

**FINANCIAL INDUSTRY REGULATORY AUTHORITY
LETTER OF ACCEPTANCE, WAIVER, AND CONSENT
NO. 2019062705801**

TO: Department of Enforcement
Financial Industry Regulatory Authority (FINRA)

RE: SoFi Securities LLC (Respondent)
Member Firm
CRD No. 151717

Pursuant to FINRA Rule 9216, Respondent SoFi Securities LLC submits this Letter of Acceptance, Waiver, and Consent (AWC) for the purpose of proposing a settlement of the alleged rule violations described below. This AWC is submitted on the condition that, if accepted, FINRA will not bring any future actions against Respondent alleging violations based on the same factual findings described in this AWC.

I.

ACCEPTANCE AND CONSENT

- A. Respondent accepts and consents to the following findings by FINRA without admitting or denying them:

BACKGROUND

SoFi Securities LLC has been a FINRA member since 2011. SoFi is headquartered in San Francisco, CA and currently has approximately 90 registered persons based out of 5 branch offices. SoFi offers commission-free, self-directed trading for retail investors through its mobile applications and website.

OVERVIEW

From December 2018 through April 2019, SoFi failed to establish and maintain a reasonable Customer Identification Program (CIP) for SoFi Money, its cash management brokerage account. SoFi used a largely automated process to approve the opening of SoFi Money accounts that was not reasonably designed to verify the customers' identity and was, therefore, vulnerable to fraud perpetrated by third parties using fictitious or stolen identities. The firm approved the opening of approximately 800 accounts that third parties then used to transfer approximately \$8.6 million from the accounts of customers at other financial institutions without authorization; approximately \$2.5 million of those transfers were subsequently withdrawn by these third parties from the SoFi Money accounts. As a result, SoFi violated FINRA Rules 3310(b) and 2010.

During this period, SoFi also failed to develop and implement a written Identity Theft Prevention Program (ITPP) reasonably designed to detect, prevent, and mitigate identity

theft. Therefore, SoFi violated Rule 201 of Regulation S-ID of the Securities Exchange Act of 1934 and FINRA Rule 2010.

FACTS AND VIOLATIVE CONDUCT

This matter originated after SoFi self-reported to FINRA that third parties had fraudulently transferred funds from accounts at unaffiliated financial institutions without authorization to SoFi Money accounts.

A. SoFi created, and rolled out to the public, a cash management brokerage account.

In 2018, SoFi began offering SoFi Money, a brokerage account that provided features associated with traditional banking services, such as check writing and the use of debit cards. Over the course of several months, SoFi rolled out SoFi Money in multiple phases to assess the effectiveness of the firm's procedures before offering it to the general public. Initially, SoFi made SoFi Money available only to employees and individuals who were already customers of SoFi. In December 2018, the firm offered SoFi Money to members of the public who had previously signed up on a waitlist for a SoFi Money account. In February 2019 it offered SoFi Money to the general public. Prior to the general public launch, there were minimal unauthorized transfers from external accounts into SoFi Money accounts.

B. SoFi Money applicants stole from customers of other financial institutions and used SoFi Money to withdraw the funds.

From December 2018 through April 2019, certain SoFi Money applicants using stolen or fictitious identities took advantage of the weaknesses in SoFi's CIP and ITPP systems and procedures to open approximately 800 SoFi Money accounts, link those accounts to external bank accounts to which they had fraudulently obtained access, and transfer funds from the external accounts to their SoFi Money accounts.¹ They then withdrew the stolen funds from the SoFi Money accounts through ACH transfers, ATM withdrawals, and debit card purchases. In total, approximately \$2.5 million in stolen funds that were transferred to SoFi Money accounts was subsequently withdrawn from those accounts.²

In response to the fraud described herein, SoFi increased staff trained to review fraud alerts, and implemented improvements to its CIP and ITPP systems and procedures. Starting in April 2019, SoFi upgraded its fraud identification tool to perform additional verification of customer identity and changed its customer verification logic to systematically decline certain applicants. Also in April 2019, SoFi hired third-party consultants to help address the significant volume of fraud alerts that had been generated

¹ For the external accounts at issue here, SoFi linked the SoFi Money account to the external account after the applicant verified trial-deposits—i.e., deposits of small amounts of money—made to the external account. Because the applicants had obtained unauthorized access to the external accounts, they were able to verify the amounts of the trial-deposits in the external accounts.

² All injured parties have been reimbursed.

beginning in February 2019, and to assist with the firm's remediation efforts. SoFi also reviewed activity in thousands of high-risk accounts and made the self-report to FINRA. In February 2022, SoFi became a bank holding company, began offering checking and savings accounts, and, in June 2022, ceased offering SoFi Money to new customers with limited exceptions.

