UNITED STATES OF AMERICA
Before the
SECURITIES AND EXCHANGE COMMISSION

SECURITIES EXCHANGE ACT OF 1934
Release No. 95368 / July 27, 2022

INVESTMENT ADVISERS ACT OF 1940
Release No. 6074 / July 27, 2022

ADMINISTRATIVE PROCEEDING
File No. 3-20937

In the Matter of **UBS FINANCIAL SERVICES 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 ("Exchange Act") and Sections 203(e) and 203(k) of the Investment Advisers Act of 1940 (the "Advisers Act"), against UBS Financial Services Inc. ("Respondent" or "UBS").

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 that:

Summary

1. These proceedings arise out of UBS's failure to adequately develop and implement a written Identity Theft Prevention Program as required by Rule 201 of Regulation S-ID (17 C.F.R. § 248.201).

2. UBS is a broker-dealer and investment adviser registered with the Commission. From at least January 1, 2017 to October 3, 2019 (the "relevant period"), UBS violated Rule 201 of Regulation S-ID because its written Identity Theft Prevention Program (the "Program") lacked reasonable policies and procedures to: (i) identify relevant red flags for the covered accounts UBS offered and maintained, and incorporate those red flags into its Program; (ii) detect red flags that have been incorporated into its Program; (iii) respond appropriately to detected red flags to prevent and mitigate identity theft; and (iv) ensure that the Program was updated periodically.

3. Moreover, UBS violated Rule 201 of Regulation S-ID during the relevant period because it did not periodically review new or existing accounts to determine whether they were "covered accounts,"[1] nor did it provide for the continued administration of its Program by not: (i) adequately involving the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the Program; and (ii) training its employees to effectively implement the Program.

Respondent

4. UBS Financial Services Inc., a Delaware corporation, is a dual-registered broker-dealer and investment adviser. UBS has been registered with the Commission as a broker-dealer and investment adviser since 1971 and has its principal place of business in Weehawken, New Jersey. It is a subsidiary of UBS Group AG, a publicly traded company incorporated in Switzerland.

Background

5. During the relevant period, UBS's Identity Theft Prevention Program failed to comply with the requirements of Regulation S-ID.

---

[1] 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).

6. Regulation S-ID requires financial institutions, including broker-dealers and investment advisers registered with the Commission with 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.[2] As part of such an Identity Theft Prevention Program, each registered broker-dealer and investment adviser must periodically determine whether it offers or maintains covered accounts. As a part of this determination, a firm must conduct a risk assessment 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.[3]

7. According to Regulation S-ID, an Identity Theft Prevention Program must also include reasonable policies and procedures to: (i) identify relevant "red flags"[4] for the covered accounts and incorporate them into the Identity Theft Prevention Program; (ii) detect the red flags that have been incorporated into the Identity Theft Prevention Program; (iii) respond appropriately to any red flags that are detected pursuant to the Identity Theft Prevention Program; and (iv) ensure that the Identity Theft Prevention Program is updated periodically to reflect changes in risks to customers and to the safety and soundness of the firm from identity theft.[5]

8. With respect to the identification of relevant red flags, Regulation S-ID requires firms to consider several factors specific to the firm in order to identify red flags that are relevant to the firm's business and the nature and scope of its activities, such as the types of covered accounts it offers or maintains, methods it provides to open accounts, methods it provides to access accounts, and its previous experiences with identity theft.[6]

9. Appendix A to Regulation S-ID, which contains guidelines intended to assist firms in the formulation and maintenance of an Identity Theft Prevention Program that satisfies the requirements of Regulation S-ID, lists categories of red flags that firms consider incorporating in an Identity Theft Prevention Program "as appropriate."[7] Supplement A to Appendix A further

---

2 17 C.F.R. § 248.201(d)(1). The rule defines "identity theft" as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201(b)(9).

3 17 C.F.R. § 248.201(c)(1)-(3).

4 "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).

5 17 C.F.R. § 248.201(d)(2)(i)-(iv).

