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

--x

In the Matter of :

BITFLYER USA, INC. :

--x

CONSENT ORDER

The New York State Department of Financial Services (the "Department") and bitFlyer USA, Inc. ("bitFlyer USA" or the "Company") are willing to resolve the matters described herein without further proceedings.

WHEREAS, bitFlyer USA operates a cryptocurrency trading platform in 48 states and the District of Columbia and provides custodial wallet services for U.S. dollars and digital currencies;

WHEREAS, bitFlyer USA is licensed by the Department, pursuant to 23 NYCRR Part 200 (the "Virtual Currency Regulation"), to engage in virtual currency business activity in New York State, is a licensee pursuant to 23 NYCRR § 200.2(f), and is registered with the Financial Crimes Enforcement Network ("FinCEN") as a money service business;

WHEREAS, New York's first-in-the-nation cybersecurity regulation, 23 NYCRR Part 500 (the "Cybersecurity Regulation"), became effective on August 29, 2017;

WHEREAS, the Cybersecurity Regulation was promulgated to strengthen cybersecurity and data protection for the industry and consumers and thus sets out clear standards and guidelines for cooperative industry compliance, robust consumer data protection, and vital cybersecurity controls;

WHEREAS, by virtue of its license, granted pursuant to the Virtual Currency Regulation, bitFlyer USA is a "Covered Entity," pursuant to 23 NYCRR § 500.01(c);

WHEREAS, the Department conducted examinations of bitFlyer USA in 2018 and 2020, together covering the period of November 27, 2017, through September 30, 2020 (the "Examinations");

WHEREAS, through the Examinations, the Department discovered multiple deficiencies in the Company's cybersecurity program, as mandated by both the Cybersecurity Regulation and the Virtual Currency Regulation;

WHEREAS, following the Examinations, the Department initiated an enforcement investigation into bitFlyer USA's cybersecurity program (the "Investigation"); and

WHEREAS, following the Investigation, the Department concluded that bitFlyer USA had violated 23 NYCRR § 500.09(a), which requires a Covered Entity to conduct a periodic risk assessment of its electronic information resources ("Information Systems") sufficient to inform the design of the cybersecurity program, and 23 NYCRR § 200.16, which requires, among other things, that each licensee establish and maintain an effective cybersecurity program and implement a written cybersecurity policy — reviewed and approved by the licensee's board of directors (or equivalent governing body) at least annually—to enact such a program.

NOW THEREFORE, in connection with an agreement to resolve this matter without further proceedings, 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 it licenses and oversees various financial services businesses, including virtual currency businesses such as bitFlyer USA.

2. The Superintendent of the Department of Financial Services (the "Superintendent") is responsible for ensuring the safety, soundness, and prudent conduct of the providers of financial services in New York State and enforcing the various laws and regulations applicable to financial services licensees, including the New York Financial Services Law and the various regulations that have been promulgated thereunder, such as the Cybersecurity and Virtual Currency Regulations.

3. The Superintendent has the authority to conduct investigations and to bring enforcement proceedings, levy monetary penalties, and order injunctive relief against parties who have violated relevant laws and regulations.

4. bitFlyer USA was granted a BitLicense pursuant to 23 NYCRR Part 200 on November 27, 2017.

5. bitFlyer USA was a subsidiary of bitFlyer, Inc. (Japan) until October 1, 2018, when bitFlyer USA, along with bitFlyer, Inc. (Japan), bitFlyer Europe S.A., and bitFlyer Blockchain, Inc., all became wholly owned subsidiaries of bitFlyer Holdings, Inc.

6. Although no longer bitFlyer USA's parent, bitFlyer, Inc. (Japan) still provides bitFlyer USA with product and application development (including operation and maintenance), customer support, information security and incident management, business continuity and disaster recovery, information system development and maintenance, and treasury, accounting, and audit support.

Cybersecurity Program Requirements

7. To support the Superintendent's critical obligation to protect private and personally sensitive consumer data, the Department requires, through its Cybersecurity and Virtual Currency Regulations, that licensees such as bitFlyer USA establish and maintain a cybersecurity program designed to protect the confidentiality, integrity, and availability of their Information Systems, as well as any non-public information ("NPI") contained therein. 23 NYCRR §§ 200.16; 500.02(b).

