NEW YORK STATE
DEPARTMENT OF FINANCIAL SERVICES
ONE STATE STREET
NEW YORK, NEW YORK 10004

----------x

In the Matter of :

BLOCK, Inc.
BLOCK OF DELAWARE:
:

----------x

CONSENT ORDER

The New York State Department of Financial Services (the "Department" or "DFS") and Block, Inc. d/b/a Block of Delaware and Block of Delaware ("Block" or "the Company") are willing to resolve the matters described herein without further proceedings;

WHEREAS, Block is a publicly-traded financial services and technologies company. In 2023, Block had revenue of $21.91 billion. The Company's total assets more than doubled from 2021 to 2023, growing from $15.02 billion to $34.06 billion;

WHEREAS, Block, formerly known as Square, Inc., has been licensed by the Department to operate a money transmission business in New York State pursuant to New York Banking Law § 641 since 2013. In June 2018, the Department issued Block a BitLicense,

permitting Block conduct Virtual Currency Business Activity ("VCBA"), as defined by 23 NYCRR § 200.02(q), in New York State;

WHEREAS, Block owns and operates Cash App, a peer-to-peer money transmission service that allows users to send and receive fiat currency. In 2018, Block began offering Bitcoin transactions through Cash App;

WHEREAS, the Department conducted two full-scope examinations of Block covering both its money transmitter ("MT") license and BitLicense ("VC");

WHEREAS, the Money Transmitter Examination ("MT Exam") covered the period of April 1, 2021 through September 30, 2022 and the Virtual Currency Examination ("VC Exam") covered the period of February 28, 2021 through September 30, 2022;

WHEREAS, following the MT Exam and VC Exam, the Department initiated an enforcement investigation into Block's compliance with applicable laws and regulations, including but not limited to anti-money laundering ("AML") regulations, consumer protection regulations, and the Department's Virtual Currency Regulation (23 NYCRR Part 200); and

WHEREAS, the MT Exam and the VC Exam, as well as the subsequent enforcement investigation, identified serious compliance deficiencies with respect to Block's Bank Secrecy Act/Anti-Money Laundering ("BSA/AML") program. These failures include insufficient Know-Your-Customer ("KYC") and transaction monitoring processes, and a backlog of Suspicious Activity Reports ("SARs") during 2018-2021, which together created a high-risk environment vulnerable to exploitation by criminal actors. The Department also identified violations of the Department's consumer protection regulations.

NOW THEREFORE, in connection with an agreement to resolve this matter without further proceedings, pursuant to the Superintendent's authority under Sections 39 and 44 of the New York Banking Law, the Department finds as follows:

THE DEPARTMENT'S FINDINGS

Introduction

1. The Department is the primary financial services regulator in the State of New York and the Superintendent of Financial Services (the "Superintendent"), is responsible for ensuring the safety, soundness, and prudent control of the various financial services businesses under the Department's supervision. To that end, the Superintendent enforces the laws and regulations applicable to the financial services, insurance, and banking sectors, including the New York Financial Services Law, the New York Banking Law, and the regulations promulgated thereunder.

2. The Superintendent has the authority to conduct investigations, to bring enforcement proceedings, to levy monetary penalties, and to revoke the license of entities who have violated the relevant laws and regulations.

Applicable Laws and Regulations

3. Block, licensed as both a money transmitter and a BitLicensee, is subject to a rigorous set of BSA/AML regulations promulgated by the Department and designed to promote the safety and soundness of the financial services industry by reducing and eliminating fraud, abuse, and unethical conduct. Additionally, Block is required to adhere to the law and the Department's regulations regarding cybersecurity and consumer protection.

Money Transmitter Regulations

4. The regulations specific to money transmitters' obligations to maintain an AML program are found in Part 417 of the Superintendent's Regulations. Specifically, Section 417.2

of the New York Codes, Rules, and Regulations requires money transmitter licensees to establish and maintain an AML program that complies with all applicable Federal anti-money laundering laws. Section 417.2 additionally requires each licensee to "demonstrate that it has in place risk-based policies, procedures and practices to ensure, to the maximum extent practicable, that its transactions comply with Office of Foreign Assets Control ("OFAC") requirements" and to comply with KYC requirements under Federal law.

5. Money transmitter licensees are further subject to the consumer protection requirements contained in 3 NYCRR § 406.

The Virtual Currency Regulation

6. The Department developed and oversees a first-of-its-kind regulatory framework pertaining to virtual currency businesses. Companies that conduct VCBA in the State of New York must be licensed to do so by the Department — either through the Department's BitLicense or a Limited Purpose Trust Company Charter — and are subject to the Department's ongoing supervision.

