FINANCIAL INDUSTRY REGULATORY AUTHORITY
LETTER OF ACCEPTANCE, WAIVER, AND CONSENT
NO. 2022076038801

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

RE: Stash Capital LLC (Respondent)
Member Firm
CRD No. 287728

Pursuant to FINRA Rule 9216, Respondent Stash Capital 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

Stash Capital LLC has been a FINRA member since August 2017. The firm, which is headquartered in New York, New York, offers self-directed investing through online brokerage accounts. Stash Capital has approximately 15 registered representatives.[1]

OVERVIEW

Between January 2019 and June 2023, Stash Capital failed to establish and maintain a customer identification program that was reasonable in light of the size and nature of the firm's business and customer base in violation of FINRA Rules 3310(b) and 2010. Stash Capital also failed to develop and implement an anti-money laundering compliance program reasonably designed to detect and cause the reporting of suspicious transactions in violation of FINRA Rules 3310(a), 3310(f), and 2010.

During the same period, the firm also failed to develop and implement a written Identity Theft Prevention Program reasonably designed to detect, prevent, and mitigate identity theft in violation of Rule 201 of Regulation S-ID of the Securities Exchange Act of 1934 and FINRA Rule 2010.

[1] For more information about the firm, visit BrokerCheck® at www.finra.org/brokercheck.

For these violations, Stash Capital is censured and fined $450,000.

FACTS AND VIOLATIVE CONDUCT

This matter arose from a FINRA examination of Stash Capital.

A. Stash Capital failed to develop and implement a reasonable AML program.

FINRA Rule 3310 requires each member firm to "develop and implement a written anti-money laundering program reasonably designed to achieve and monitor the [firm's] compliance with the requirements of the Bank Secrecy Act (BSA) (31 U.S.C. 5311, et seq.), and the implementing regulations promulgated thereunder by the Department of the Treasury."

A violation of FINRA Rule 3310 also constitutes a violation of FINRA Rule 2010, which requires member firms to "observe high standards of commercial honor and just and equitable principles of trade" in the conduct of their business.

Stash Capital provides online brokerage accounts. During the relevant period, the firm grew rapidly and, by the end of 2023, the firm had opened more than 9 million customer accounts since its inception. From January 2019 to June 2023, the firm failed to develop and implement an AML program that was reasonably designed to achieve compliance with the BSA and its implementing regulations in light of the size and nature of the firm's customer base.

1. Stash Capital failed to establish and implement a customer identification program reasonably designed to verify customers' identities.

FINRA Rule 3310(b) requires member firms to establish and implement policies, procedures, and internal controls reasonably designed to achieve compliance with the requirements of the BSA and its implementing regulations. One of the U.S. Department of the Treasury's implementing regulations, 31 C.F.R. § 1023.220, requires every broker-dealer, as part of its AML compliance program, to establish, document, and maintain a written customer identification program (CIP) that is appropriate for the firm's size and business.

A firm's CIP must include risk-based procedures for verifying customers' identities to the extent reasonable and practicable, and those procedures must enable the firm to form a reasonable belief that it knows the true identity of each customer. Absent an exception, firms must obtain, at a minimum, the following information prior to opening an account: name; date of birth for an individual; address; and an identification number (*e.g.*, a tax identification number for a U.S. person or a passport number for a non-U.S. person). The CIP procedures must be based on the firm's assessment of the relevant risks, including those presented by its size, location, customer base, account types, and methods of opening accounts. The CIP also must include procedures for responding to circumstances

in which the broker-dealer cannot form a reasonable belief that it knows the true identity of a customer, including when the firm should not open an account.

From January 2019 to June 2023, Stash Capital failed to establish and maintain a written CIP that was reasonably designed to verify customers' identities, because its account approval process caused customer accounts to be opened without a reasonable review of potential indications that the customer's identity was not verified, including incomplete CIP information. Prior to February 2022, the firm's written procedures did not reasonably describe its CIP processes, including how the firm verified customers' identities, what databases the firm searched, when and how the firm would manually review customer information, or how the firm would respond to red flags encountered during the application and account opening process.

In practice, Stash Capital used several proprietary and third-party automated systems to verify customer identities. The initial system used by the firm either approved customer applications or designated them as rejected (*e.g.*, identity could not be verified) or indeterminate (*e.g.*, identifying information was verified but there was an alert for potential identity theft). Stash Capital submitted accounts deemed rejected or indeterminate through additional automated reviews, which did not address the specific reasons that certain customer account applications were designated rejected or indeterminate in the initial verification. As a result, the firm approved numerous applications without sufficiently forming a reasonable belief that it knew the true identity of each of its customers.

For example, the firm approved customer accounts without obtaining complete and valid social security numbers as required by the CIP rules. Between January 2019 and April 2022, the firm approved approximately 350 accounts despite applicants providing only the last four digits of a social security number; the firm inaccurately believed its vendor had been verifying complete social security numbers. In other instances, Stash Capital approved certain customers that purported to be born in the 1930s and 1940s without additional verification, despite the presence of other indicia of potential identity fraud for those customers during the application process.

In February 2022, the firm enhanced its written CIP, including identifying the databases searched and the order in which they were searched. In June 2023, the firm revised its procedures related to verifying customer identities in instances where customer accounts were designated rejected or indeterminate in the initial verification.

As a result of Stash Capital's failure to establish and implement a CIP reasonably designed to verify customers' identities from January 2019 to June 2023, the firm violated FINRA Rules 3310(b) and 2010.