8. The Cybersecurity Regulation requires that each Covered Entity conduct a periodic risk assessment of its Information Systems sufficient to inform the design of the entity's cybersecurity program and update such risk assessment as necessary to address changes to the Covered Entity's Information Systems, NPI, or business operations. 23 NYCRR § 500.09(a).

9. Further, a Covered Entity's cybersecurity risk assessment must be carried out pursuant to written policies and procedures that include: (1) criteria for evaluating and categorizing identified cybersecurity risks or threats; (2) criteria for assessing the "confidentiality, integrity, security, and availability of the Covered Entity's Information Systems and [NPI]"; and (3) requirements describing how identified risks will be addressed. 23 NYCRR § 500.09(b).

10. The results of the risk assessment should inform the design of the Covered Entity's cybersecurity program (23 NYCRR § 500.02) and policies and procedures (23 NYCRR § 500.03) and should be reported at least annually to the Covered Entity's board of directors (23 NYCRR § 500.04(b)(3)). Additionally, a risk assessment is a necessary prerequisite for compliance with the Department's requirements for penetration testing (23 NYCRR § 500.05), audit trails (23 NYCRR § 500.06), review of access privileges (23 NYCRR § 500.07), third-party provider policies (23 NYCRR § 500.11), implementation of multi-factor authentication (23 NYCRR § 500.12), cybersecurity awareness training (23 NYCRR § 500.14(b)), and data encryption (23 NYCRR § 500.15). As such, a comprehensive risk assessment necessarily precedes the design of an effective cybersecurity program.

11. The Virtual Currency Regulation requires that each licensee establish and maintain an effective cybersecurity program to ensure the availability and functionality of the licensee's electronic systems and to protect those systems and any sensitive data stored on those systems from unauthorized access, use, or tampering. Such a cybersecurity program should identify internal and external cyber risks by, at a minimum, identifying the information stored on the licensee's systems, the sensitivity of such information, and how and by whom such information may be accessed. The cybersecurity program should also protect the licensee's electronic systems and the information stored on those systems from unauthorized access, use, or other malicious acts through the use of defensive infrastructure and the implementation of policies and procedures. Further, a licensee's cybersecurity program must be able to detect systems intrusions, data breaches, unauthorized access to systems or information, malware infiltration, and other cybersecurity events; respond to detected events to mitigate any negative effects; and recover from events and restore normal operations and services. 23 NYCRR

§ 200.16(a). The licensee is required to enact its cybersecurity program via a written policy that must be reviewed and approved at least annually by the licensee's board of directors. 23 NYCRR § 200.16(b).

bitFlyer USA's Compliance Deficiencies

12. Through its Examinations and Investigation, the Department found that bitFlyer USA failed to meet its regulatory obligations both by failing to fully comply with the Department's Cybersecurity Regulation and by failing to establish and maintain an effective cybersecurity program via the implementation of written policies, as required by the Virtual Currency Regulation.

13. At the time of the Examinations, bitFlyer USA had not performed periodic assessments of its internal and external cybersecurity risks and threats, in violation of 23 NYCRR § 500.09(a). Instead, the Company relied upon an IT audit performed by bitFlyer (Japan). Although an IT audit ensures the existence of policies and procedures to protect an organization's networks and computer systems, it does not provide visibility into the organization's security risks or how the organization can mitigate those risks and, therefore, is not an acceptable substitute for a comprehensive risk assessment. bitFlyer USA's incomplete approach to risk assessment is at odds with the requirements of 23 NYCRR § 500.09 and the many additional sections of the Cybersecurity Regulation that rely on informed decision-making pursuant to the risk assessment.

14. Because bitFlyer USA had not performed a comprehensive risk assessment as required by 23 NYCRR § 500.09(a), bitFlyer USA's cybersecurity program was not designed to protect its electronic systems, and the information stored on those systems, from unauthorized

access, use, or other malicious acts through the use of defensive infrastructure, in violation of 23 NYCRR § 200.16(a).

15. At the time of the Examinations, bitFlyer USA had not implemented a written cybersecurity policy, approved by its board of directors at least annually, setting forth the Company's policies and procedures for the protection of its electronic systems and customer and counterparty data stored on those systems, in violation of 23 NYCRR § 200.16(b).