7. The specific obligations of those companies operating pursuant to a BitLicense are set forth in the Virtual Currency Regulation. The licensing and compliance requirements contained in the Virtual Currency Regulation include the requirement that each licensee develop and implement various compliance policies and programs, including a robust AML program, *see* 23 NYCRR § 200.15, a cybersecurity program, *see* 23 NYCRR § 200.16, and a comprehensive business continuity and disaster recovery ("BCDR") policy, *see* 23 NYCRR § 200.17; and ensure that consumers are fully informed as to all aspects of the transactions they enter into, *see* 23 NYCRR § 200.19.

Events at Issue

Background

8. Block is a Delaware corporation that, through its various lines of business, offers an array of financial services and products designed to help both businesses and individual consumers store, receive, spend, and invest their money. Block is licensed by the Department to engage in the business of money transmission and VCBA in the State of New York.

9. The Department, through reviews conducted during both the MT Exam and the VC Exam, as well as during the enforcement investigation, determined that Block failed to maintain a compliant and effective AML program, as well as failed to comply with other critical requirements contained in the Superintendent's Money Transmitter and Virtual Currency Regulations.

10. The policies, procedures, and processes at Block did not keep pace with the significant growth the Company experienced immediately prior to and during the period covered by the MT Exam and VC Exam, resulting in Block's inability to fully comply with its obligation to effectively monitor, and thereafter report, the transactions being conducted on its platforms for suspected money laundering and other illicit criminal activity.

Deficiencies in Block's Anti-Money Laundering Program

11. Section 417.2 of the Superintendent's Regulations requires that each licensee establish and maintain an AML program that complies with applicable federal laws and regulation. Federal regulation dictates that money services businesses, such as Block, must develop an effective AML program "that is reasonably designed to prevent the money services business from being used to facilitate money laundering and the financing of terrorist activities." 31 CFR § 1022.210(a). This requirement is reiterated for BitLicensees in the Virtual Currency

Regulation which requires that a licensee's AML program "provide for a system of internal controls, policies, and procedures designed to ensure ongoing compliance with all applicable anti-money laundering laws, rules, and regulations." 23 NYCRR § 200.15(c)(1). Importantly, the Virtual Currency Regulation also requires that licensees "monitor for transactions that might signify money laundering, tax evasion, or other illegal activity." 23 NYCRR § 200.15(e)(3).

12. The AML program run by Block, which governs both fiat and Bitcoin transactions on the Cash App platform, failed to adequately consider the substantial risks posed to an entity of its new size and complexity. This is demonstrated by the suspicious activity alert backlog Block maintained for an extended period of time which delayed the filing of suspicious activity reports ("SARs") and action against potential suspicious activity, insufficient screenings as required for OFAC compliance, and shortcomings in its KYC and Consumer Due Diligence ("CDD") practices, among other things.

Backlog in SAR Filings and Transaction Monitoring Alerts

13. Between 2018 and 2021, Block experienced a significant transaction monitoring alerts backlog. In 2018, Block had accumulated a transaction monitoring backlog of approximately 18,000 alerts, which grew to over 169,000 by 2020. This extensive backlog was caused, in part, by Block's inability to predict the impact of Cash App's growing customer base on alert volumes and staffing needs, as well as the increase in alerts generated by the implementation of new transaction monitoring tools.

14. The backlog of alerts waiting to be processed caused an unacceptable number of days to elapse between the filed SARs' last transaction date and the report filing dates. Block's procedures for investigating and reporting suspicious activity require analysts to review an alert

and document a recommendation to file or not file a SAR within sixty days after an alert is generated.

15. A review conducted by the Department revealed that between February 2021 and September 2022 SARs, for both Bitcoin and fiat transactions, were at times filed over a year after the alerts were first generated. The average number of days between the date of the transaction monitoring alert and the SAR filing was 129 days. The average number of days between the date of the transaction monitoring alert and the start of a case investigation was 70 days, which further delayed Block's reporting of suspicious activity.

16. The backlog and delays in processing transaction alerts allowed potential suspicious, and illicit activity to continue on Block's platforms unaddressed for an extended period.

Transaction Monitoring Failures

17. Pursuant to both Part 417 and Part 200, licensees are required to implement risk-based policies and procedures to ensure compliance with the requirements and regulations of OFAC. OFAC rules and regulations are designed to ensure that licensed entities are not engaging in transactions with sanctioned entities or individuals.

