

**UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION**

COMMISSIONERS: **Lina M. Khan, Chair**
 Noah Joshua Phillips
 Rohit Chopra
 Rebecca Kelly Slaughter
 Christine S. Wilson

In the Matter of

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.**

DOCKET NO. C-4751

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

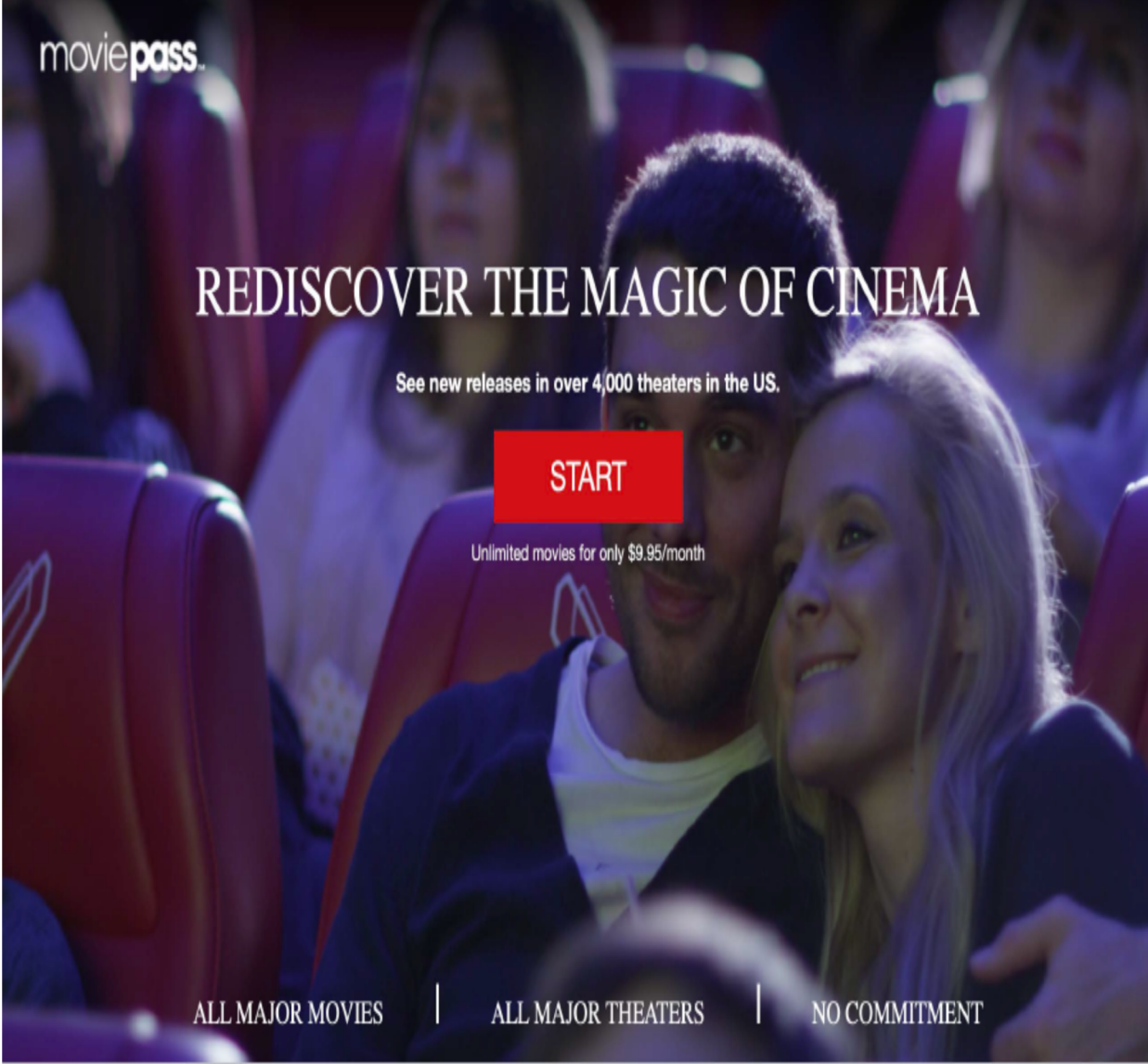
1. Respondent MoviePass, Inc. is a Delaware corporation with its principal place of business at 350 Fifth Avenue, Suite 5330, New York, New York 10118. Respondent MoviePass is a subsidiary of Helios and Matheson Analytics, Inc., which acquired a controlling interest in August 2017 and more than 90 percent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

