UNITED STATES OF AMERICA
Before the
SECURITIES AND EXCHANGE COMMISSION

SECURITIES EXCHANGE ACT OF 1934
Release No. 104255 / November 25, 2025

INVESTMENT ADVISERS ACT OF 1940
Release No. 6928 / November 25, 2025

ADMINISTRATIVE PROCEEDING
File No. 3-22562

In the Matter of **M HOLDINGS SECURITIES, INC.** **Respondent.**	**ORDER INSTITUTING ADMINISTRATIVE AND CEASE-AND-DESIST PROCEEDINGS PURSUANT TO SECTIONS 15(b) AND 21C OF THE SECURITIES EXCHANGE ACT OF 1934 AND SECTIONS 203(e) AND 203(k) OF THE INVESTMENT ADVISERS ACT OF 1940, MAKING FINDINGS, AND IMPOSING REMEDIAL SANCTIONS AND A CEASE-AND-DESIST ORDER**

I.

The Securities and Exchange Commission ("Commission") deems it appropriate and in the public interest that public administrative and cease-and-desist proceedings be, and hereby are, instituted pursuant to Sections 15(b) and 21C of the Securities Exchange Act of 1934 (the "Exchange Act"), and Sections 203(e) and 203(k) of the Investment Advisers Act of 1940 (the "Advisers Act"), against M Holdings Securities, Inc. ("M Holdings" or "Respondent").

II.

In anticipation of the institution of these proceedings, Respondent has submitted an Offer of Settlement (the "Offer") which the Commission has determined to accept. Solely for the purpose of these proceedings and any other proceedings brought by or on behalf of the Commission, or to which the Commission is a party, and without admitting or denying the findings herein, except as to the Commission's jurisdiction over it and the subject matter of these proceedings, which are admitted, Respondent consents to the entry of this Order Instituting Administrative and Cease-and-Desist Proceedings Pursuant to Sections 15(b) and 21C of the Securities Exchange Act of 1934 and Sections 203(e) and 203(k) of the Investment Advisers Act of 1940, Making Findings, and Imposing Remedial Sanctions and a Cease-and-Desist Order ("Order"), as set forth below.

III.

On the basis of this Order and Respondent's Offer, the Commission finds[1] that:

Summary

1. These proceedings arise out of M Holdings' failure to adopt written policies and procedures reasonably designed to protect customer records and information, in violation of Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30(a)) (the "Safeguards Rule"), and M Holdings' failure to develop and implement a written Identity Theft Prevention Program as required by Rule 201 of Regulation S-ID (17 C.F.R. § 248.201) (the "Identity Theft Red Flags Rule"), between July 2019 and March 2024 (the "Relevant Period").

2. The Safeguards Rule required, during the Relevant Period, every broker-dealer and every investment adviser registered with the Commission to adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information. Those policies and procedures must be reasonably designed to: (1) ensure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (3) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

3. M Holdings provides brokerage and investment advisory services through a nationwide network of registered representatives and investment adviser representatives (collectively, "representatives") who operate out of 120 branch offices known as "member firms." M Holdings violated the Safeguards Rule by failing to adopt policies and procedures reasonably designed to safeguard records and information of its brokerage customers and advisory clients (collectively, "customers"). M Holdings did not have written policies and procedures to govern information security across its member firms until September 2020, when M Holdings adopted an information security policy that required member firms to adopt their own information security policies and controls in 17 categories, which included multi-factor authentication ("MFA"),[2] incident response policies, and security awareness training ("Information Security Policy" or "Policy"). The Policy and its new requirements for member firms, however, were not reasonably designed because, as M Holdings was aware, a significant number of M Holdings member firms continued to lack required information security policies and controls through the Relevant Period. M Holdings did not revise its policies and procedures related to information security across member firms to address these issues.

[1] The findings herein are made pursuant to Respondent's Offer of Settlement and are not binding on any other person or entity in this or any other proceeding.

[2] MFA requires at least one authentication factor in addition to a username and password to log in to an account. The additional factor is commonly a one-time passcode generated by a hardware token or an application on the user's mobile device or computer, or sent to the user by email or text message.