C. SoFi established and implemented a CIP that was not reasonably designed to verify customer identity.

FINRA Rule 3310(b) requires member firms to establish and implement policies, procedures, and internal controls, reasonably designed to achieve and monitor compliance with the requirements of the Bank Secrecy Act (31 U.S.C. § 5311, *et seq.*) (BSA) and its implementing regulations. The BSA's implementing regulations require, among other things, that firms establish, document, and maintain a written Customer Identification Program appropriate for the firm's size and business and that the program contain risk-based procedures for verifying the identity of each customer to the extent reasonable and practicable. A violation of FINRA Rule 3310 also constitutes a violation of FINRA Rule 2010, which requires members, in the conduct of their business, to "observe high standards of commercial honor and just and equitable principles of trade."

From December 2018 through April 2019, SoFi failed to establish and maintain a CIP reasonably designed to verify customers' identity because its account approval process allowed opening of SoFi Money accounts without a reasonable review of potential red flags associated with some applicants. During this period, SoFi used a third-party vendor as a key part of its customer identity verification process for applicants. After completing its identity verification analysis, the vendor provided SoFi with a number score for the applicant. In addition to the number score, the vendor provided a report outlining any risks its analysis identified. If the number score provided by the vendor for the applicant did not satisfy SoFi's threshold, the firm would manually review the application. If the vendor's number score for the applicant did satisfy SoFi's threshold, and other commercial tools used by SoFi also supported the authenticity of the applicant's identity, SoFi automatically approved the account without reviewing the vendor's report. As a result of this process, SoFi automatically approved the opening of numerous accounts despite the presence of red flags contained in the vendor's report without further review or follow up. Red flags included the following:

- The applicant provided information, such as a telephone number or residential address, that was inconsistent or in conflict with other available information;
- The applicant provided the same address and/or telephone number associated with another unrelated account;
- The applicant had no credit history;
- The applicant used an Internet Protocol (IP) address to apply for the account that was over 100 miles from his/her residential address; and

- The applicant provided a social security number (SSN) that was not valid or was associated with the name of a different person, including a deceased individual.

In certain instances, multiple red flags were present in a single application and identified in the vendor report. Yet these applications were automatically approved without further review because they met the scoring threshold. For example, in one vendor report the firm did not review because the application met its standards for automatic approval, the applicant had an invalid name, the address provided by the applicant did not exist or was not valid, the email address and phone number provided were both considered high risk, the vendor was unable to verify the date of birth, and the SSN provided by the applicant was issued prior to the entered date of birth and was associated with a different name and address.³

In addition, SoFi's system was not designed, and failed, to detect that some of the applicants had previously attempted to engage in fraud with respect to a separate SoFi product. Prior to offering SoFi Money to the public, consultants SoFi hired to test the firm's fraud detection and supervisory systems recommended, among other things, that SoFi implement a process to identify former SoFi customers whose loan or investment accounts were previously rejected or closed for potential fraud so that SoFi could screen them if they tried to apply for a SoFi Money account. SoFi, however, did not implement this recommendation prior to making SoFi Money available to the public.

Therefore, Respondent violated FINRA Rules 3310(b) and 2010.

D. SoFi developed and implemented a program that was not reasonably designed to detect, prevent, and mitigate identity theft.

Rule 201 of Regulation S-ID of the Securities Exchange Act of 1934 requires broker-dealers to develop and implement a written ITPP that is designed to detect, prevent, and mitigate identity theft in connection with new and existing covered accounts. A covered account includes an account offered or maintained primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions. A firm's ITPP must include "reasonable policies and procedures" to identify red flags of identity theft relevant to the firm's business, detect those red flags, respond appropriately to any red flags detected, and ensure that the firm's program remains up-to-date. In designing its ITPP, firms are expected to consider a number of factors, including the methods of accessing covered accounts, the detection of red flags of identity theft in connection with authenticating customers, the types of covered accounts it offers or

³ Certain information was considered "high risk" if the factors identified indicated a higher risk of fraud. For example, if a phone was prepaid, recently transferred to a new provider, or allowed calls to be made over the internet, or if an email address was relatively new.

maintains, and its previous experiences with identity theft. A violation of Rule 201 of Regulation S-ID is also a violation of Rule 2010.

From December 2018 through April 2019, SoFi's identity theft program was not reasonable. First, SoFi failed to identify SoFi Money as a covered account in its written ITPP until April 2019.

Second, as described herein, SoFi failed to implement a reasonable program to respond to red flags of identity theft identified elsewhere in the ITPP. For example, the firm's ITPP noted red flags of identity theft, including inconsistencies in the personal identifying information such as an address that does not match a consumer report, or the SSN has not been issued or is listed on the Social Security Administration's Death Master File, or personal identifying information presented has been used on an account the firm knew was fraudulent.

Red flags identified in SoFi's ITPP were outlined in certain vendor reports. In addition, it had information that some of the applicants had previously been rejected for other SoFi accounts. Nonetheless, because the application satisfied SoFi's threshold for automatic approval, the firm did not review the reports and therefore failed to reasonably respond to these red flags. To the contrary, it automatically approved the accounts without further investigation.

