov/opinions/20pdf/19-508_l6gn.pdf.

¹² See, e.g., *The Consumer Protection and Recovery Act: Returning Money to Defrauded Consumers*, Hearing on H.R. 2668 Before the Subcomm. on Consumer Prot. and Com. of the H. Comm. on Energy and Com., 117th Cong. 3 (2021) (statement of Rebecca Kelly Slaughter, Acting Chairwoman, Fed. Trade Comm’n).

Analysis to Aid Public Comment

ANALYSIS OF CONSENT ORDER TO AID PUBLIC COMMENT

The Federal Trade Commission (“FTC” or “Commission”) has accepted, subject to final approval, an agreement containing a proposed consent order (“Proposed Order”) from MoviePass, Inc., a corporation, Helios and Matheson Analytics, Inc. (“Helios”), a corporation, Mitchell Lowe, individually and as an officer of MoviePass, Inc., and Theodore Farnsworth, individually and as an officer of Helios (“Respondents”). The Proposed Order has been placed on the public record for 30 days to receive comments by interested persons. Comments received during this period will become part of the public record. After 30 days, the Commission will again review the agreement and the comments received and will decide whether it should withdraw from the agreement and take appropriate action or make final the agreement’s Proposed Order.

This matter involves Respondents’ advertising, promotion and sale of the movie-viewing subscription service “MoviePass,” which offered consumers access to one movie per day at their local movie theaters for a monthly subscription price. The FTC complaint challenges two aspects of Respondents’ marketing of MoviePass:

First, the complaint alleges that Respondents’ offer of one movie per day was deceptive due to several measures Respondents took to prevent consumers from using the service as promised—measures that included invalidating certain consumers’ passwords, adding a difficult and defective ticket verification procedure to view movies, and placing undisclosed usage caps on frequent users.

The complaint alleges that this conduct violated two laws the FTC enforces. First, the FTC alleges the conduct to be a “deceptive act[] or practice[]” that violates Section 5(a) of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 45(a). The conduct described above was deceptive because Respondents engaged in it to prevent consumers from using MoviePass once per day as advertised. Second, the FTC alleges that Respondents violated the Restore Online Shoppers’ Confidence Act (“ROSCA”), 15 U.S.C. § 8403, through the same conduct by failing to disclose the steps that they took to prevent consumers from using MoviePass once per day. This failure violated ROSCA in two ways—by failing to disclose all material terms of the transaction as required by 15 U.S.C. § 8403(1) and by failing to secure consumers’ express informed consent to the transaction before charging their financial accounts as required by 15 U.S.C. § 8403(2).

In addition to the deceptive marketing of MoviePass’s “one movie per day” service, the complaint further alleges that Respondents MoviePass, Inc., Helios, and Lowe misrepresented the data security measures they took to protect consumers’ personal information against unauthorized access. The complaint alleges that Respondents’ actions constitute unfair or deceptive acts or practices and the making of false advertisements, in violation of Section 5(a) of the FTC Act.

The Proposed Order is designed to prevent Respondents from engaging in similar acts or practices in the future. It includes injunctive relief to address these alleged violations and to prohibit similar and related conduct:

Analysis to Aid Public Comment

Part I prohibits Respondents from future misrepresentations similar to those at issue in the complaint by prohibiting them from misrepresenting that:

- A service will allow consumers to view one movie per day at their local theaters;
- A service will allow consumers to view any movie, in any theater, at any time; and
- Respondents will take reasonable administrative, technical, physical, or managerial measures to protect consumers' personal information from unauthorized access.

Part I also features ancillary relief relating to the challenged conduct by prohibiting misrepresentations relating to (1) the total costs to purchase, receive, or use, and the quantity of, any good or service, (2) any material restrictions, limitations, or conditions to purchase, receive, or use the product or service, (3) the extent to which Respondents otherwise protect the privacy, security, availability, confidentiality, or integrity of consumers' personal information, and (4) any other material fact.

Parts II—VI provide ancillary relief relating to the data security practices of MoviePass, Inc., Helios, and Lowe. The provisions thus only apply to businesses these three respondents operate.

