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

----------x

In the Matter of :

PAYPAL, INC. :

----------x

CONSENT ORDER

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

WHEREAS, the Department has issued PayPal multiple licenses, including a money transmitter license and a BitLicense;

WHEREAS, August 29, 2017 marked the initial effective date of New York's first-in-the-nation cybersecurity regulation, 23 NYCRR Part 500 (the "Cybersecurity Regulation")[1];

WHEREAS, the Cybersecurity Regulation defines clear standards for cooperative industry compliance, robust consumer data protection, vital cybersecurity controls, and timely

[1] All citations to 23 NYCRR Part 500 herein refer to the Cybersecurity Regulation as it read prior to November 1, 2023.

reporting of Cybersecurity Events, as defined by 23 NYCRR § 500.1(d), and was promulgated to strengthen cybersecurity and data protection for the industry and consumers;

WHEREAS, the Department has been investigating a Cybersecurity Event experienced at PayPal, as well as the Company's general compliance with the Cybersecurity Regulation; and

WHEREAS, based on the investigation, the Department concluded that PayPal violated the following sections of the Cybersecurity Regulation: (1) 23 NYCRR § 500.3(d), (i), and (k), which require that all DFS-regulated entities ("Covered Entities") implement and maintain written policies and procedures that address, *inter alia*, access controls and identity management, systems and application development and quality assurance, and customer data privacy; (2) 23 NYCRR § 500.10(a), which requires that Covered Entities utilize qualified cybersecurity personnel and provide those personnel with updates and training sufficient to address relevant cybersecurity risks; and (3) 23 NYCRR § 500.12(a), which requires that Covered Entities use effective controls to protect against unauthorized access to Nonpublic Information ("NPI") or Information Systems.

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 under the Department's supervision.

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

3. Among the Superintendent's many obligations to the public is a consumer protection function, which includes the protection of individuals' private and personally sensitive data from negligent or willful exposure by licensees of the Department.

4. To support this critical obligation, the Cybersecurity Regulation places on all Covered Entities, including PayPal, a duty to establish and implement a cybersecurity program, including the implementation of certain cybersecurity policies and procedures based on a risk assessment and designed to protect the confidentiality and integrity of their Information Systems, as well as any consumer NPI contained therein. 23 NYCRR §§ 500.1(c), 500.1(e), 500.1(g), 500.1(k), 500.2(b), 500.3.

5. Critical to developing and maintaining a robust cybersecurity program is the requirement that Covered Entities utilize qualified cybersecurity personnel to perform and oversee the performance of the cybersecurity program, and that such personnel are provided with updates and training sufficient to address relevant cybersecurity risks. 23 NYCRR § 500.10(a).

6. To secure and protect customer NPI and prevent Cybersecurity Events, Covered Entities must "use effective controls, which may include Multi-Factor Authentication [("MFA")] or Risk-Based Authentication, to protect against unauthorized access to [NPI] or Information Systems." 23 NYCRR § 500.12(a).

Events at Issue

The December 2022 Cybersecurity Event

7. On December 6, 2022, a PayPal security analyst identified a message posted online that stated, "PP EXPLOIT TO GET SSN," and explained that a user could follow a link to PayPal's website to view PayPal customers' Social Security Numbers ("SSNs").

8. Later that day, PayPal discovered that the Form 1099-Ks available on PayPal's online platform contained unmasked consumer information, including names, dates of birth, and full SSNs.

9. The Internal Revenue Service ("IRS") requires third-party payment organizations such as PayPal to issue Form 1099-Ks to certain taxpayers who receive payments through such organizations. In 2021, as a part of the American Rescue Plan Act, the IRS lowered the threshold for when third-party payment organizations must issue Form 1099-Ks. Previously, a taxpayer had to receive more than $20,000 in yearly income and conduct more than 200 transactions. Under the new law, this threshold was dropped to $600 in yearly income with no minimum number of transactions.[2]

10. To comply with the American Rescue Plan Act, in 2022, PayPal's Program Development Team and Business Risk Compliance Leadership were tasked with making Form 1099-Ks accessible to customers who were newly eligible to receive them under the new $600 reporting threshold. PayPal did so by implementing changes to existing data collection flows (the "Form 1099-K change").

11. The updated Form 1099-Ks went "live" on October 18, 2022. As PayPal later learned, the forms contained unmasked customer NPI.

[2] The IRS later delayed the implementation of this new threshold to the 2025 tax year and, for the 2024 tax year, set the threshold at $5,000.

12. On December 7, 2022—one day after the PayPal security analyst saw the online message—PayPal's cybersecurity team noticed a spike in attempts to access PayPal's online platform and concluded that threat actors were using credential stuffing to gain access to the NPI available in the unmasked Form 1099-Ks.[3]

13. In response to this Cybersecurity Event (hereinafter the "December 2022 Cybersecurity Event"), PayPal added CAPTCHA and rate limiting, which successfully stopped the automated account access. PayPal also conducted additional remediation efforts, including masking the exposed NPI and forcing password resets for accounts impacted by the incident.

Causes of the December 2022 Cybersecurity Event

14. Pursuant to PayPal's application development policies and procedures at the time, when there is a new product or a new capability or feature for an existing product, as was the case here, a Risk and Control Identification Process ("RCIP") must be conducted. This process includes reviewing, analyzing, and testing the product or change.

