UNITED STATES OF AMERICA
Before the
SECURITIES AND EXCHANGE COMMISSION

SECURITIES EXCHANGE ACT OF 1934
Release No. 84828 / December 17, 2018

INVESTMENT ADVISERS ACT OF 1940
Release No. 5075 / December 17, 2018

ADMINISTRATIVE PROCEEDING
File No. 3-18931

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 SECTION 203(e) 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 Section 203(e) of the Investment Advisers Act of 1940 ("Advisers Act") against UBS Financial Services Inc. ("Respondent" or "UBSFS").

II.

In anticipation of the institution of these proceedings, Respondent has submitted an Offer of Settlement ("Offer") that the Commission has determined to accept. Solely for the purpose of these proceedings and any other proceeding 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 to the extent contained in paragraph 1(a) of the Consent to the Assessment of Civil Money Penalty in the matter of *UBS Financial Services Inc.,* No. 2018-03 issued by the United States Department of the Treasury, Financial Crimes Enforcement Network, and 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 Section 203(e) 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:

A. SUMMARY

1. A registered broker-dealer is required to file a suspicious activity report ("SAR") when it knows, suspects, or has reason to suspect that certain transactions (1) involve funds derived from illegal activity, (2) involve the use of the broker-dealer to facilitate criminal activity, (3) are designed to evade any requirement of the Bank Secrecy Act ("BSA"), or (4) have no business or apparent lawful purpose. This matter concerns Respondent's violations of Section 17(a) of the Exchange Act and Rule 17a-8 thereunder in connection with its failure to file suspicious activity reports ("SARs") in compliance with these reporting requirements. As with some broker-dealers, Respondent, in addition to buying and selling securities, offered its customers other services, such as wires, internal transfers between accounts ("journals"), check writing, ATM withdrawals, cash advances, and ACH transfers. By offering these services, UBSFS was susceptible to the risks of money laundering associated with these services.

2. From January 2011 through March 2013 (the "relevant period"), Respondent had an anti-money laundering ("AML") program that was not reasonably designed to account for the risks associated with these additional services used by customers in their retail brokerage accounts. Because of the deficiencies detailed below, Respondent did not adequately monitor for, detect, and report suspicious activity for certain transactions or patterns of transactions occurring in non-resident alien ("NRA") customer accounts in a San Diego, California branch office.

B. RESPONDENT

3. UBSFS has been dually registered as a broker-dealer (SEC # 8-16267) and an investment adviser with the Commission since 1971. UBSFS is a Delaware corporation with its principal place of business in Weehawken, New Jersey. It is a subsidiary of UBS Group AG, a public reporting company headquartered in Switzerland. UBS Group AG's business unit, called "Wealth Management Americas," consists of branch networks in the United States, Puerto Rico, Canada and Uruguay, with over 7,000 financial advisors as of December 2015. In the U.S., retail securities and operations activities are conducted primarily through UBSFS.

C. RESPONDENT FAILED TO FILE CERTAIN SARS

4. During the relevant period, Respondent offered brokerage accounts that allowed customers to move funds via wires, journals, check writing, ATM withdrawals, cash advances, and ACH transfers. The products and services offered by Respondent through its brokerage accounts, which are also offered by other broker-dealers, presented additional money laundering risks not typically associated with brokerage-only accounts.

5. Prior to the relevant period, Respondent adopted as part of its AML program a document entitled "Money Laundering Prevention Guide" ("Prevention Guide"), which was a component of its firm-wide compliance policies. The Prevention Guide recognized that NRA accounts presented greater money laundering concerns than did domestic accounts, specifically identified certain countries as "sensitive" because of concerns associated with money laundering, among other things, and imposed additional requirements for opening those accounts. The document listed numerous red flags for identifying potentially suspicious activity. In fact, many of the examples of red flags identified by Respondent in the Prevention Guide are consistent with guidance issued by FinCEN to inform and assist banks and other financial institutions in reporting instances of suspected money laundering and fraud.[1] The Prevention Guide was actively reviewed and updated and was a component of Respondent's AML policies and procedures during the relevant period.[2] The Prevention Guide identified potential indicators for money laundering including, but not limited to:

- Large or repetitive wire transfers from a customer or journals among customers;
- Attempts to engage in large or unusual transactions without adequate explanation;
- Transactions that seem unnecessarily complicated;
- Frequent actual or attempted deposits of large amounts of cash or cash-like instruments; and
- Receiving many small incoming wire transfers or deposits or numerous checks and shortly thereafter requesting wire transfers to another country.