6 17 C.F.R. § 248.201 app. A, sec. II(a)(1)-(4).

7 17 C.F.R. § 248.201 app. A, sec. II(c). These categories are: "(i) [a]lerts, notifications, or [other] warnings received from consumer reporting agencies . . . ;" (ii) "suspicious documents," such as documents that appear to have been altered or forged; (iii) "suspicious personal identifying information, such as a suspicious address change;" (iv) "unusual use of, or other suspicious activity related to, a covered account;

provides a non-comprehensive list of examples of red flags from each of these categories that the firm "may consider incorporating into its Program, whether singly or in combination…in connection with covered accounts."[8]

10. Regulation S-ID requires an Identity Theft Prevention Program's policies and procedures to address the detection of red flags in connection with the opening of covered accounts and existing covered accounts. In order to prevent and mitigate identity theft, the Identity Theft Prevention Program "should [also] provide for appropriate responses" to detected red flags "that are commensurate with the degree of risk posed."[9] In determining an appropriate response, a firm "should consider aggravating factors that may heighten the risk of identity theft…."[10] In that regard, appropriate responses might include, among others, contacting the consumer, not opening a new account, or notifying law enforcement.[11]

11. With respect to periodically updating the Identity Theft Prevention Program, Appendix A 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.[12]

12. Regulation S-ID also requires firms to provide for the continued administration of the Identity Theft Prevention Program by involving the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the Identity Theft Prevention Program, and training staff, as necessary, to effectively implement the Identity Theft Prevention Program.[13]

13. The oversight by the board of directors, an appropriate committee thereof, or senior management should include reviewing reports of compliance with Regulation S-ID at least annually. Those reports should address material matters related to the Identity Theft Prevention Program and evaluate issues such as: (i) the effectiveness of the policies and procedures of the firm in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts; (ii) service provider arrangements; (iii) significant incidents

---

and" (v) "[n]otice from customers, victims of identity theft, [or] law enforcement authorities . . . ." 17 C.F.R. § 248.201 app. A, sec. II(c)(1)-(5).

8 17 C.F.R. § 248.201 app. A, supp. A .

9 17 C.F.R. § 248.201 app. A, sec. IV.

10 *Id.*

11 17 C.F.R. § 248.201 app. A, sec. IV(b), (e), (h).

12 17 C.F.R. § 248.201 app. A, sec. V(a)-(e).

13 17 C.F.R. § 248.201(e)(2)-(3).

involving identity theft and management's response; and (iv) recommendations for material changes to the Identity Theft Prevention Program.[14]

UBS's Identity Theft Prevention Program

14. In November 2008, UBS adopted its Program which was intended to comply with the then-applicable Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, issued jointly in November 2007 by several federal agencies including the Federal Trade Commission (16 C.F.R. § 681.1). The Program applied to UBS and several other entities and branch offices in the United States and Puerto Rico which offered private and retail banking, mortgage, and private investment services that operated under UBS Group AG's Wealth Management Americas' line of business.

15. UBS did not make material changes to the Program after Regulation S-ID went into effect in May 2013 and throughout the relevant period. The Program was only updated, effective March 28, 2017, to add a reference to "the SEC's Regulation S-ID" when discussing "related regulations" with which the Program was established to comply, and to revise the list of legal entities and branch offices subject to the Program.

16. During the relevant period, UBS did not periodically review new or existing accounts to determine whether they were "covered accounts" under Regulation S-ID. The Program provided no policies or procedures for identifying covered accounts, including new types of covered accounts offered by the firm. Moreover, while the written Program characterized all client accounts as "covered accounts," UBS did not conduct any risk assessments or other evaluations of these accounts for it to determine the types of covered accounts it offered or maintained and thereby identify red flags based on those types of covered accounts.