2. Stash Capital failed to establish and implement policies and procedures that could be reasonably expected to detect and cause the reporting of suspicious transactions.

FINRA Rule 3310(a) provides a firm must "[e]stablish and implement policies and procedures that can be reasonably expected to detect and cause the reporting of transactions required under 31 U.S.C. 5318(g) and the implementing regulations thereunder." Implementing regulation 31 C.F.R. § 1023.320 requires every broker-dealer, in specified circumstances, to file with the Financial Crimes Enforcement Network (FinCEN) a suspicious activity report (SAR) of "any suspicious transaction relevant to a possible violation of law or regulation." In addition, FINRA Rule 3310(f)(ii) requires, in relevant part, that a firm's AML program include appropriate risk-based procedures for conducting ongoing customer due diligence to include, but not be limited to, conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.

Regulatory Notice 19-18, issued in May 2019, provided examples of red flags suggestive of suspicious activity, including, among others where a "customer is publicly known or known to the firm to have criminal, civil or regulatory proceedings against him or her for crime, corruption or misuse of public funds, or is known to associate with such persons. Sources for this information could include news items, the Internet or commercial database searches." Notice 19-18 further explained that "[u]pon detection of red flags through monitoring, firms should consider whether additional investigation, customer due diligence measures or a [suspicious activity report] SAR filing may be warranted."

Between January 2019 and June 2023, Stash Capital failed to establish and implement policies and procedures in its AML program that could have reasonably been expected to cause the reporting of transactions in accounts where red flags of potential new account fraud provided the firm with knowledge of or reason to suspect suspicious activity in those accounts. The firm's procedures omitted identification of AML-specific red flags, including ones directly relevant to the firm's business. For example, the procedures did not reference red flags relating to customers publicly known or known to the firm to have criminal, civil or regulatory proceedings against them for crime, corruption or misuse of public funds.

In practice, Stash Capital identified suspicious activity using automated alerts that flagged only deposits and withdrawals of funds deemed large or excessively frequent by the firm. Moreover, the firm had no comprehensive policies or procedures that linked red flags present in the account opening process with red flags that arose after the account had been opened, whether related to additional information learned about the customer, the customer's risk profile, or related to specific transactions in the customer's account. Instead, the firm relied solely on manual reviews by Stash Capital personnel to discover and identify any links between red flags in the account opening process and red flags that arose later, despite the millions of customer accounts held at the firm.

From 2019 to June 2023, Stash Capital failed to detect, reasonably investigate, and report suspicious transactions occurring through the firm. For example, the firm did not identify approximately 200 accounts that had been opened using a common phone number. Stash Capital's clearing firm notified Stash Capital that it had identified many such accounts as part of a group potentially engaging in suspicious requests to reverse electronic payments that appeared to be indicative of attempted securities free riding. The firm previously locked certain of the accounts for reasons unrelated to having a common phone number, and subsequently locked the additional accounts identified by its clearing firm. However, the firm did not take additional investigative steps regarding the use of the common phone number and allowed additional accounts to be opened using the same number flagged by its clearing firm for almost six additional months. Similarly, during the relevant period, Stash Capital failed to timely detect that numerous unrelated accounts were opened using email addresses that were routed to the same inboxes or were opened using temporary email address domains.

Therefore, Stash Capital violated FINRA Rules 3310(a), 3310(f)(ii), and 2010.

B. Stash failed to develop and implement a reasonable identity theft prevention program (ITPP).

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, a firm should consider a number of factors, including the methods of accessing covered accounts, the types of covered accounts it offers or maintains, and its previous experiences with identity theft.

A violation of Rule 201 of Regulation S-ID is also a violation of FINRA Rule 2010.

From January 2019 to June 2023, Stash Capital failed to develop and implement a reasonable ITPP. Prior to October 2021, the firm primarily relied on customers to report instances where they believed their identity had been stolen or on its clearing firm to report when mail could not be delivered to customers' purported mailing addresses. Even when alerted to potential identity theft methods, the firm failed to take timely corrective action with respect to its ITPP. For instance, the firm did not implement written procedures for monitoring for accounts using shared phone numbers until May 2022, despite its clearing firm identifying this issue as early as 2020. Moreover, even when the firm implemented a procedure, its ITPP failed to identify who was responsible for monitoring, how often the monitoring should be performed, or what the firm would do with the results. Finally, as described above, the firm failed to reasonably respond to red flags of potential identity theft identified in its account opening process, instead

approving certain accounts on an automated basis even if the accounts exhibited indicia of potential identity theft.

Throughout the relevant period, the firm made periodic updates to its ITPP, and in June 2023 began implementing new procedures to review red flags of identity theft in its account opening process.

Therefore, Stash Capital 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 $450,000 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 18, 2026
Date

Brandon Krieg
Stash Capital LLC
Respondent
Print Name: Brandon Krieg
Title: CEO

Reviewed by:

Joseph Floren
Joseph Floren
Ali Rivett
Counsel for Respondent
Morgan, Lewis & Bockius LLP
600 Montgomery Street, Suite 2300
San Francisco, CA 94111-2725

Accepted by FINRA:

March 20, 2026
Date

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

Myla G. Arumugam
Myla G. Arumugam
Senior Counsel
FINRA
Department of Enforcement
581 Main St., 7th Floor
Woodbridge, NJ 07095