6. During the relevant period, Respondent used two surveillance system programs to monitor accounts for potentially suspicious transactions related to fund movements. First, it used a commercial program called Fortent, which, among other components, included parameter-based rules to surveil customers and/or activity and detect known AML typologies. Second, it used a proprietary program it called the Report Delivery System ("RDS"). Fortent had a function called "Security Blanket," which assigned peer group designations to all customers, and also tracked customers' historical activity. If the activity of a customer deviated from expected activity in a defined peer grouping, as well as the customer's own previous activity measured over a given period of time, Fortent would generate an alert. RDS also alerted on transaction patterns and customer types that fit within specific set scenarios or if the activity fell within certain parameters.

7. The Money Laundering Prevention Group ("MLPG") was the group within Respondent responsible for reviewing and investigating potentially suspicious transactions. The MLPG was also responsible for determining whether to file a SAR relating to a customer's account activity. There were two key units within the MLPG responsible for reviewing and assessing transactions and customer account activity: Surveillance and Investigations.

8. Analysts in the MLPG Surveillance Unit reviewed alerts that were generated from Fortent and RDS, and also handled certain referrals from various areas within Respondent relating

[1] *See* Bank Secrecy Act Anti-Money Laundering Examination Manual, Appendix F: Money Laundering and Terrorist Financing "Red Flags".

[2] *See* 31 CFR § 1023.210 et seq.

to transactions that might be indicative of money laundering, fraud or other suspicious activities. Alerts that could not be resolved and closed by the surveillance analysts were elevated to the MLPG Investigations Unit, which conducted a more comprehensive investigation. Investigations were also generated from referrals from other units within UBSFS, negative news on UBSFS customers, and inquiries from law enforcement and other financial institutions. Upon completion of an investigation, the investigations manager determined whether or not a SAR should be filed.

9. During the relevant period, Respondent had an average of over 300,000 NRA accounts in any given year. During this period of time, more than $83 billion moved through NRA accounts at UBSFS.

10. One branch in San Diego, California, was at increased risk for money laundering because its business model predominantly was to service NRA accounts. While there is nothing inherently suspicious about NRA customers, there may be an increased AML risk for NRA customers who engage in i) cross-border money movements, including to and from high risk jurisdictions and/or ii) use of off-shore shell companies or personal investment companies for complicated fund movements. This branch, internally coded as K2 Branch, was part of Respondent's network of international branches dedicated to servicing NRAs and had nearly 6,000 NRA accounts. Moreover, although the NRA customers at this branch resided in countries located throughout the world, some NRA customers lived in countries that Respondent itself had identified as sensitive due to the increased risk of money laundering, such as Mexico, Venezuela, and Panama. During the relevant period, customers moved over $9 billion through the NRA accounts at the K2 Branch.

a) <u>Respondent Did Not Have a Reasonably Designed AML Program to Detect Suspicious Activity in NRA Customer Accounts with Elevated AML Risk</u>

11. As described below, transaction patterns engaged in by NRA accounts at the K2 Branch that matched the red flags identified by Respondent in its Prevention Guide did not alert. Certain NRA customers at that branch used multiple Respondent accounts, including use of multiple individual and entity accounts with common control or ownership, to move funds in suspicious long-term patterns. These patterns of money movements had a consistent typology or profile of using Respondent accounts as intermediaries between other financial institutions with no business or apparent lawful purpose. Respondent, however, did not adequately surveil for such NRA account activity because its parameters for detecting such suspicious activity through the RDS system were too narrow under the circumstances.

12. For example, UBSFS had an RDS alert that was designed to capture all incoming journal transactions into an account that aggregated to $100,000 or more if 90% of that amount was withdrawn from the account within a 5-day period by a wire transfer, check, account transfer, or ATM withdrawals. These parameters were too narrow under the circumstances. Additionally, this RDS alert did not capture other variations of journal patterns that are commonly indicative of suspicious activity, such as deposits of wires into an account, shortly followed by outgoing journals, or incoming journals into an account, shortly followed by outgoing journals from the same account. The RDS alert for journal activity therefore was deficient in its ability to detect suspicious fund movements through multiple accounts via internal journal transfers.