18. Specifically, Section 417.2(c) of the Money Transmitter Regulation and Section 200.15(i) of the Virtual Currency Regulation require that each licensee implement risk-based policies, procedures, and practices to ensure compliance with OFAC regulations.

19. Block utilized information from two vendors to block and alert transactions with exposure to terrorism associated wallets. The Department's investigation revealed that, with respect to one of the vendors, Block's system did not generate alerts on Bitcoin transactions until the recipient's wallet had more than 1% exposure to terrorism-connected wallets, and Block did

not automatically block transactions to wallets with exposure to terrorism-connected wallets until the exposure exceeded 10%. Any amount of funds transferred to terrorism-connected wallets is illegal and setting threshold alerts above 0% without a risk-based analysis supporting that decision, falls short of the regulatory requirement that licensees implement risk-based policies, procedures, and practices to ensure compliance with BSA and OFAC regulations.

20. The Department also determined that existing service providers and employees were not subject to subsequent screening against updated OFAC sanctions listings. In 2021, Block also reported fifteen rejected Bitcoin transactions late with OFAC during the examination period in violation of 31 CFR § 501.604(c). Further, prior to 2023, Block did not conduct OFAC screening for restricted accounts, which transact in fiat and are subject to certain dollar-amount thresholds.

21. Contributing to Block's failure to effectively monitor Bitcoin transactions for sanctioned counterparties, money laundering, and other potential illicit activity risks in violation of Section 200.15(e)(3) of the Virtual Currency Regulation, was Block's deficient monitoring and risk rating of transactions that used anonymizing services aka "mixers," a type of service that obfuscates the source, destination and/or amount involved by combining different users assets in an intermediary wallet. The untraceable and anonymous features of "mixers" makes them highly susceptible to abuse by criminal and sanctioned actors, that pose a threat to National Security.

22. The Department issued guidance on April 28, 2022, in which it identified mixers as a typology virtual currency licensees should be considering when evaluating their transaction monitoring risk. Specifically, the Department's guidance states that "it is important that VC Entities evidence appropriately tailored transaction monitoring coverage against applicable typologies and red flags, identify deviations from the profile of a customer's intended purposes,

and address other risk considerations as applicable. Relevant typologies related to virtual currency business activity include but are not limited to: assessing whether a virtual currency (1) has substantial exposure to a high-risk or sanctioned jurisdiction; (2) is processed through a mixer or tumbler; (3) is sent to or from darknet markets; (4) is associated with scams/ransomware; and (5) is associated with other illicit activity relevant to the VC Entity's business model."[1]

23. The use of mixers allows criminal actors to purchase illicit items on the "darkweb," including drugs, contraband, child sex-abuse material, and other illegal items with little risk of detection. It allows a sender to obscure the ultimate destination of funds, which could end up in the hands of terrorist organizations or sanctioned parties.

24. Despite the Department highlighting the elevated risk of these wallets, Block risk rated transactions identified as having exposure to mixers as "medium" risk, rather than the "high" risk rating that is appropriate.

KYC/CDD Deficiencies

25. A core tenet of an effective AML program is the adoption of a risk based and robust KYC/CDD policies and procedures. Both the Virtual Currency and Money Transmitter regulations require licensees to maintain effective processes and controls to identify and understand the nature and purpose of customer relationships to mitigate the risks related to money laundering and other criminal activity. *See* 3 NYCRR § 417.2(a)(1)(i)(A) and 23 NYCRR § 200.15(h).

26. The Department's investigation identified several deficiencies in Block's KYC/CDD program. For example, Block did not have a formal KYC refresh process to identify

[1] https://www.dfs.ny.gov/industry_guidance/industry_letters/il20220428_guidance_use_blockchain_analytics

changes to a customer's initial KYC information and apply those changes to review and update a customer's risk rating. Further, customers opened multiple accounts using different email addresses and phone numbers, thereby bypassing the transaction limits Block places on certain accounts or individuals.

27. Of particular concern was Block's oversight of Cash App "restricted" accounts. Cash App restricted accounts are only permitted to transact in fiat under a certain limit and do not require the customer to pass full Identity Verification ("IDV"). Block did not prohibit opening of restricted Cash App accounts that shared attributes such as an email, phone number, device, and/or financial instrument with customers that were denylisted for being the subject of a SAR. This allowed bad actors to re-enter Block's platform. During the exam period, Block imposed a transaction limit of $1,000 in a rolling 30-day period for each individual Cash App (fiat only) restricted accounts that used the same linked financial instrument. However, the monetary limit, without the limit on the number of accounts that could be opened, did not constitute an effective control, as individuals could have created multiple restricted accounts using multiple financial instruments, thereby circumventing the transaction limits. For example, a SAR was filed for $1.6 million with 91 subjects that were holders of 16,811 accounts with 19,518 transactions.

