

**FINANCIAL INDUSTRY REGULATORY AUTHORITY
LETTER OF ACCEPTANCE, WAIVER, AND CONSENT
NO. 2021071100401**

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

RE: Brex Treasury LLC (Respondent)
Member Firm
CRD No. 299606

Pursuant to FINRA Rule 9216, Respondent Brex Treasury 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

Brex Treasury became a FINRA member firm in 2019 and began onboarding customers in early 2020. The firm provides cash management securities accounts to corporate customers. It has two branch offices and approximately 40 registered persons.¹

OVERVIEW

From 2020 through 2021, Brex Treasury's anti-money laundering (AML) program failed to include reasonably-designed procedures for verifying the identities of customers or for identifying and verifying the identities of beneficial owners of legal entity customers based on the risks presented by the firm's customer base, its online account-opening methods, and the nature of the cash management accounts it offered. During this time, the firm expanded its targeted customer base from venture-backed and middle-market companies to a wider market, including a small-business segment. The firm relied on regulatory technology that was not reasonably designed to verify the identities of new customers and approved hundreds of potentially-fraudulent small business and other corporate accounts. It also failed to have AML policies and procedures reasonably designed to cause the filing of suspicious activity reports (SARs) in connection with transactions in these accounts when required. As a result, Brex Treasury violated FINRA Rules 3310 and 2010.

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

FACTS AND VIOLATIVE CONDUCT

This matter originated from FINRA's 2021 cycle exam of Brex Treasury.

1. Brex Treasury's AML program failed to include reasonably-designed procedures for verifying the identities of customers or for identifying and verifying the identities of the beneficial owners of legal entity customers.

FINRA Rule 3310 requires firms to develop and implement written AML programs that are reasonably designed to achieve and monitor compliance with the requirements of the Bank Secrecy Act (BSA) and its implementing regulations. FINRA Rule 3310(b) further requires firms' AML programs to establish and implement policies, procedures, and internal controls reasonably designed to achieve compliance with the BSA and its implementing regulations. A violation of FINRA Rule 3310 is also a violation of FINRA Rule 2010, which requires firms to observe high standards of commercial honor and just and equitable principles of trade in the conduct of their business.

The BSA and its implementing regulations require broker-dealers to establish, document, and maintain a written customer information program (CIP) appropriate for their size and business as part of their AML programs.² CIPs must include risk-based procedures for verifying the identity of each customer to the extent reasonable and practicable. CIPs must also 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, which should include a description of when the broker-dealer should not open an account and when the broker-dealer should close an account after attempts to verify a customer's identity have failed. CIPs must address situations where, based on the broker-dealer's risk assessment of a new account opened by a customer that is not an individual, the broker-dealer will obtain information about individuals with authority or control over such account when the broker-dealer cannot verify the customer's true identity using documentary or non-documentary methods with respect to the customer alone.

The BSA and its implementing regulations also separately require broker-dealers to establish and maintain written procedures reasonably designed to identify and verify the identity of beneficial owners of legal entity customers and to include such customer due diligence procedures in their AML programs.³

For identification of beneficial owners, broker-dealers must obtain the names, dates of birth, addresses, and identification numbers of their legal entity customers' beneficial owners from the individual opening the account on behalf of the legal entity customer at the time a new account is opened, as well as a certification with respect to the accuracy of

² See 31 U.S.C. 31 § 5318(l) and 31 C.F.R. § 1023.220.

³ See 31 C.F.R. § 1010.230. For purposes of these requirements, a beneficial owner is defined to include each individual directly or indirectly owning 25% or more of the equity interests of the customer plus a single individual with significant responsibility to control, manage, or direct the customer, such as an executive officer or senior manager; and legal entity customers are defined to exclude certain categories of legal entities, including, for example, SEC-registered investment advisers and investment companies.

that information from the individual.⁴ Broker-dealers may rely on the identifying information about beneficial owners that they obtain in accordance with this requirement, provided they have no knowledge of facts that would reasonably call into question the reliability of such information.

For verification of beneficial owners of legal entity customers, broker-dealers' procedures must contain the elements required for verifying individual customers under the CIP regulation. In particular, broker-dealers must have procedures for using the beneficial owner identifying information they obtain from each customer to verify the identity of each beneficial owner and for responding to circumstances in which the broker-dealer cannot form a reasonable belief that it knows their true identity, which should include a description of when the broker-dealer should not open an account and when the broker-dealer should close an account after attempts to verify a beneficial owner's identity fail. Broker-dealers must also establish procedures for making and maintaining a record of all information obtained under their beneficial owner identity verification procedures. Such records must include, for identification, any identifying information obtained; and for verification, a description of any document relied on, of any non-documentary methods and the results of any measures undertaken, and of the resolution of each substantive discrepancy.

a. Brex Treasury primarily relied on an automated identity-verification algorithm that was not reasonably designed to achieve compliance with the applicable AML requirements.

From its inception in 2020 through 2021, Brex Treasury relied on a software algorithm as its primary procedure—in conjunction with manual review in certain instances—for verifying the identities of new legal entity customers, for identifying and verifying the identities of their beneficial owners, and for determining when the firm should not open an account.

In relevant part, Brex Treasury's identity-verification algorithm attempted to match certain beneficial owner information provided by the customer through an online account application to known identities on file with various identity vendors. If there was a match that the algorithm considered sufficient, then the algorithm conducted a series of risk-based fraud checks. For example, certain fraud checks involved querying third-party databases for information about the beneficial owners and others required uploading a copy of the beneficial owner's photo ID for automated review. Beginning in early 2021, the algorithm incorporated a machine learning model to assign a score to each customer that helped determine how to evaluate the results of certain fraud checks.⁵ If the algorithm considered the applicable fraud checks to have been passed, then the account

⁴ See 31 C.F.R. § 1010.230(b)(1).

⁵ Unlike traditional rules-based programming, machine learning models learn from input data to make predictions or identify meaningful patterns without being explicitly programmed to do so; as a result, they can be considered an artificial intelligence technology. See, e.g., FINRA, *Report on Artificial Intelligence (AI) in the Securities Industry* at 2 (June 2020), available at <https://www.finra.org/rules-guidance/key-topics/fintech/report/artificial-intelligence-in-the-securities-industry>.

could be automatically approved. Otherwise, the algorithm could either automatically reject the account; request and analyze additional information (such as a photo ID, if one had not already been required); or escalate the application for manual review.

Brex Treasury's identity-verification algorithm was not reasonably designed to achieve compliance with the applicable AML requirements. The algorithm had substantive weaknesses, including that it did not collect all of the identifying information required from customers and that it allowed accounts to be opened without a reasonable review of information from the firm's fraud checks that may have raised red flags about the true identity of a legal entity customer or beneficial owner.

Brex Treasury's identity-verification algorithm relied in part on matching information about purported beneficial owners to known identities. Initially, however, the firm did not collect all of the identifying information required for beneficial owners in accordance with the BSA implementing regulations discussed above. Instead, the firm collected only the names and phone numbers of beneficial owners from prospective customers and not dates of birth, addresses, or identification numbers. Using only that limited information, the firm queried a third-party vendor for a similar identity. If the vendor's files contained an identity it considered at least a "strong" match to the applicant's name and a "possible" match to the applicant's phone number, then the firm sought the remaining pieces of identifying information required for beneficial owners indirectly from the vendor. If the vendor could provide that information then the firm's identity-verification algorithm considered the applicant's beneficial owner to be a match for the identity on file at the vendor. In January 2021, the firm began to collect the name, date of birth, address, and identification number for each beneficial owner directly from legal entity customers. The firm then submitted this information to its identity vendor. If the vendor had a matching identity in its files with the same name and identification number, the firm considered the identity of the beneficial owner verified, as long as *either* the date of birth or address were also an exact match. In this scenario, however, the firm did not reasonably consider whether the date of birth or address that did not match presented a substantive discrepancy or otherwise required resolution in order for the firm to reach a reasonable belief that it knew the true identity of the beneficial owner or the legal entity customer.

Brex Treasury also conducted automated fraud checks on new accounts, some of which incorporated an external "fraud score" provided by a third-party vendor. This external fraud score was intended to reflect the relative risk of potential identity fraud associated with the beneficial owner information being presented for review and ranged from zero to one, with one representing the highest risk. The score was accompanied by "reason codes" showing the particular discrepancies or indicators of potential identity fraud that were present or had contributed to the fraud score. For example, there was a reason code to indicate that the identity being presented had been previously reported as stolen.

Brex Treasury's identity-verification algorithm did not reasonably evaluate information the firm obtained during its fraud checks that may have called into question the true identity of a legal entity customer or beneficial owner. For example, the firm set unreasonably high thresholds before the vendor's fraud score would trigger additional

review and did not incorporate certain probative reason codes into the algorithm. As a result of this process, the firm approved the opening of certain accounts despite the presence of red flags associated with the vendor's fraud score and reason codes.

By early 2021, Brex Treasury was allowing applications to bypass manual reviews of certain fraud check results based on the results of a machine learning account risk model that generated an "ARM score" for prospective accounts using various attributes of prospective customers and beneficial owners as inputs. The ARM score was intended to roughly correspond to the risk of fraud generally, including the risk of new account fraud involving a stolen or synthetic beneficial owner identity. At times during the relevant period, if a prospective customer's ARM score fell below thresholds the firm had deemed indicative of a lower-risk account, then the firm's identity verification algorithm did not require manual review for certain fraud checks. However, the firm had initially developed the account risk model by taking data primarily from its historical customer base of venture-backed and middle-market companies and attempting to apply it to a wider potential customer base that included small business customers. Those customers were relatively higher-risk because, for example, small businesses were less likely to have funding from professional investors and less likely to have been referred to the firm through its network of strategic partners in the startup community. But because the firm did not have reasonable policies and procedures governing the design, testing, and validation of the account risk model or the identity-verification algorithm in general, the technology was not generalizable to that wider population.

Due to the weaknesses in its identity-verification algorithm, Brex Treasury verified certain identities and approved new accounts despite substantive discrepancies and red flags of potential identity fraud. For example, the firm automatically approved an account for a self-described "fBusiness [sic] financial technology & sotffware [sic] development" company whose beneficial owner was flagged by the firm's identity vendor for having a fraud score of .992 and by the firm's photo ID vendor for presenting an ID with a potentially manipulated image. In another example, the firm automatically approved an account for a self-described "e-commerce" company with two beneficial owners, one of whom appeared to be applying from a high-risk jurisdiction that didn't match his stated address. The firm's identity vendor also flagged date-of-birth, address, and phone number discrepancies and the firm's photo ID vendor flagged the other owner's foreign passport as potentially fake.

b. Brex Treasury also relied on a manual customer screening process that was not reasonably designed to achieve compliance with the applicable AML requirements.

Brex Treasury's written policies and procedures for the manual screening of account applications were also not reasonably designed to verify customers or to identify and verify beneficial owners of legal entity customers. The firm's written procedures, training materials, and other guidance did not include reasonable standards for (i) what these manual reviews should include, (ii) the criteria and parameters that reviewers should use to make a decision, or (iii) how decisions should be documented. As a result, the firm was unable to ensure that its manual reviews permitted the firm to reach a reasonable

belief that it knew the true identities of customers or beneficial owners. For example, the firm manually approved an account for a company whose beneficial owner had a vendor fraud score of .995 without resolving the identity discrepancies flagged by the vendor, instead noting only: “Not enough information to determine if fraudulent. Ok to onboard[.]” In another example, the firm manually approved an account for a company despite the beneficial owner’s high vendor fraud score and unresolved identity discrepancies, instead noting only: “benefit of the doubt.”

c. Brex Treasury approved hundreds of potentially fraudulent accounts that attempted over \$15 million of transactions using deposited funds that failed to settle.

From 2020 through 2021, as a result of the violative conduct described above, Brex Treasury approved hundreds of potentially fraudulent accounts that attempted over \$15 million of transactions using deposited funds that failed to settle. In these incidents, new accounts that had been approved using the firm’s unreasonable identity-verification processes initiated ACH or check deposits from external accounts and then withdrew or spent the funds that the firm made available. Subsequently, those deposits were recalled as unauthorized, rejected due to insufficient funds, or refused for other reasons. After reversing such deposits, the firm in most cases could not recover the funds or confirm the customers’ true identities.⁶

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

2. Brex Treasury’s AML program was not reasonably designed to cause the reporting of suspicious activity.

FINRA Rule 3310(a) requires firms to establish and implement policies and procedures in their AML programs 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. Those regulations require broker-dealers to file SARs with the United States Department of the Treasury’s Financial Crimes Enforcement Network to report certain suspicious transactions conducted or attempted by, at, or through the broker-dealer that involve or aggregate funds or other assets of at least \$5,000, including transactions that the broker-dealer knows, suspects, or has reason to suspect have no apparent lawful purpose or involve use of the broker-dealer to facilitate criminal activity.⁷ In addition, FINRA Rule 3310(f)(ii) requires that firms’ AML programs 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.

During the relevant period, Brex Treasury failed to establish or implement policies or procedures for its AML program that could have been reasonably expected to cause the

⁶ By reversing the deposits, Brex Treasury reimbursed any innocent third parties whose funds may have been transferred from their external accounts without their authorization.

⁷ See 31 C.F.R. § 1023.320(a)(2)(iii)-(iv).

reporting of transactions in accounts where red flags of potential new account fraud or fraudulent ACH or check deposits provided the firm with knowledge or reason to suspect that those transactions had no apparent lawful purpose or may have involved the use of the firm to facilitate criminal activity.

Brex Treasury monitored AML alerts generated by certain AML exception reports to determine if a SAR should be filed to report the alerted transaction. However, those AML exception reports focused narrowly on certain patterns of money movement that the firm deemed to be “behavior associated with financial crime schemes.” Although the firm also had broader transaction-based fraud surveillance that generated fraud alerts, it monitored those fraud alerts primarily to reject suspicious transactions and to close accounts. Fraud alerts involving potentially-reportable transactions could be manually escalated for AML review and disposition. However, the firm did not have procedures, training, or guidance for monitoring fraud alerts reasonably designed to ensure it consistently identified potentially-reportable transactions for escalation in that process. As a result, the firm failed to establish and implement policies and procedures to reasonably consider whether SAR filings were required in connection with the majority of new account fraud incidents during the relevant period.

In response to the events described in this AWC, Brex Treasury began taking steps to improve its procedures for screening legal entity customers and their beneficial owners, its suspicious activity reporting, and its overall AML program with respect to the issues identified in this AWC. In particular, the firm began updating its policies, procedures, and systems; hiring additional experienced staff, including at senior levels; and engaging a third-party consultant to review the firm’s AML program.

Therefore, Brex Treasury violated FINRA Rules 3310(a), 3310(f)(ii), and 2010.

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

- a censure and
- a \$900,000 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.

August 27, 2024

Date

Erik Zhou

Brex Treasury LLC
Respondent

Print Name: Erik Zhou

Title: President

Reviewed by:

Susan Schroeder

Susan Schroeder
Counsel for Respondent
Wilmer Cutler Pickering Hale and Dorr LLP
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

August 30, 2024

Date

Andrew Boldt

Andrew Boldt
Senior Counsel
FINRA
Department of Enforcement
55 West Monroe Street, Suite 2600
Chicago, IL 60603