4. During the Relevant Period, the electronic mail ("email") accounts of 17 registered representatives and employees at 13 out of 120 member firms were accessed by unauthorized third parties who sent malicious credential-harvesting emails from the compromised accounts to approximately 8,500 individuals, which included a significant number of customers ("email account takeovers").[3] These email account takeovers occurred at these 13 member firms that either had no written information security policies or had policies that were not reasonably designed because, for example, they did not have information security controls required by the Policy, such as MFA, incident response policies, or annual security awareness training. These incidents also resulted in the exposure of affected customers' records and information, including personally identifiable information ("PII").[4] Four of these member firms experienced two email account takeovers in the Relevant Period.

5. M Holdings also violated the Identity Theft Red Flags Rule, which requires certain financial institutions and creditors, including broker-dealers and investment advisers registered or required to be registered with the Commission, to develop and implement a written Identity Theft Prevention Program ("Program") that is designed to detect, prevent, and mitigate identity theft[5] in connection with the opening of a covered account or any existing covered account.[6] The Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities. Each financial institution's Program must include reasonable policies and procedures to: (i) identify relevant Red Flags[7] for the covered accounts that the financial institution or creditor offers or maintains, and incorporate those Red Flags into the Program; (ii) detect Red Flags that have been incorporated into the Program; (iii) respond appropriately to any Red Flags that are detected pursuant to the Program to prevent and mitigate identity theft; and (iv) ensure the Program (including the Red Flags determined to be relevant) is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.[8] Appendix A to Regulation S-ID directs firms to incorporate relevant identity theft Red Flags from sources like past incidents of identity theft

[3] As used in this Order, an "email account takeover" occurs when an unauthorized third party gains access to the email account and is also able to take actions of a legitimate user, such as sending emails or setting up forwarding rules.

[4] As used in this Order, "exposure of affected customers' records and information, including PII," means that an unauthorized third party has the ability to view (but has not necessarily viewed) the customer records and information, including PII.

[5] The rule defines "identity theft" as a fraud committed or attempted using the identifying information of another person without authority. *See* 17 C.F.R. § 248.201(b)(9).

[6] The rule defines a "covered account" to include an account that a broker-dealer or investment adviser "offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a brokerage account with a broker-dealer." 17 C.F.R. § 248.201(b)(3)(i).

[7] "Red Flags" are defined as "a pattern, practice, or specific activity that indicates the possible existence of identity theft." 17 C.F.R. § 248.201(b)(10).

[8] 17 C.F.R. § 248.201(d)(2)(i)-(iv).

that the firm has experienced and methods of identity theft that the firm has identified.[9] The Identity Theft Red Flags Rule also requires certain financial institutions to periodically determine whether they offer or maintain covered accounts.[10]

6. M Holdings had a written Identity Theft Prevention Program, and its trainings included topics on identity theft prevention. However, M Holdings did not ensure the Program was updated periodically to reflect changes in risks to customers. For example, M Holdings' Program was not substantively updated from at least 2015 through the end of the Relevant Period and did not include any specific Red Flags related to cybersecurity, despite ongoing cybersecurity incidents at member firms during the Relevant Period. The Program also did not include reasonable policies and procedures to respond appropriately to detected Red Flags. Finally, M Holdings did not conduct any periodic assessments of new or existing accounts during the Relevant Period to determine whether they were covered accounts and did not have policies and procedures for identifying covered accounts.

Respondent

7. Respondent M Holdings Securities, Inc., incorporated in Oregon and headquartered in Portland, Oregon, has been dually registered with the Commission as an investment adviser and broker-dealer since March 14, 2000 and October 30, 1997, respectively. In its Form ADV filed March 28, 2025, Respondent reported regulatory assets under management of approximately $4.1 billion. M Holdings is a wholly-owned subsidiary of M Financial Holdings Inc. ("M Financial"), which is not registered with the Commission in any capacity.