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:



The advertisement features a background image of a man and a woman sitting in a theater, looking towards the camera. The man is in the foreground, and the woman is slightly behind him. They are both smiling. The theater seats are red. The overall lighting is dim, typical of a movie theater.

moviepass.

REDISCOVER THE MAGIC OF CINEMA

See new releases in over 4,000 theaters in the US.

START

Unlimited movies for only \$9.95/month

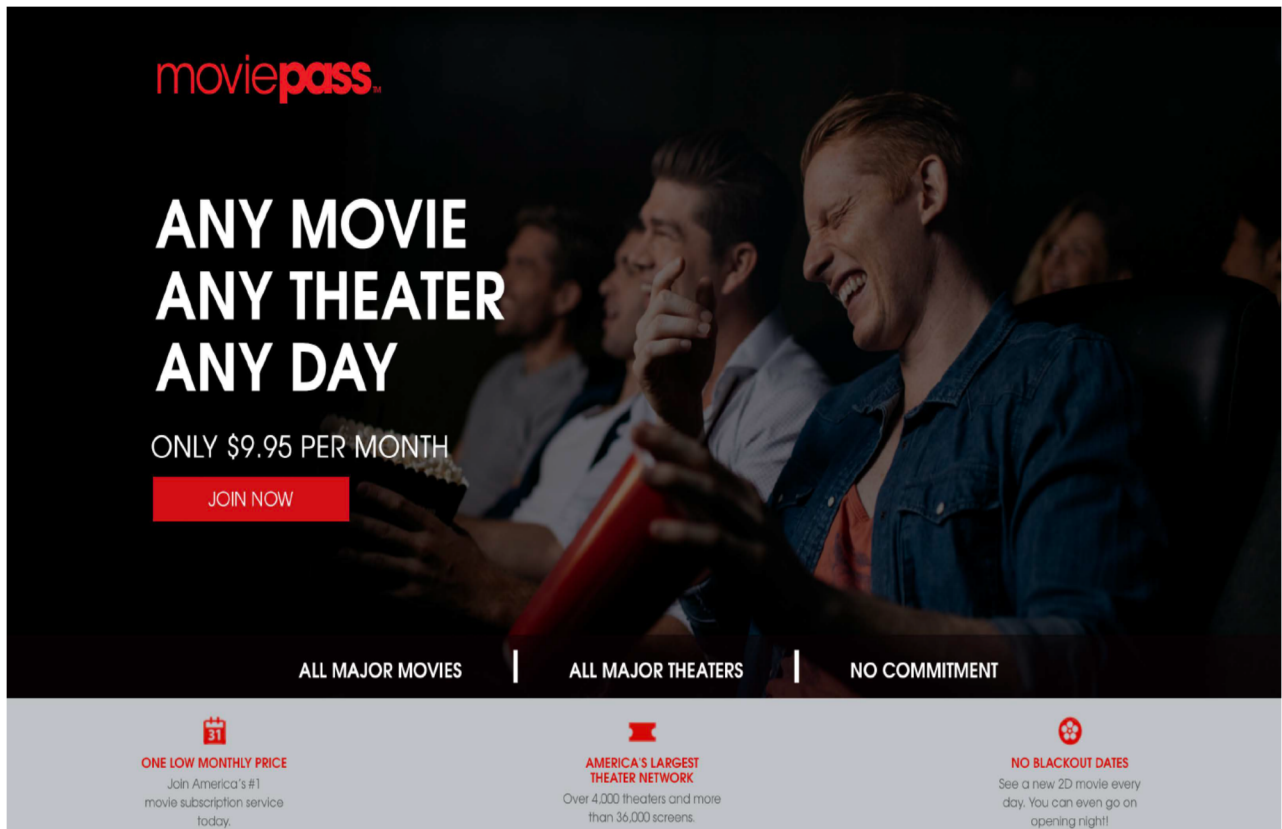
ALL MAJOR MOVIES | ALL MAJOR THEATERS | NO COMMITMENT

ONE LOW MONTHLY PRICE
Join America's #1 movie subscription service today.

AMERICA'S LARGEST THEATER NETWORK
Over 4,000 theaters and more than 36,000 screens.

NO BLACKOUT DATES
See a new 2D movie every day. You can even go on opening night!

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

A promotional banner for MoviePass. The background is dark with a photo of people in a theater. The text is white and red. The top left has the 'moviepass' logo. The main headline reads 'ANY MOVIE ANY THEATER ANY DAY' in large white letters. Below it, 'ONLY \$9.95 PER MONTH' is written in white. A red button with 'JOIN NOW' is positioned below the price. At the bottom, three white text boxes are separated by vertical lines: 'ALL MAJOR MOVIES', 'ALL MAJOR THEATERS', and 'NO COMMITMENT'. Below these are three red icons with corresponding text: a calendar icon for 'ONE LOW MONTHLY PRICE', a theater icon for 'AMERICA'S LARGEST THEATER NETWORK', and a calendar with a red 'X' for 'NO BLACKOUT DATES'.

moviepass.

**ANY MOVIE
ANY THEATER