Third, SoFi failed to implement timely reviews of other red flags that it separately detected. SoFi's systems generated fraud alerts associated with some of the accounts described herein. The firm's policies and procedures required review of fraud alerts within 48-72 hours of the alert's generation. However, due to the large volume of fraud alerts generated by the third party fraud, the firm took an average of 63 days—and in some instances up to 132 days—to review the alerts. While alerts were pending for review, SoFi failed to put any holds or restrictions on the corresponding accounts and, in some instances, funds were withdrawn from accounts opened with stolen identities while the fraud alerts were being reviewed. Prior to offering SoFi Money to the public, consultants SoFi hired to test the firm's fraud detection and supervisory systems recommended that SoFi increase staff to review suspicious activity because, based on projected growth forecasts, the number of alerts generated would not be capable of being addressed with the firm's current resources. SoFi, however, did not hire additional staff sufficient to meet its projected growth forecasts prior to making SoFi Money available to the public.

Therefore, SoFi violated Rule 201 of Regulation S-ID and FINRA Rule 2010.

B. Respondent also consents to the imposition of the following sanctions:

- a censure; and
- a \$1,100,000 fine.

Respondent agrees to pay the monetary sanction upon notice that this AWC has been accepted and that such payment is due and payable. Respondent has submitted an Election of Payment form showing the method by which it proposes to pay the fine imposed.

Respondent specifically and voluntarily waives any right to claim an inability to pay, now or at any time after the execution of this AWC, the monetary sanction imposed in this matter.

The sanctions imposed in this AWC shall be effective on a date set by FINRA.

II.

WAIVER OF PROCEDURAL RIGHTS

Respondent specifically and voluntarily waives the following rights granted under FINRA's Code of Procedure:

- A. To have a complaint issued specifying the allegations against it;
- B. To be notified of the complaint and have the opportunity to answer the allegations in writing;
- C. To defend against the allegations in a disciplinary hearing before a hearing panel, to have a written record of the hearing made, and to have a written decision issued; and
- D. To appeal any such decision to the National Adjudicatory Council (NAC) and then to the U.S. Securities and Exchange Commission and a U.S. Court of Appeals.

Further, Respondent specifically and voluntarily waives any right to claim bias or prejudgment of the Chief Legal Officer, the NAC, or any member of the NAC, in connection with such person's or body's participation in discussions regarding the terms and conditions of this AWC, or other consideration of this AWC, including its acceptance or rejection.

Respondent further specifically and voluntarily waives any right to claim that a person violated the ex parte prohibitions of FINRA Rule 9143 or the separation of functions prohibitions of FINRA Rule 9144, in connection with such person's or body's participation in discussions regarding the terms and conditions of this AWC, or other consideration of this AWC, including its acceptance or rejection.

III.

OTHER MATTERS

Respondent understands that:

- A. Submission of this AWC is voluntary and will not resolve this matter unless and until it has been reviewed and accepted by the NAC, a Review Subcommittee of the NAC, or the Office of Disciplinary Affairs (ODA), pursuant to FINRA Rule 9216;
- B. If this AWC is not accepted, its submission will not be used as evidence to prove any of the allegations against Respondent; and
- C. If accepted:
 - 1. this AWC will become part of Respondent's permanent disciplinary record and may be considered in any future action brought by FINRA or any other regulator against Respondent;
 - 2. this AWC will be made available through FINRA's public disclosure program in accordance with FINRA Rule 8313;
 - 3. FINRA may make a public announcement concerning this agreement and its subject matter in accordance with FINRA Rule 8313; and
 - 4. Respondent may not take any action or make or permit to be made any public statement, including in regulatory filings or otherwise, denying, directly or indirectly, any finding in this AWC or create the impression that the AWC is without factual basis. Respondent may not take any position in any proceeding brought by or on behalf of FINRA, or to which FINRA is a party, that is inconsistent with any part of this AWC. Nothing in this provision affects Respondent's right to take legal or factual positions in litigation or other legal proceedings in which FINRA is not a party. Nothing in this provision affects Respondent's testimonial obligations in any litigation or other legal proceedings.
- D. Respondent may attach a corrective action statement to this AWC that is a statement of demonstrable corrective steps taken to prevent future misconduct. Respondent understands that it may not deny the charges or make any statement that is inconsistent with the AWC in this statement. This statement does not constitute factual or legal findings by FINRA, nor does it reflect the views of FINRA.

The undersigned, on behalf of Respondent, certifies that a person duly authorized to act on Respondent's behalf has read and understands all of the provisions of this AWC and has been given a full opportunity to ask questions about it; that Respondent has agreed to the AWC's

provisions voluntarily; and that no offer, threat, inducement, or promise of any kind, other than the terms set forth in this AWC and the prospect of avoiding the issuance of a complaint, has been made to induce Respondent to submit this AWC.

March 14, 2024

Date

Tobin McDaniel

SoFi Securities LLC
Respondent

Print Name: Tobin McDaniel

Title: President

Reviewed by:

Susan Schroeder

Susan Schroeder
Counsel for Respondent
WilmerHale
7 World Trade Center
250 Greenwich Street
New York, NY 10007

Accepted by FINRA:

Signed on behalf of the
Director of ODA, by delegated authority

May 2, 2024

Date

Maya Krugman

Maya Krugman
Senior Counsel
FINRA
Department of Enforcement
200 Liberty Street
New York, NY 10821