Background

M Holdings and Its Branch Office Member Firm Network

8. M Holdings provides brokerage and investment advisory services to its customers through a nationwide network of representatives at 120 branch offices known as "member firms." Approximately 700 of these representatives are registered representatives with M Holdings and provide brokerage services to customers through M Holdings, and under M Holdings' supervision, such as effecting transactions in securities. Additionally, 220 of these registered representatives are also registered with M Holdings as investment adviser representatives and provide investment advisory services to customers through M Holdings, and under M Holdings' supervision. Customers who receive brokerage and/or investment advisory services from M Holdings through registered representatives and investment adviser representatives at member firms sign service agreements directly with M Holdings. M Holdings sends its Form ADV and Brochure directly to customers who receive investment advisory services through an investment adviser representative. M Holdings collects fees from member firms by retaining a portion of the transaction-based commissions on securities transactions and/or a portion of the quarterly amount of total investment advisory fee revenue generated at each member firm.

[9] Appendix A to Subpart C of 17 C.F.R. Part 248.

[10] 17 C.F.R. § 248.201(c).

9. M Financial is owned by the member firms and the relationship between M Financial and the member firms is governed by a Marketing Agreement, which outlines requirements for membership. Such requirements include minimum production standards and compliance with "business standards," such as following legal and regulatory requirements. A member firm's membership with M Financial may be terminated for a number of reasons, including conduct that is inconsistent with the required "business standards."

M Holdings' Information Security Policy Failures

10. During the Relevant Period, M Holdings failed to adopt written policies and procedures reasonably designed to safeguard customer records and information. Before September 2020, M Holdings did not have written policies and procedures reasonably designed to govern information security across its member firms. M Holdings' lack of information security policies and procedures for its member firms resulted in inadequate and inconsistent information security policies and controls across member firms.

11. M Holdings adopted the Information Security Policy in September 2020 to address information security shortcomings at member firms. The Policy outlined information security policies and procedures required in 17 categories, including that member firms have their own written information security policies, MFA, annual security awareness training, and written incident response policies. All member firms received a model information security policy via an online platform.

12. The policies and procedures M Holdings adopted in 2020, however, were not reasonably designed. For example, data collected by M Holdings in 2021 and 2023 regarding member firms' compliance with all 17 categories of the Policy indicated that a significant number of member firms were not in compliance with requirements of the Policy from its adoption through the Relevant Period. The data also showed that several member firms continued to lack the customer protections outlined in the Policy, including written information security policies, MFA, annual security awareness training, and written incident response policies. M Holdings did not impose any consequences on member firms that did not comply with the Policy. Even though M Holdings was aware of member firms' ongoing self-reported failures to comply with the Policy during the Relevant Period, it did not revise its policies and procedures related to information security across member firms to address these issues.

Cybersecurity Incidents at Member Firms

13. Between July 2019 and March 2024, 17 email account takeovers occurred at 13 out of 120 M Holdings member firms in which unauthorized persons accessed the business email accounts of registered representatives and other employees via phishing[11] or other modes of attack and had the ability to take action in the accounts. The email account takeovers occurred at member

[11] Phishing is a means of gaining unauthorized access to a computer system or service by using a fraudulent or "spoofed" email to trick a victim into downloading malicious software or entering his or her log-in credentials on a fake website purporting to be the legitimate log-in website for the system of service.

firms that did not have information security controls required by M Holdings' Information Security Policy, such as written information security policies, MFA, annual security awareness training, or incident response policies.

14. These email account takeovers primarily resulted in unauthorized, malicious phishing and credential-harvesting emails being sent by third parties from the compromised business email accounts to approximately 8,500 individuals, which included a significant number of customers, further exposing customers to potential disclosure of their PII to bad actors. For example, these unauthorized emails sent from affected accounts asked customers to click on links, open documents, or enter information that would harvest customer credentials and information if entered. One of the email account takeovers resulted in an unauthorized wire from a customer's account. These incidents also resulted in the exposure of affected customers' records and information, including PII, stored in the compromised email accounts. Four of these member firms experienced two email account takeovers during the Relevant Period. The second email account takeovers at these member firms affected approximately 2,952 of the approximately 8,500 affected individuals mentioned above.