17. During the relevant period, UBS's Program did not have reasonable policies and procedures to identify relevant red flags and incorporate them into the Program. The Program only provided that UBS and other covered affiliates would identify red flags based on the "types of covered accounts" at the firm, the "[p]revious experience" the firm has had with identify theft, and "[a]pplicable regulatory guidance." The Program provided no further information for relevant red flags tailored to UBS's business and the nature and scope of its brokerage and advisory activities to be identified. Moreover, the Program did not specifically identify any red flags for identity theft, or otherwise incorporate or reference any other policies and procedures that enumerated specific red flags.

18. During the relevant period, UBS's Program did not have reasonable policies and procedures to address the detection of red flags in connection with the opening of covered accounts and existing covered accounts. The Program only provided that each UBS-affiliated entity was "responsible for maintaining procedures to address the detection of Red Flags" and listed general categories of activities (e.g., changes to client profiles, unusual client transactions, complaints, and ongoing monitoring) that those procedures should address. The Program did not identify any

[14] 17 C.F.R. § 248.201 app. A, sec. VI(b)(2).

relevant red flags that employees at UBS should be aware of or include, incorporate, or reference any procedures addressing those categories or the detection of red flags.

19. During the relevant period, UBS's Program did not have reasonable policies and procedures to respond appropriately to red flags in order to prevent and mitigate identify theft. While the Program provided that a "response to and mitigation of identity theft consists of two parts," including "[p]rocedures to address responses to identity theft attempts" and "[i]mplementation of additional account protections," it did not include policies and procedures on these 'two parts,' or incorporate or reference other policies and procedures addressing responding to red flags.

20. During the relevant period, UBS's Program did not have reasonable policies and procedures to ensure that it was updated periodically. Despite significant changes in external cybersecurity risks related to identity theft,[15] for example, there had been no material changes to the Program from its inception in 2008, and throughout the relevant period. During that entire time period, while the Program provided that it would be updated periodically to reflect material changes in "procedures and activities" of the entities subject to the Program "for identifying and responding to identity theft flags and in risks to customers" or those entities, the Program did not identify or incorporate any relevant red flags or include, incorporate, or reference any policies and procedures addressing detecting and responding to red flags.

21. During the relevant period, UBS failed to adequately provide for the continued administration of its Program. The annual reports provided to the board of directors that related to the Program during the relevant period did not provide sufficient information addressing the effectiveness of the Program's policies and procedures concerning the risk of identity theft at UBS or the firm's service providers, nor did they provide sufficient detail about significant identity theft-related incidents and management's responses, or metrics related to identity theft at the firm, to enable its board of directors to be sufficiently involved in the oversight, development, implementation and administration of the Program. In that regard, board minutes do not reflect any discussion of compliance with Regulation S-ID during the relevant period. In addition, UBS did not conduct any training of its staff specific to the Program or training on how to identify, detect, monitor, or respond to red flags involving identity theft.

Violation

22. As a result of the conduct described above, Respondent willfully[16] violated Rule 201 of Regulation S-ID (17 C.F.R. § 248.201), which requires registered broker-dealers and

---

15 *See, e.g.*, Identity Theft Red Flags Rules, Exchange Act Release No. 34-69359 (Apr. 10, 2013) ("Advancements in technology also have led to increasing threats to the integrity and privacy of personal information.") (footnote omitted).

16 "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

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.

UBS's Remedial Efforts

23. UBS has undertaken substantial remedial acts, including auditing and revising its Program.

24. In particular, UBS voluntarily retained an outside consulting firm to review its Program, which recommended various enhancements involving, among other things, identifying and responding to red flags, identifying covered accounts, and the periodic updating and administration of the Program, including the training of employees, all of which UBS adopted. UBS also made detailed presentations to the Commission's staff regarding the Program's enhancements.

25. 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's 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 cease and desist from committing or causing any violations and any future violations of Rule 201 of Regulation S-ID (17 C.F.R. § 248.201).

B. Respondent is censured.

C. Respondent shall, within 30 days of the entry of this Order, pay a civil money penalty in the amount of $925,000.00 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:

---

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).

(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 UBS Financial Services Inc. as the 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 Carolyn Welshhans, Associate Director, Division of Enforcement, Securities and Exchange Commission, 100 F St., NE, Washington, DC 20549.

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