16. Further, bitFlyer USA's policies and procedures were not customized to the Company's needs and risks. Among other deficiencies, bitFlyer USA's policies and procedures did not accurately reflect the organizational structure of the Company and referenced entities and groups that did not exist within the Company. At the same time, entities and groups that did operate within bitFlyer were not referenced in the policies and procedures. Moreover, many of bitFlyer USA's written policies and procedures were English translations of Japanese originals; some portions were poorly translated, while others (such as graphs) were not translated at all. Certain documents were clearly templates, one referring to bitFlyer USA as "ABC Company," and another referring to bitFlyer USA as "the Covered Entity." Further, the Company did not conduct annual reviews and obtain board approvals of its policies, as required by 23 NYCRR § 200.16(b).

Violations of Law and Regulations

17. bitFlyer USA failed to produce a risk assessment sufficient to inform the design of its cybersecurity program, in violation of 23 NYCRR § 500.09.

18. bitFlyer USA failed to establish and maintain an effective cybersecurity program, implemented via a written cybersecurity policy that is annually approved by its board of directors, in violation of 23 NYCRR § 200.16.

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

19. 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 Financial Services Law § 408 to the Department in the amount of one million, two hundred thousand dollars ($1,200,000.00). The payment shall be in the form of a wire transfer in accordance with instructions provided by the Department.

20. bitFlyer USA 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.

21. bitFlyer USA 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.

22. In assessing a penalty for failure to maintain a compliant cybersecurity program in violation of 23 NYCRR §§ 200.16 and 500.09(a), 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, the entity's size and revenue, and such other matters as justice and the public interest may require.

23. The Department acknowledges bitFlyer USA's cooperation throughout this investigation. The Department also recognizes and credits bitFlyer USA's ongoing efforts to remediate the shortcomings identified in this Consent Order. Among other things, the Company

has demonstrated its commitment to remediation by devoting significant financial and other resources to a remediation plan that has been approved by the Department and must be completed as described below.

Remediation

24. During the course of this investigation, bitFlyer USA performed a comprehensive review of its current compliance programs with respect to the Virtual Currency and Cybersecurity Regulations. Based on this review, bitFlyer USA presented, and the Department approved, a remediation plan designed to bring bitFlyer USA into compliance by December 31, 2023. bitFlyer USA will report its progress to the Department on a quarterly basis.

25. Any deviations from this remediation plan will be determined based on discussions with the Department. The Department may amend the remediation plan as it deems appropriate in its sole regulatory discretion.

Full and Complete Cooperation

26. 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

27. 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.

28. Notwithstanding any other provision in this Consent Order, however, the Department may undertake additional action against the Company for transactions or conduct

that were not disclosed in the written materials submitted to the Department in connection with this matter.

Waiver of Rights

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

30. 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

31. 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

32. 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.

33. 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 the 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

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

For the Department:

David Casler
Senior Assistant Deputy Superintendent
Consumer Protection and Financial Enforcement
One State Street
New York, New York 10002

For bitFlyer USA:

Zachary Figueroa
Chief Compliance Officer
Counsel
548 Market St #25696
San Francisco, CA 94104

David Aaron
Perkins Coie LLP
700 Thirteenth Street, N.W. Suite 800
Washington, DC 20005-3960

Miscellaneous

35. 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.

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

37. 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.

38. 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.

39. 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.

40. 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.

41. 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.

42. 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/ Elizabeth A. Farid
ELIZABETH A. FARID
Senior Assistant Deputy Superintendent
for Consumer Protection and Financial
Enforcement
April 14, 2023

By: /s/ Alison L. Passer
ALISON L. PASSER
Deputy Director of Enforcement Consumer
Protection and Financial Enforcement
April 14, 2023

By: /s/ Christopher B. Mulvihill
CHRISTOPHER B. MULVIHILL
Deputy Superintendent for Consumer
Protection and Financial Enforcement
April 14, 2023

By: /s/ Kevin R. Puvalowski
KEVIN R. PUVALOWSKI
Acting Executive Deputy Superintendent for
Consumer Protection and Financial
Enforcement
April 24, 2023

BITFLYER USA

By: /s/ Takahiro Kinoshita
TAKAHIRO KINOSHITA
Chief Executive Officer

April 13, 2023

THE FOREGOING IS HEREBY APPROVED. IT IS SO ORDERED.

/s/ Adrienne A. Harris
ADRIENNE A. HARRIS
Superintendent of Financial Services
May 1, 2023