ANY DAY**

ONLY \$9.95 PER MONTH

JOIN NOW

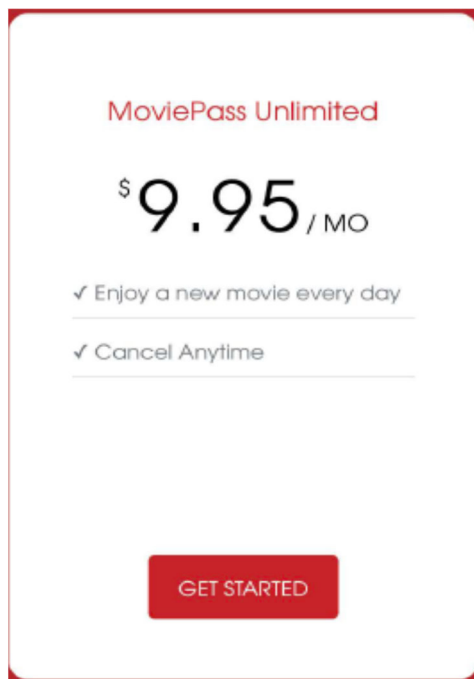
ALL MAJOR MOVIES | ALL MAJOR THEATERS | NO COMMITMENT

ONE LOW MONTHLY PRICE
Join America's #1 movie subscription service today.

AMERICA'S LARGEST THEATER NETWORK
Over 4,000 theaters and more than 36,000 screens.

NO BLACKOUT DATES
See a new 2D movie every day. You can even go on opening night!

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

A white rectangular card with a red border. At the top, 'MoviePass Unlimited' is written in red. Below that, '\$9.95 / MO' is displayed in large black font. Underneath are two checkmarks with the text 'Enjoy a new movie every day' and 'Cancel Anytime'. At the bottom center is a red button with 'GET STARTED' in white.

MoviePass Unlimited

\$9.95 / MO

✓ Enjoy a new movie every day

✓ Cancel Anytime

GET STARTED

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.
 - 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.

- 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."
 - 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.
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.
 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.
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:
- 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."
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.

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.

THEREFORE, the Federal Trade Commission this 1st day of October, 2021, has issued this Complaint against Respondents.

By the Commission, Commissioner Phillips dissenting.



April J. Tabor
Secretary

SEAL: