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

---x

In the Matter of :

BITPAY, INC. :

---x

CONSENT ORDER

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

WHEREAS**,** BitPay is a payment service provider that allows merchants to accept Bitcoin payments from customers in exchange for the equivalent value in local currency credited to the merchant's bank account;

WHEREAS, BitPay 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 and is a "Licensee" pursuant to 23 NYCRR § 200.2(f);

WHEREAS, among other obligations, the Virtual Currency Regulation requires that Licensees adhere to federal and New York laws and regulations that require businesses to maintain effective controls to guard against money laundering and certain other illicit activities;

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, BitPay is a "Covered Entity," pursuant to 23 NYCRR § 500.01(c);

WHEREAS, in 2018, the Department conducted its first full-scope examination of BitPay covering the period of July 10, 2018, through December 31, 2018 (the "First Examination") and found deficiencies in BitPay's overall compliance function, including with respect to its anti-money laundering ("AML") and cybersecurity compliance programs;

WHEREAS, in 2022, the Department conducted its second full-scope examination of BitPay covering the period of January 1, 2019, through December 31, 2021 (the "Second Examination") and determined that, although improvements were made to address the deficiencies identified during the First Examination, BitPay's AML program and its cybersecurity program required additional improvement to achieve compliance with the applicable regulatory requirements;

WHEREAS, following the Second Examination, the Department initiated an enforcement investigation into BitPay's AML and cybersecurity programs (the "Enforcement Investigation");

WHEREAS, following the Enforcement Investigation, the Department concluded that BitPay violated the following sections of the Virtual Currency Regulation: (1) 23 NYCRR § 200.15(c), which requires Licensees to develop a system of internal controls, policies, and procedures to ensure compliance with applicable AML laws, rules, and regulations, as well as to develop independent testing to ensure such compliance; and (2) 23 NYCRR § 200.15(i), which requires Licensees to develop risk-based policies, procedures, and practices designed to ensure compliance with the applicable U.S Treasury Department's Office of Foreign Assets Control ("OFAC") regulations; and

WHEREAS, the Department further concluded that BitPay violated the following sections of the Cybersecurity Regulation: (1) 23 NYCRR § 500.04, which requires Covered Entities to formally designate "a qualified individual responsible for overseeing and implementing the covered entity's cybersecurity program and enforcing its cybersecurity policy" (a "Chief Information Security Officer" or "CISO") who must report to the Covered Entity's board of directors, annually and in writing, on the Covered Entity's cybersecurity program; and (2) 23 NYCRR § 500.09(a), which requires Covered Entities to conduct a periodic Risk Assessment of the Covered Entity's Information Systems, sufficient to inform the design of the cybersecurity 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 the Superintendent of Financial Services (the "Superintendent") is responsible for ensuring the safety, soundness, and prudent control of the various financial services businesses that the Department oversees through the enforcement of the various laws and regulations applicable to financial services licensees, including the New York Financial Services Law and the regulations promulgated thereunder.

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

3. The Virtual Currency Regulation requires that Licensees establish an effective AML program, that, at a minimum, shall provide for a system of internal controls, policies, and procedures designed to ensure ongoing compliance with all applicable AML laws, rules, and regulations. The effectiveness of the AML program must be independently tested by qualified internal personnel of the regulated entity or a qualified external party. 23 NYCRR §§ 200.15(c)(1), 200.15(c)(2).

4. The Virtual Currency Regulation also requires Licensees to comply with applicable regulations issued by OFAC. 23 NYCRR § 200.15(i).

5. To support the Superintendent's critical obligation to protect private and sensitive data, the Department requires, through the Cybersecurity Regulation, that all Covered Entities, including BitPay, conduct a periodic risk assessment of its Information Systems sufficient to inform the design of the cybersecurity program and update such risk assessment(s) as necessary

to address changes to the Covered Entities' Information Systems, Nonpublic Information ("NPI"), or business operations. 23 NYCRR §§ 500.01(e), 500.01(g), 500.09(a), 200.16.

6. To facilitate ongoing compliance with the Cybersecurity Regulation and maintain the security of a Covered Entity's Information Systems and NPI, Covered Entities must designate a qualified CISO. The CISO is responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy. In so doing, the CISO must report in writing, at least annually, to the Covered Entity's board of directors about the cybersecurity program, as well as any material cybersecurity risks facing the Covered Entity. 23 NYCRR § 500.04.

Events at Issue

Background

7. BitPay is a provider of Bitcoin payment technology, serving more than 100,000 merchants worldwide. The BitPay platform allows merchants to accept Bitcoin payments from customers at the point of sale in exchange for the equivalent value in local currency credited to the merchant's bank account the next day.

8. The Enforcement Investigation concluded that BitPay failed to maintain an effective AML program and to comply with the Department's Cybersecurity Regulation.

Deficiencies in BitPay's AML Program

9. The Enforcement Investigation determined that BitPay's AML program deficiencies identified during the Second Exam included, customer/merchant risk rating processes being applied on an *ad hoc* basis, a lack of sufficient policies and procedures governing BSA/AML Risk Assessment, quality assurance, and rule management, and an onboarding process that is semi-automated and siloed in multiple stand-alone systems that are not integrated. These failures, individually as well as collectively, raise significant concerns

about the quality of risk-based BSA/AML oversight of BitPay's customers and program as a whole.

10. These identified deficiencies related to BitPay's AML oversight demonstrates BitPay's failure to establish proper internal controls, policies, and procedures, as required by 23 NYCRR § 200.15(c)(1).

11. Furthermore, BitPay did not have sufficient independent testing of its transaction monitoring system to provide assurance that the system operated as intended, as is required for all Licensees pursuant to 23 NYCRR § 200.15(c)(2).

12. The Enforcement Investigation further determined that BitPay's first-level screening process failed to identify certain names from the current sanction listing when tested. BitPay also failed to establish an OFAC quality assurance process, especially with respect to alert dispositions, in violation of 23 NYCRR § 200.15(i).

Deficiencies in BitPay's Cybersecurity Program

13. The Cybersecurity Regulation requires Covered Entities to conduct periodic risk assessments, which should be updated as necessary to address changes to the Covered Entities' Information Systems, NPI, or business operation. 23 NYCRR § 500.09(a). This section of the Cybersecurity Regulation became effective on March 1, 2018.

14. Risk Assessments constitute a core component of a robust cybersecurity program. For example, Section 500.02(b) of the Cybersecurity Regulation requires the cybersecurity program to be based on the Covered Entity's Risk Assessment, and Section 500.03 of the Cybersecurity Regulation requires the implementation of a written cybersecurity policy to be based on the Covered Entity's Risk Assessment.

15. The Enforcement Investigation concluded that despite this clear and unequivocal requirement, BitPay conducted only one Risk Assessment, in March 2021 (the "2021 Risk

Assessment"), years after BitPay was initially licensed by the Department on July 10, 2018. BitPay's failure to conduct a periodic risk assessment meant that BitPay operated its cybersecurity program without being sufficiently informed as to the risks facing its Information Systems. Such failure to conduct periodic risk assessments constitutes a violation of 23 NYCRR § 500.09(a).

16. Additionally, the Cybersecurity Regulation requires Covered Entities to designate a CISO who is "responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy." 23 NYCRR § 500.04(a). The CISO is also responsible for submitting an annual report to the Covered Entity's board of directors. 23 NYCRR § 500.04(b).

17. The CISO requirement became effective prior to BitPay's licensure; however, BitPay failed to formally designate a CISO until May 2022, in violation of Part 500.04(a).

18. Moreover, the examinations and Enforcement Investigation found that no one, let alone a properly designated CISO, was annually reporting in writing to BitPay's board of directors regarding the cybersecurity program and material cybersecurity risks facing BitPay, in violation of Part 500.04(b).

19. The lack of annual reporting is especially troubling given the relatively new and constantly fluctuating industry in which BitPay operates, as well as the large amount of consumer NPI stored on its Information Systems.

Violations of Law and Regulations

20. BitPay failed to establish a system of internal controls designed to ensure ongoing compliance with the relevant AML laws and failed to provide for independent testing of its AML program, in violation of 23 NYCRR §§ 200.15(c)(1) & 200.15(c)(2).

21. BitPay failed to establish an OFAC quality assurance process, especially with respect to alert dispositions, in violation of 23 NYCRR § 200.15(i).

22. BitPay failed to conduct periodic cybersecurity risk assessments, in violation of 23 NYCRR § 500.09(a).

23. BitPay failed to timely designate a formal CISO, and failed to ensure that the CISO submitted a written report to BitPay's board of directors, in violation of 23 NYCRR §§ 500.04(a) & 500.04(b).

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

24. 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 Dollars and 00/100 Cents ($1,000,000.00). The payment shall be in the form of a wire transfer in accordance with instructions provided by the Department.

25. 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.

26. 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.

27. The Department acknowledges BitPay's cooperation throughout this investigation. The Department also recognizes and credits BitPay's ongoing efforts to remediate

the shortcomings identified in this Consent Order. Among other things, BitPay has demonstrated its commitment to remediation by devoting significant financial and other resources to enhance its cybersecurity and AML programs, including through changes to its policies, procedures, systems, and governance structures.

Remediation

28. BitPay shall continue to strengthen its controls, policies, and procedures to ensure robust compliance programs in connection with its cybersecurity and virtual currency business activity programs, as required by 23 NYCRR § 200 and 23 NYCRR § 500.

Action Plan

29. Within one hundred and eighty (180) days of the Effective Date of this Consent Order, BitPay shall submit an action plan that is acceptable to the Department with updates on the violations and deficiencies identified in this Consent Order and during the Second Examination (the "Action Plan"). At a minimum, the Action Plan must include a detailed description of any remediation that is planned and/or underway of the violations identified in this Consent Order and during the Second Examination and projected completion dates.

30. One year from the Department's approval of the Action Plan, BitPay shall submit to the Department a written status update as to the implementation of the Action Plan. BitPay shall continue to submit a written status update annually until all items contained in the Action Plan are complete.

Cybersecurity Risk Assessment

31. Within one hundred and fifty (150) days of the Effective Date of this Consent Order, BitPay shall conduct a comprehensive Cybersecurity Risk Assessment of its Information Systems consistent with 23 NYCRR § 500.09 and submit the results of the same to the

Department within ten (10) days of completion. The Cybersecurity Risk Assessment results shall contain:

a. the reasonably necessary changes BitPay plans to implement to address any issues raised in the Cybersecurity Risk Assessment;

b. a plan for revisions of controls to respond to technological developments and evolving threats, which shall consider the particular risks of BitPay's business operations related to cybersecurity, NPI collected or stored, Information Systems utilized, and the availability and effectiveness of controls to protect NPI and Information Systems; and

c. a plan for updating or creating written policies and procedures to include:

   i. criteria for the evaluation and categorization of identified cybersecurity risks or threats facing BitPay;

   ii. criteria for assessment of the confidentiality, integrity, security, and availability of BitPay's Information Systems and NPI, including the adequacy of existing controls in the context of identified risks;

   iii. criteria for the periodic assessments of any third-party services providers used by BitPay; and

   iv. requirements describing how identified risks will be mitigated or accepted based on the Cybersecurity Risk Assessment and how the cybersecurity program will address the risk.

32. Along with the results of the Cybersecurity Risk Assessment, BitPay will, within sixty (60) days of the completion of the Cybersecurity Risk Assessment submit a report to the Department for the Department's approval detailing BitPay's plan for addressing each of the

risks identified in the Cybersecurity Risk Assessment (the "Cybersecurity Risk Assessment Report").

33. One hundred and eighty (180) days after receipt of the Department's approval of the Cybersecurity Risk Assessment Report, BitPay will provide the Department with a written report detailing all actions taken by BitPay to implement the measures contained in the Cybersecurity Risk Assessment Report. Such reports will continue to be submitted to the Department every one hundred and eighty (180) days until all action items identified in the Cybersecurity Risk Assessment Report have been satisfied.

CISO

34. Within ninety (90) days of the Effective Date of this Consent Order, BitPay shall develop and implement written guidelines addressing the CISO's responsibility to submit annual written reports to the board of directors pursuant to 23 NYCRR § 500.04(b).

Full and Complete Cooperation

35. 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

36. 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.

37. 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

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

39. 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

40. 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

41. 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.

42. 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 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

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

For the Department:

Ariana F. Reinhertz
Attorney, Excelsior Fellow
Consumer Protection and Financial Enforcement
New York State Department of Financial Services
One State Street
New York, NY 10004

For BitPay, Inc.:

Allison E. Raley
Chief Compliance Officer and General Counsel (Chief Risk Officer)
BitPay, Inc.
8000 Avalon Blvd, Suite 300
Alpharetta, GA 30009

Jagruti Solanki
Chief Financial Officer
BitPay, Inc.
8000 Avalon Blvd, Suite 300
Alpharetta, GA 30009

Laurel Loomis Rimon
Aaron Charfoos
Paul Hastings LLP
2050 M Street NW
Washington, DC
20036

Miscellaneous

44. 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.

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

46. 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.

47. 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.

48. 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.

49. 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.

50. 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.

51. 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	**BITPAY, INC.**
By: /s/ Madeline W. Murphy MADELINE W. MURPHY Assistant Deputy Superintendent Consumer Protection and Financial Enforcement	By: /s/ Stephen Pair STEPHEN PAIR CHIEF EXECUTIVE OFFICER
March 10, 2023	March 9, 2023

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

March 10, 2023

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

March 10, 2023

THE FOREGOING IS HEREBY APPROVED. IT IS SO ORDERED.

/s/ Adrienne A. Harris
ADRIENNE A. HARRIS
Superintendent of Financial Services

March 16, 2023