28. As part of a 2022 internal investigation, Block self-identified over 8,000 accounts linked to a Russian criminal network. The Department acknowledges the immediate action Block took in response to this issue, which included filing SARs, closing and denylisting the accounts, and implementing new controls. However, this discovery further highlights the gaps in Block's KYC and on-boarding practices. The approximately 25-30 subjects involved in the Russian

criminal network were able to open 8,359 Cash App accounts using falsified information, auto-generated email addresses and phone numbers before the conduct was detected by Block.

Cybersecurity Deficiencies

29. Cash App operates in an entirely virtual environment and collects non-public information ("NPI") for each of its approximately 54 million[2] monthly transacting active accounts, in addition to any new and inactive users registered on the platform. As such, it is critical that Block maintain a robust cybersecurity program to protect its own information systems and the consumer NPI stored in them. Management oversight, as well as ensuring that all cybersecurity policies are sufficient and robust are critical components of the cybersecurity requirements contained in both the Virtual Currency Regulation and the Cybersecurity Regulations (23 NYCRR Part 500).

30. Notwithstanding these regulatory requirements, the Department's examinations and enforcement investigation revealed certain compliance failures within Block's cybersecurity program.

31. Initially, the Department's investigation revealed that Block's Information Security Policy("ISP"), as well as other policies that make up the Company's cybersecurity program were not subject to annual board review and approval, as required by 23 NYCRR § 200.16(b) until October 26, 2023. Instead, ISP review was delegated to Block's Chief Information Security Officer ("CISO"), which falls short of the requirement in Section 200.16(b) that the licensee's cybersecurity policy "be reviewed and approved by the Licensee's board of directors or equivalent governing body at least annually." 23 NYCRR § 200.16(b). The

[2] Estimate as of June 2023.

Department further determined that Block's cybersecurity policy failed to address capacity and performance planning as required by 23 NYCRR § 200.16(b)(5).

32. Block also failed to maintain a compliant Business Continuity and Disaster Recovery ("BCDR") plan. Block's BCDR plan was narrow, addressing only the Company's pandemic response plan and one additional scenario. Section 200.17(a) of the Virtual Currency Regulation requires that a licensee's BCDR plan address the documents, data, facilities, infrastructure, personnel, and competencies essential to the continued operation of the Company's business, the procedures for back up of documents and data essential to the operations of the Company and storing of information offsite, and identification of the third parties necessary for the continued operations of the Company's business. 23 NYCRR § 200.17(a). Though product-level teams at Block undertook business continuity processes, this was not reflected in a companywide BCDR plan that complied with the regulation.

33. Moreover, while Block did conduct testing of its BCDR plan on an annual basis, the Department found no evidence that the tests were observed by qualified internal personnel or qualified third parties, in violation of 23 NYCRR § 200.17(e).

Consumer Protection Deficiencies

34. The Department's regulations require certain disclosures to be made at various points for both Bitcoin and fiat transactions. The Department concluded that while all disclosures required for virtual currency transactions pursuant to 23 NYCRR § 200.19(a) were present, Block failed to present those disclosures to the consumer in "clear, conspicuous, and legible writing." Instead, the required disclosures were disseminated between various pages of the Cash App Terms of Service document.

35. With respect to receipts provided for fiat transactions from a customer's stored balance, Block failed to provide receipts containing the Company's refund policy or a statement of liability for non-delivery or delayed delivery as required by 3 NYCCRR § 406.3(f).

Violations of Law and Regulations

36. Block failed to maintain an effective and compliant anti-money laundering program in violation of 23 NYCRR § 200.15 and 3 NYCRR § 417.2.

37. Block failed to obtain annual approval of its cybersecurity policy by its board of directors, in violation of 23 NYCRR § 200.16(b).

38. Block failed to maintain an adequate business continuity and disaster recovery policy and ensure independent testing of its business continuity and disaster recovery policy, in violation of 23 NYCRR § 200.17.

39. Block failed to provide required disclosures of the risks of virtual currency transactions in a clear and conspicuous manner, in violation of 23 NYCRR § 200.19(a).

40. Block failed to provide required disclosures on receipts for money transmission transactions, in violation of 3 NYCRR § 406.3(f).