15. The teams responsible for implementing the change to the existing data collection flows in connection with the new Form 1099-K threshold, however, misclassified the change as a "platform migration" rather than a "new capability or feature for an existing product" and, therefore, no RCIP was conducted for the Form 1099-K change.

16. This misclassification arose from a failure to adequately train the engineering team assigned to deploy the code for the Form 1099-K change. As a result, the engineering team failed to effectively implement PayPal's policies and procedures on access controls and identity management, systems and application development and quality assurance, and customer data

[3] "Credential stuffing" occurs when usernames and passwords are taken from one source and tested for validity via login portals belonging to other sources through automated processes.

privacy with respect to the Form 1099-K change. 23 NYCRR §§ 500.3(d), 500.3(i), 500.3(k), 500.10(a).

17. The engineering team responsible for implementing the Form 1099-K change was not adequately trained on PayPal's policies and procedures for deploying code and, therefore, incorrectly determined that following RCIP was not required. Thus, contrary to RCIP and PayPal's Change Management Policy, a risk assessment, penetration test, and/or vulnerability scan of this change did not occur, and no formal approval to launch was given with respect to the Form 1099-K change. As a result, the Form 1099-K change went live with NPI unmasked.

18. Additionally, because of the engineering team's failure to implement the policies and procedures PayPal had in place to protect NPI with respect to the Form 1099-K change, PayPal failed to use effective controls to protect NPI from exposure to threat actors who leveraged their access to PayPal's platform to obtain the NPI of tens of thousands of consumers.

19. PayPal's Authentication and Session Management policy requires that "[a]ll activity that permits access to account information must be protected by risk-based authentication." Notwithstanding this requirement, the use of MFA for customer accounts, such as the ones that were accessed during the December 2022 Cybersecurity Event, was optional, which resulted in the unauthorized access of NPI. 23 NYCRR § 500.12(a).

Violations of Law and Regulations

20. PayPal failed to ensure the proper implementation of its cybersecurity policies and procedures, in violation of 23 NYCRR § 500.3(d), (i), and (k).

21. PayPal failed to utilize qualified cybersecurity personnel to perform and oversee the performance of core cybersecurity functions, for example, the Form 1099-K change, and failed to provide cybersecurity personnel with training in PayPal's policies and procedures

sufficient to address relevant cybersecurity risks, in violation of 23 NYCRR § 500.10(a)(1) & (2).

22. PayPal failed to use effective controls to protect against unauthorized access to NPI, in violation of 23 NYCRR § 500.12(a).

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

23. 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 to the Department in the amount of Two Million Dollars and 00/100 Cents ($2,000,000). The payment shall be in the form of a wire transfer in accordance with instructions provided by the Department.

24. 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.

25. 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.

26. In assessing a penalty for failures in PayPal's cybersecurity program and compliance with the Cybersecurity Regulation, 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.

27. The Department acknowledges PayPal's commendable cooperation throughout this investigation. The Department also recognizes and credits PayPal's efforts to remediate the issues identified in this Consent Order, beginning immediately after it discovered the vulnerability. That remediation included, in addition to masking the exposed NPI and implementing CAPTCHA, updating the relevant policies to ensure additional clarity as to when RCIP applies, providing training on PayPal's policies and procedures for deploying code to the engineering team that failed to execute RCIP, and improving capabilities to monitor code as it is pushed to production to ensure that an RCIP approval is associated with the new or changed code when one is required by PayPal's policies and procedures. In addition, PayPal now requires MFA for all United States customer account logins.

Full and Complete Cooperation

29. 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

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

31. 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

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

33. 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

34. 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

35. 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.

36. 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, the Banking Law, and any other applicable laws, and may use any evidence available to the Department in any ensuing hearings, notices, or orders.

Notices

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

For the Department:

Christina Glekas
Assistant Deputy Superintendent
Consumer Protection and Financial Enforcement
One State Street
New York, New York 10004

Esther Kang
Assistant Attorney
Cybersecurity Division
One State Street
New York, New York 10004

For PayPal:

Andrea Donkor
SVP, Global Chief Compliance Officer
117 Barrow Street
New York, New York 10014

Bimal Patel
SVP, General Counsel
117 Barrow Street
New York, New York 10014

Miscellaneous

38. 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.

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

40. 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.

41. 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.

42. 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.

43. 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.

44. 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.

45. 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/ Madeline W. Murphy
MADELINE W. MURPHY
Deputy Director of Enforcement
Consumer Protection and Financial Enforcement

January 23, 2025

By: /s/ Alison L. Passer
ALISON L. PASSER
Deputy Superintendent
Consumer Protection and Financial Enforcement

January 23, 2025

By: Samantha R. Darche
SAMANTHA R. DARCHE
Acting Executive Deputy Superintendent
Consumer Protection and Financial Enforcement

January 23, 2025

PAYPAL, INC.

By: /s/ Andrea Donkor
ANDREA DONKOR
SVP, Global Chief Compliance Officer

January 14, 2025

THE FOREGOING IS HEREBY APPROVED. IT IS SO ORDERED.

/s/ Adrienne A. Harris
ADRIENNE A. HARRIS
Superintendent of Financial Services
January 23, 2025