13. Because of these system deficiencies, certain patterns of suspicious activity did not trigger alerts, and, as a result, Respondent failed to file certain SARs on suspicious transactions involving the NRA accounts at the K2 Branch, as required by Rule 17a-8.

b) Respondent Did Not Adequately Review Alerts Relating to NRA Accounts

14. When the K2 Branch did generate alerts, Respondent's Surveillance Unit analysts reviewed them to determine if they should be closed or elevated to the Investigations Unit for further investigation. Certain transactions or account activity in certain NRA accounts from the K2 Branch matched red flags present in the Prevention Guide, which Respondent was alerted to from its surveillance systems. For these accounts, the Surveillance Unit sometimes closed alerts, even though the transactions on their face were suspicious and may have required the filing of a SAR.

15. In certain NRA accounts, the event that triggered the alert was also accompanied by patterns of suspicious money movements between customer accounts, with no securities trading activity occurring in the accounts before the funds were disbursed. These fund movements often involved round-dollar amounts, sometimes large, with multiple journals during a short timeframe between accounts having common ownership or control. In those instances, while the analysts reviewed the transaction that triggered the alert, they did not inquire into the long-term patterns of fund movements in the accounts and did not determine if they had a legitimate business purpose. The analysts did not inquire despite the fact that the activity matched red flags identified in the Prevention Guide. The analysts' decision to close alerts under these circumstances prevented Respondent from elevating the transactions to the Investigations Unit and potentially filing SARs.

16. With respect to certain NRA accounts, analysts closed alerts based on work done on previous account alerts even when the new alerts were on transactions later in time and involving different types of potentially suspicious activity. The analysts' notes referred to the previous alert review but did not address the new activity or the red flags present in the account. Second, analysts reviewed transactions on a stand-alone basis, instead of viewing the transactions in the context of longer-term patterns of activity in a customer's account. Because of this, the analysts did not uncover the suspicious nature of the patterns of activity.

17. Due to these deficiencies in the alert review process, Respondent did not identify certain long-term patterns of suspicious activity involving NRA accounts at the K2 Branch, and therefore failed to file SARs on some suspicious transactions as required by Rule 17a-8.

c) Examples of Respondent Not Filing SARs

18. As a result of the deficiencies in its AML program identified above, Respondent did not file SARs on suspicious movements of funds through certain of its NRA accounts. During the relevant period, at the K2 Branch Respondent did not file SARs on certain accounts engaged in suspicious money movement activity that exhibited certain of the red flags indicative of money laundering consistent with guidance from FinCEN and contained in Respondent's Prevention Guide. As set out in the examples below, Respondent's failure to file SARs arose

either because the transactions did not generate an alert due to the narrow parameters in RDS or the transactions did generate an alert but the analysts at Respondent who reviewed those transactions did not escalate the review to the Investigations Unit. For example:

(1) An off-shore personal holding company received, several times a week, large, primarily round dollar wire deposits. The funds were then either wired out to related entities at other financial institutions, or journaled from the personal holding company to the beneficial owner's individual account at UBSFS, and at that point withdrawn via checks and wires to other financial institutions. There was no securities activity in either the personal holding company account or individual account. Despite several million dollars moving through the accounts in repetitive patterns that matched certain of the red flags identified in the Prevention Guide, the activity did not generate an alert in the UBSFS AML monitoring systems due to the thresholds in RDS.

(2) An off-shore entity received wires in a pattern of transactions reflecting suspicious activity. During the relevant time period, these wires totaled millions of dollars. This entity received primarily $100,000 wire transfers from a separate, commonly-owned off-shore entity. Once a deposit was received, the customer then moved the funds, via internal journals in smaller amounts, to an account at another branch. The journals sometimes occurred daily. There was no trading in the entity account. Despite several million dollars moving through the accounts in patterns that matched certain red flags in the Prevention Guide, the activity did not alert due to the thresholds in RDS.

(3) An NRA entity customer in the business of customs brokerage services with a high-risk jurisdiction received primarily large, round-dollar denominated checks in a repetitive pattern over a period of several years. The funds were then either journaled to the beneficial owner's individual account at UBSFS or withdrawn via large, even-dollar denominated checks soon after the deposits were made. There were no securities transactions in the account and no AML alerts due to the thresholds in RDS.

(4) An off-shore company received large, round dollar wire deposits in a repetitive pattern, minus wire transfer fees, from its off-shore businesses. The company then journaled funds to multiple individual family member accounts also at Respondent in nearly identical patterns. Those family member accounts then disbursed those funds in the same patterns through another series of journals to commonly-owned accounts at other financial institutions, often in even-dollar denominated checks and wires. The account alerted and the surveillance analyst reviewed the transactions, including the deposits, journals and withdrawals. However, the analyst focused on identifying the source of funds into Respondent, and, based on the available documentation, did not detect the repetitive nature of the transactions. The analyst did not inquire into the patterns of funds moving through the account, despite the fact that they matched certain red flags in the

Prevention Guide. Despite these suspicious transactions, analysts did not escalate the transactions to the investigations unit.

(5) An NRA customer received large wire deposits in a repetitive pattern into his personal account from third parties and commonly-owned entities. The customer journaled the funds through multiple entity accounts held at UBSFS, often in the same amounts and on the same day. The customer then wired the funds out to another financial institution with the majority of the accounts involved having no securities activity. The activity generated alerts, but the AML surveillance analyst did not escalate the transactions to the Investigations Unit.

D. RESPONDENT'S REMEDIAL EFFORTS

19. The Commission considered the substantial remedial acts undertaken by Respondent. UBSFS has remediated the issues described above as follows:

(1) Enhanced Surveillance System: In early 2016, UBS Group AG began the process of upgrading its AML surveillance monitoring system globally across all its separate business lines to a new surveillance system. Once fully implemented at Respondent, the new system will provide enhanced grouping and alert features, thus strengthening the ability to monitor transactions between related accounts.

(2) Accountability: Respondent has enhanced its oversight of AML monitoring and also implemented back-testing protocols, which help enhance the quality of the alerts and reduce false positives.

(3) Enhanced Training and Minimum Standards for Key AML Monitoring Staff: In order to enhance the quality of alert handling, Respondent has set minimum experience requirements for its AML monitoring staff and provided them extensive training.

(4) Alert Handling, Documentation, and Inventory Tracking: Respondent has enhanced its minimum standards for alert handling, documentation and tracking. The enhancements include, among other things, detailed written instructions on how to handle alerts, document a review, and escalate an alert through the proper personnel channels.

(5) Quality Assurance: Under the new quality assurance ("QA") system, Respondent assesses the quality of the AML monitoring analysts' work and substantive accuracy of the disposition of the alert. Findings are reported monthly to designated senior officers.

E. VIOLATIONS

20. The BSA, and implementing regulations promulgated by the Financial Crimes Enforcement Network ("FinCEN"), require that broker-dealers file SARs with FinCEN to report

a transaction (or a pattern of transactions of which the transaction is a part) conducted or attempted by, at, or through the broker-dealer involving or aggregating to at least $5,000 that the broker dealer knows, suspects, or has reason to suspect: (1) involves funds derived from illegal activity or is conducted to disguise funds derived from illegal activities; (2) is designed to evade any requirement of the BSA; (3) has no business or apparent lawful purpose and the broker-dealer knows of no reasonable explanation for the transaction after examining the available facts; or (4) involves use of the broker-dealer to facilitate criminal activity. 31 C.F.R. § 1023.320(a)(2) ("SAR Rule").

21. Rule 17a-8 under the Exchange Act requires broker-dealers to comply with the reporting, recordkeeping and record retention requirements of the BSA. Not filing a SAR as required by the SAR Rule is a violation of Section 17(a) of the Exchange Act and Rule 17a-8 thereunder.

22. As a result of not filing SARs reporting the suspicious movement of funds through certain of its NRA accounts, as described above, Respondent willfully violated Exchange Act Section 17(a) and Rule 17a-8 thereunder.[3]

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 Section 203(e) 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 Exchange Act Section 17(a) or Rule 17a-8 thereunder;

B. Respondent is censured;

C. Respondent shall, within 14 days of entry of this Order, pay a civil money penalty in the amount of $5,000,000 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

[3] A willful violation of the securities laws means merely "'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.'" *Id.* (quoting *Gearhart & Otis, Inc.* v. *SEC*, 348 F.2d 798, 803 (D.C. Cir. 1965)).

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, Oklahoma 73169

Payments by check or money order must be accompanied by a cover letter identifying UBSFS 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 Alka Patel, Associate Regional Director, Division of Enforcement, Securities and Exchange Commission, 444 S. Flower Street, Suite 900, Los Angeles, CA 90071.

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.

Brent J. Fields
Secretary