Identity Theft Prevention Program Failures

15. During the Relevant Period, M Holdings had a Program that was within the firm's Broker-Dealer and Registered Investment Adviser Compliance Manuals. All member firms received these Compliance Manuals and updated versions annually.

16. Regulation S-ID requires each financial institution or creditor that offers or maintains one or more covered accounts to develop and implement a Program that includes reasonable policies and procedures to "[e]nsure the Program (including the Red Flags determined to be relevant) is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft."[12] Appendix A to Regulation S-ID provides that firms should consider factors such as: (i) the firm's experiences with identity theft; (ii) changes in methods of identity theft; (iii) changes in methods to detect, prevent or mitigate identity theft; (iv) changes in the types of accounts offered or maintained; and (v) changes in the firm's structure or service provider arrangements.[13]

17. M Holdings, however, did not develop or implement reasonable policies and procedures to ensure that the Program was updated periodically. Despite significant changes in external cybersecurity risks related to identity theft from ongoing cybersecurity incidents at member firms that affected customers, as discussed above, there were no material changes to M Holdings' Program since at least 2015, and throughout the Relevant Period. For example, M Holdings did not update its Program to include Red Flags relevant to the cybersecurity incidents described above.

[12] 17 C.F.R. § 248.201(d)(2)(iv).

[13] 17 C.F.R. § 248.201 app. A, sec. V(a)-(e).

18. Moreover, despite changes in external cybersecurity risks, M Holdings' Program was not updated to include reasonable policies and procedures to address the detection of, and appropriate responses to, Red Flags in connection with cybersecurity breaches or intrusions at member firms to prevent and mitigate identify theft. Although M Holdings' Program included "procedures to prevent and mitigate identity theft," those procedures did not contain or reference steps that member firms should take in response to a cybersecurity incident, such as the email account takeovers experienced by member firms in the Relevant Period.

19. Finally, M Holdings did not periodically review new or existing accounts to determine whether they were "covered accounts" under Regulation S-ID during the Relevant Period. The Program provided no policies or procedures for identifying covered accounts, including new types of covered accounts offered or maintained by the firm. Nor did M Holdings conduct any periodic risk assessments required by Regulation S-ID to determine whether it offers or maintains covered accounts, taking into consideration: (1) the methods it provides to open its accounts; (2) the methods it provides to access its accounts; and (3) its previous experiences with identity theft.[14]

Violations

20. As a result of the conduct described above, M Holdings willfully[15] violated Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30(a)), which requires every broker-dealer and every investment adviser registered with the Commission to adopt written policies and procedures that are reasonably designed to address administrative, technical, and physical safeguards for the protection of customer records and information.

21. As a result of the conduct described above, M Holdings willfully violated Rule 201 of Regulation S-ID (17 C.F.R. § 248.201), which requires registered broker-dealers and investment advisers to periodically determine whether they offer or maintain covered accounts and requires registered broker-dealers and investment advisers that offer or maintain covered accounts to develop and implement a written Identity Theft Prevention Program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.

[14] 17 C.F.R. § 248.201(c)(1)-(3).

[15] "Willfully," for purposes of imposing relief under Section 15(b) of the Exchange Act and Section 203(e) of the Advisers Act, "'means no more than that the person charged with the duty knows what he is doing.'" *Wonsover v. SEC*, 205 F.3d 408, 414 (D.C. Cir. 2000) (quoting *Hughes v. SEC*, 174 F.2d 969, 977 (D.C. Cir. 1949)). There is no requirement that the actor "also be aware that he is violating one of the Rules or Acts." *Tager v. SEC*, 344 F.2d 5, 8 (2d Cir. 1965). The decision in *The Robare Group, Ltd. v. SEC*, which construed the term "willfully" for purposes of a differently structured statutory provision, does not alter that standard. 922 F.3d 468, 478-79 (D.C. Cir. 2019) (setting forth the showing required to establish that a person has "willfully omit[ted]" material information from a required disclosure in violation of Section 207 of the Advisers Act).