- Part II requires a comprehensive information security program for any enterprise that collects consumers' personal information, requiring among other things:
 - That the information security program contain safeguards that are based on the volume and sensitivity of the personal information at risk;
 - That testing and monitoring of the safeguards are conducted regularly but no less often than once a year; and
 - That the information security program be documented, evaluated, and adjusted in light of any changes to business operations or new technological advancements.
- Parts III and IV respectively require the three respondents (1) to obtain an initial and then biennial third-party information security assessments and (2) to cooperate with the third parties conducting the assessments.
- Part V requires the three respondents to report to the Commission any event involving consumers' personal information that constitutes a reportable event to any U.S. federal, state, or local government authority.

Analysis to Aid Public Comment

- Part VI mandates that the three respondents submit an annual certification regarding their compliance with the Proposed Order's data security requirements.

Parts VII through XI are reporting and compliance provisions. Part VII mandates that all Respondents acknowledge receipt of the Proposed Order and, for 20 years, distribute the Proposed Order to certain employees and agents and secure acknowledgments from recipients of the Proposed Order. Part VIII requires that Respondents submit compliance reports to the FTC one year after the order's issuance and submit additional reports when certain events occur. Part IX requires that, for 20 years, Respondents create certain records and retain them for at least 5 years. Part X provides for the FTC's continued compliance monitoring of Respondents' activity during the Proposed Order's effective dates. Part XI is a provision "sunsetting" the Proposed Order after 20 years, with certain exceptions. Respondents MoviePass, Inc. and Helios are exempt from Sections II—X of the Proposed Order until their bankruptcy cases are closed, and these bankruptcies led the FTC to not seek a monetary judgment in this matter.

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 complaint or Proposed Order, or to modify in any way the Proposed Order's terms.

Complaint

IN THE MATTER OF

**TRAFFIC JAM EVENTS, LLC.
AND
DAVID J. JEANSONNE II**

COMPLAINT AND FINAL ORDER IN REGARD TO ALLEGED VIOLATIONS OF SECTION 5 OF THE
FEDERAL TRADE COMMISSION ACT AND SECTION 144 OF THE TRUTH IN LENDING ACT

*Docket No. 9395; File No. X200041
Complaint, August 7, 2020 – Decision, October 25, 2021*

This order addresses Traffic Jam Events, LLC.’s advertisements for the sale of motor vehicles on behalf of auto dealerships. The complaint alleges that Traffic Jam Events, LLC. deceptively represented that consumers are receiving COVID-19 stimulus relief from the federal government and that consumers have won a prize which can be collected by visiting a particular motor vehicle dealership where no prize was available. The complaint also alleges that Respondent failed to disclose or failed to disclose clearly and conspicuously the terms for close-end credit transactions. Under the order Respondent is prohibited from advertising, marketing, promoting, selling, or leasing automobiles and prohibits misrepresentation in any future marketing that violates the FTC or Truth in Lending Acts.

Participants

For the *Commission*: Michael Tankersley and Sanya Shahrabi

For the *Respondents*: L. Etienne Balart [Jones Walker LLP]

COMPLAINT

The Federal Trade Commission, having reason to believe that Traffic Jam Events, LLC, a limited liability company, and David J. Jeansonne II, individually and as an officer of Traffic Jam Events, LLC (collectively, “Respondents”), have violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Traffic Jam Events, LLC (“Traffic Jam Events”) is a Louisiana limited liability company with its principal place of business at 2232 Idaho Avenue, Kenner, LA 70062.
2. Respondent David J. Jeansonne II, is the owner, managing member, and president of Traffic Jam Events, LLC. Individually or in concert with others, he controlled, had the authority to control, or participated in the acts and practices of Traffic Jam Events, including the acts and practices alleged in this complaint. His principal office or place of business is the same as that of Traffic Jam Events.
3. Respondents have advertised, marketed, promoted, or offered for sale or lease, and sold or leased motor vehicles for or on behalf of auto dealerships nationwide. Respondents create advertising, offer direct mail marketing services, and staff tent sales events to automotive dealerships.