NOW THEREFORE, to resolve this matter without further proceedings, the Department and the Company stipulate and agree to the following terms and conditions:

SETTLEMENT PROVISIONS

Monetary Penalty

41. No later than ten (10) days after the Effective Date (as defined below) of this Consent Order, the Company shall pay a total civil monetary penalty pursuant to NYBL § 44(1)(c) to the Department in the amount of Forty Million Dollars and 00/100 Cents

($40,000,000). The payment shall be in the form of a wire transfer in accordance with instructions provided by the Department.

42. The Company shall not claim, assert, or apply for a tax deduction or tax credit with regard to any U.S. federal, state, or local tax, directly or indirectly, for any portion of the civil monetary penalty paid pursuant to this Consent Order.

43. The Company shall neither seek nor accept, directly or indirectly, reimbursement or indemnification with respect to payment of the penalty amount, including but not limited to, payment made pursuant to any insurance policy.

44. In assessing a penalty for the failures alleged in this Consent Order, the Department has taken into account factors that include, without limitation: the extent to which the entity has cooperated with the Department in the investigation of such conduct, the gravity of the violations, and such other matters as justice and the public interest may require.

45. The Department acknowledges Block's cooperation throughout this investigation. The Department also recognizes and credits Block's ongoing efforts to remediate the shortcomings identified in this Consent Order. Among other things, Block has demonstrated its commitment to remediation by devoting significant financial and other resources to resolving backlogs and mitigating the risk of future backlogs, increasing compliance staffing resources, limiting the number of accounts a customer can create, implementing additional controls to better prevent bad actors from accessing or returning to the platform, and updating its BSA/AML and OFAC compliance practices.

Independent Monitor

46. The Company agrees to engage the services of an Independent Monitor selected by the Department for a period of twelve (12) months following the execution of this Consent

Order, extendable by the Department in its sole regulatory discretion. The primary objective of the engagement of the Independent Monitor is to inform and enhance the Company's efforts to remediate any deficiencies in the Company's compliance programs.

47. The Independent Monitor shall base its monitoring on the findings and violations contained in this Consent Order.

a. The Independent Monitor will report to the Department and will: (i) commence a comprehensive review of the effectiveness of Block's BSA/AML and Sanctions programs, which will primarily focus on Block's current programs (the "Compliance Review"); (ii) prepare a written report of findings, conclusions, and recommendations (the "Compliance Report"); and (iii) oversee remedial measures ("Remediation"), as deemed appropriate between the Monitor and the Department. The Compliance Review and Compliance Report will, at a minimum, address and include:

i. A comprehensive, risk-based assessment of Block's compliance with the Virtual Currency Regulation, Money Transmitter Regulation, and Part 504 of the Superintendent's Regulations (the "Transaction Monitoring Regulation");

ii. A review of Block's suspicious activity identification, investigation, escalation, tracking, documentation, and reporting procedures to determine whether Block is meeting its suspicious activity reporting requirements pursuant to 23 NYCRR § 200.15, 3 NYCRR § 417.2, and 3 NYCRR § 504.3;

iii. A review of the adequacy of any planned or implemented corrective measures to prevent the types of historical transaction monitoring alert backlogs referenced in the Consent Order;

iv. A review of a sample, based on the Independent Monitor's expertise, of Block's transaction activity to determine whether transactions inconsistent with or in violation of applicable OFAC regulations or suspicious activity involving high-risk customers or transactions involving possible money laundering, terrorist financing, or other illicit financial activity at, by, or through Block were properly identified and reported in accordance to the relevant OFAC regulations, suspicious activity regulations, and New York State law. Nothing herein shall limit the Independent Monitor's ability to access any transactions it deems appropriate; and

v. A review of Block's Blockchain Analytics Transaction Monitoring (TM) Program to determine whether Block is in compliance with state and federal BSA/AML and OFAC regulations, Part 504 of the Superintendent's Regulations ("Transaction Monitoring Regulations") and the Department's April 28, 2022 "Guidance on Use of Blockchain Analytics."

48. The Independent Monitor shall, as it deems necessary, have system access to all historical data and transactions at the Company from January 1, 2021, to the present.

49. The specific work to be performed by the Independent Monitor described herein will be established through discussions with the Department and may be updated, in the

Department's sole regulatory discretion, after consultation with the Company and the Independent Monitor, as the engagement progresses, and additional information is obtained.

50. The Independent Monitor's report to the Department will summarize the remediation efforts completed and provide a further evaluation of the Company's compliance program, including recommendations for additional remediation that remains necessary, if any.