M Holdings' Remedial Efforts

22. M Holdings has undertaken remedial acts to strengthen its information security and cybersecurity programs. In particular, M Holdings has now hired a Chief Information Security Officer, a Chief Privacy Officer, and an Assistant Vice President of Technology. M Holdings is in the process of updating the Information Security Policy and plans to create mechanisms in 2025 to hold member firms accountable and impose consequences on those member firms that do not comply with the Policy's cybersecurity requirements. M Holdings has also implemented formal member firm risk assessments, mandatory cybersecurity onboarding reviews, and annual Information Security Policy compliance attestations. M Holdings also conducts cybersecurity training for member firms, hosts quarterly webinars, and provides newsletters on incident response topics to member firms. M Holdings has deployed data loss prevention and monitoring tools and established a third-party vendor risk management team for enterprise-wide risk oversight. Finally, in addition to providing training materials, M Holdings has also required additional cybersecurity and privacy training for all employees, registered representatives, and investment adviser representatives.

23. In determining to accept the Offer, the Commission considered the remedial acts undertaken by Respondent.

IV.

In view of the foregoing, the Commission deems it appropriate, and in the public interest, to impose the sanctions agreed to in Respondent M Holdings' Offer.

Accordingly, pursuant to Sections 15(b) and 21C of the Exchange Act and Sections 203(e) and 203(k) of the Advisers Act, it is hereby ORDERED that:

A. Respondent M Holdings cease and desist from committing or causing any violations and any future violations of Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30(a)) and of Rule 201 of Regulation S-ID (17 C.F.R. § 248.201);

B. Respondent M Holdings is censured; and

C. Respondent M Holdings shall, within 14 days of the entry of this Order, pay a civil money penalty in the amount of $325,000 to the Securities and Exchange Commission for transfer to the general fund of the United States Treasury, subject to Exchange Act Section 21F(g)(3). If timely payment is not made, additional interest shall accrue pursuant to 31 U.S.C. § 3717.

Payment must be made in one of the following ways:

(1) Respondent may transmit payment electronically to the Commission, which will provide detailed ACH transfer/Fedwire instructions upon request;

(2) Respondent may make direct payment from a bank account via Pay.gov through the SEC website at http://www.sec.gov/about/offices/ofm.htm; or

(3) Respondent may pay by certified check, bank cashier's check, or United States postal money order, made payable to the Securities and Exchange Commission and hand-delivered or mailed to:

Enterprise Services Center
Accounts Receivable Branch
HQ Bldg., Room 181, AMZ-341
6500 South MacArthur Boulevard
Oklahoma City, OK 73169

Payments by check or money order must be accompanied by a cover letter identifying M Holdings as a Respondent in these proceedings, and the file number of these proceedings; a copy of the cover letter and check or money order must be sent to Rahul Kolhatkar, Assistant Regional Director, Division of Enforcement, Securities and Exchange Commission, San Francisco Regional Office, 44 Montgomery Street, Suite 700, San Francisco, CA 94104.

D. Amounts ordered to be paid as civil money penalties pursuant to this Order shall be treated as penalties paid to the government for all purposes, including all tax purposes. To preserve the deterrent effect of the civil penalty, Respondent agrees that in any Related Investor Action, it shall not argue that it is entitled to, nor shall it benefit by, offset or reduction of any award of compensatory damages by the amount of any part of Respondent's payment of a civil penalty in this action ("Penalty Offset"). If the court in any Related Investor Action grants such a Penalty Offset, Respondent agrees that it shall, within 30 days after entry of a final order granting the Penalty Offset, notify the Commission's counsel in this action and pay the amount of the Penalty Offset to the Securities and Exchange Commission. Such a payment shall not be deemed an additional civil penalty and shall not be deemed to change the amount of the civil penalty imposed in this proceeding. For purposes of this paragraph, a "Related Investor Action" means a private damages action brought against Respondent by or on behalf of one or more investors based on substantially the same facts as alleged in the Order instituted by the Commission in this proceeding.

By the Commission.

Vanessa A. Countryman
Secretary