Full and Complete Cooperation

51. The Company commits and agrees that it will fully cooperate with the Department regarding all terms of this Consent Order.

Further Action by the Department

52. No further action will be taken by the Department against the Company or its successors for the conduct set forth in this Consent Order, or in connection with the remediation set forth in this Consent Order, provided that the Company fully complies with the terms of the Consent Order.

Waiver of Rights

53. The Company submits to the authority of the Superintendent to effectuate this Consent Order.

54. The parties understand and agree that no provision of this Consent Order is subject to review in any court, tribunal, or agency outside of the Department.

Parties Bound by the Consent Order

55. This Consent Order is binding on the Department and the Company, as well as any successors and assigns. This Consent Order does not bind any federal or other state agency or any law enforcement authority.

Breach of Consent Order

56. In the event that the Department believes the Company to be in material breach of the Consent Order, the Department will provide written notice to the Company, and the Company must, within ten (10) days of receiving such notice, or on a later date if so determined in the Department's sole discretion, appear before the Department to demonstrate that no material breach has occurred or, to the extent pertinent, that the breach is not material or has been cured.

57. The Company understands and agrees that its failure to make the required showing within the designated time period shall be presumptive evidence of the Company's breach. Upon a finding that a breach of this Consent Order has occurred, the Department has all the remedies available to it under New York Banking Law and New York Financial Services Law, and any other applicable laws, and may use any evidence available to the Department in any ensuing hearings, notices, or orders.

Notices

58. All notices or communications regarding this Consent Order shall be sent to:

For the Department:

Ndidi C. Obicheta
Senior Assistant Deputy Superintendent
Consumer Protection and Financial Enforcement Division
One State Street
20th Floor
New York, NY 10004

Joseph C. Mineo
Assistant Deputy Superintendent
Consumer Protection and Financial Enforcement Division
One Commerce Plaza
20th Floor
Albany, NY 12257

For Block, Inc. and Block of Delaware:

Chrysty Esperanza
Counsel Lead
1955 Broadway, Suite 600
Oakland, CA 94612

Roberto J. Gonzalez
Paul, Weiss, Rifkind, Wharton & Garrison LLP
2001 K St NW
Washington, DC 20006

Miscellaneous

59. This Consent Order and any dispute thereunder shall be governed by the laws of the State of New York without regard to any conflicts of laws principles.

60. This Consent Order may not be altered, modified, or changed unless in writing and signed by the parties hereto.

61. This Consent Order constitutes the entire agreement between the Department and the Company and supersedes any prior communication, understanding, or agreement, whether written or oral, concerning the subject matter of this Consent Order.

62. Each provision of this Consent Order shall remain effective and enforceable against the Company, its successors, and assigns, until stayed, modified, suspended, or terminated by the Department.

63. In the event that one or more provisions contained in this Consent Order shall for any reason be held to be invalid, illegal, or unenforceable in any respect, such invalidity, illegality, or unenforceability shall not affect any other provision of this Consent Order.

64. No promise, assurance, representation, or understanding other than those contained in this Consent Order has been made to induce any party to agree to the provisions of this Consent Order.

65. Nothing in this Consent Order shall be construed to prevent any consumer or any other third party from pursuing any right or remedy at law.

66. This Consent Order may be executed in one or more counterparts and shall become effective when such counterparts have been signed by each of the parties hereto (the "Effective Date").

[*remainder of this page intentionally left blank*]

IN WITNESS WHEREOF, the parties have caused this Consent Order to be signed on the dates set forth below.

NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES

By: /s/ Ndidi C. Obicheta
NDIDI C. OBICHETA
Senior Assistant Deputy Superintendent
Consumer Protection and Financial Enforcement

April 7, 2025

By: /s/ Madeline W. Murphy
MADELINE W. MURPHY
Deputy Director of Enforcement
Consumer Protection and Financial Enforcement

April 8, 2025

By: /s/ Christopher B. Mulvihill
CHRISTOPHER B. MULVIHILL
Deputy Superintendent
Consumer Protection and Financial Enforcement

April 8, 2025

BLOCK, INC.
BLOCK OF DELAWARE

By: /s/ Jack Dorsey
JACK DORSEY
Principal Executive Officer

April 7, 2025

THE FOREGOING IS HEREBY APPROVED. IT IS SO ORDERED.

/s/ Adrienne A. Harris
ADRIENNE A. HARRIS
Superintendent of Financial Services
April 10, 2025