MARY ANN SMITH
Deputy Commissioner
BORYANA ARSOVA
Assistant Chief Counsel
PAUL YEE (State Bar No. 142381)
Senior Counsel
LOUIS LAVERONE (State Bar No. 296990)
Senior Counsel
Department of Financial Protection and Innovation
One Sansome Street, Suite 600
San Francisco, California 94104-4448
Telephone: (415) 972-8569
Facsimile: (415) 972-8500

Attorneys for Complainant

BEFORE THE DEPARTMENT OF FINANCIAL PROTECTION AND INNOVATION

OF THE STATE OF CALIFORNIA

In the Matter of: THE COMMISSIONER OF FINANCIAL PROTECTION AND INNOVATION, Complainant, v. PATELCO CREDIT UNION, Respondent.	CONSENT ORDER

This Consent Order (Consent Order) is entered into between the Commissioner of Financial Protection and Innovation (Commissioner) and Patelco Credit Union (Patelco or Respondent) (collectively, the Parties).

///

///

///

///

I.

RECITALS

Legal Background

A. The Commissioner has jurisdiction over the licensing and regulation of credit unions in California under the California Credit Union Law (Fin. Code, § 14000 et seq.).

B. Patelco is a credit union licensed in California since September 20, 1939, license no. 955 0152, with headquarters located at 3 Park Place, Dublin, California 94568.

C. The Commissioner conducted an investigation and examination pursuant to section 14250 into Patelco's cybersecurity systems and processes (the investigation) following a ransomware attack on Patelco that caused various Patelco banking systems to be shut down from June 29, 2024 to July 15, 2024 (the event).

D. As a result of the event, among other things:

i. Patelco customers were unable to access account information of savings or checking accounts to verify balances;

ii. Patelco supported customers during the event by advising them that they were able to access $500 per day in-branch and at an ATM and that customers were able to use their credit and debit cards, checks, and ACH transfers and wires;

iii. Patelco customers were unable to conduct any online banking;

iv. Information taken from Patelco's computer systems during the event Included certain personal identifying information (PII) of Patelco's customers.

E. At the time of the event, Patelco's membership was approximately 500,000 members.

Commissioner's Findings and Conclusions

F. Following the investigation, the Commissioner required corrective action. The Commissioner identified areas of concern, associated corrective actions, and a time by which to complete each of the actions. The corrective actions and associated completion times that were communicated to Patelco on November 14, 2024 which relate to:

i. risk management practices

ii. information technology risk assessment processes

iii. board reporting

iv. the security control environment

v. business continuity management program

vi. internal audit program

G. Patelco has cooperated with the Commissioner's investigation and represents that it is committed to working with regulatory agencies for the benefit of its consumers, and that this Consent Order reflects Patelco's willingness to work with regulatory agencies to ensure that its cybersecurity systems and processes comply with the law for an institution of its size, complexity, and risk profile.

H. Patelco agrees to comply with the terms and conditions of this Consent Order as outlined below.

I. Without admitting or denying the Commissioner's Findings or Conclusions, Patelco desires to enter into this Consent Order, which the Commissioner finds is appropriate, in the public interest, and consistent with the purposes of the Financial Code.

NOW THEREFORE, in consideration of the foregoing, and the terms and conditions set forth herein, the Parties agree as follows:

II.

TERMS AND CONDITIONS

1. Purpose. This Consent Order resolves the issues before the Commissioner in a manner that avoids the business disruption and expense of a hearing and other possible court proceedings, protects consumers, is in the public interest, and is consistent with the purposes, policies, and provisions of the applicable law.

2. Finality of Consent Order. Patelco agrees to comply with this Consent Order and stipulates this Consent Order is hereby deemed final.

3. Cease and Desist Order. Pursuant to Financial Code § 580, the Commissioner orders Patelco to cease and desist from unsafe and unsound acts with respect to its inadequate cybersecurity system and processes and further orders Patelco as follows:

i. Within the timelines as set forth in the in the Commissioner's requirements following the investigation, Respondent shall implement an adequate program to ensure the security and confidentiality of customer records and information, protect against any anticipated threats or hazards to the security and integrity of such records, and protect against unauthorized access to or use of such records or information, which could result in substantial harm or inconvenience to any customer (hereafter, the Cybersecurity Program). Respondent shall maintain a program that is commensurate with Respondent's risk profile and reasonably designed to comply with the cybersecurity provisions of the federal Gramm-Leach Bliley Act, Chapter 94 of Subchapter I of Title 15, United States Code, beginning at section 6801; implementing regulations at Title 12, Code of Federal Regulations, Parts 748-749 and Appendix A to Part 748; and Division 1.4 of the California Financial Code, beginning at section 4050.

ii. Respondent shall designate and maintain a qualified individual responsible for overseeing and implementing the Cybersecurity Program, including incident response and business continuity functions. Respondent's Board of Directors shall oversee the development, implementation, and maintenance of the Cybersecurity Program, including assigning specific responsibility for its implementation and reviewing reports from management. A qualified individual shall have sufficient authority to oversee and implement the Cybersecurity Program, and adequate resources, funding, and personnel should be allocated to the Cybersecurity Program.

iii. Respondent shall have and maintain a written risk assessment that identifies reasonably foreseeable internal and external threats that could result in the

unauthorized disclosure, misuse, alteration, or destruction of such customer information, assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of member information; and assesses the sufficiency of any controls, policies, procedures, information systems, and other arrangements in place to address risks (the Risk Assessment). Respondent shall report to Respondent's Board of Directors or an appropriate committee of the Board of Directors at least annually regarding the overall status of the Cybersecurity Program. The report should discuss material matters related to the Cybersecurity Program, addressing issues such as the Risk Assessment, risk management and control decisions, service provider arrangements, results of testing, security incidents and management's responses, and recommendations for changes in the Cybersecurity Program. The Risk Assessment shall be prepared and updated periodically and updated as needed in response to changes or anticipated changes in Respondent's risk profile.

iv. Respondent shall have and maintain written policies and procedures that allow personnel to effectively implement the Cybersecurity Program. Such policies and procedures shall be designed to control identified risks, commensurate with the sensitivity of the information and complexity and scope of Respondent's activities. Respondent's Board of Directors or an appropriate committee of the Board of Directors shall approve the written information security policy and program on an annual basis. Respondent's Executive staff shall review and approve these written procedures on an annual basis.

v. Respondent shall have and maintain independent testing requirements that are appropriate for Patelco's size, complexity, and overall risk profile. Respondent may perform independent testing through an internal audit

function or an external assessor. Internal audit functions shall be performed by employees independent from those who develop and maintain the Cybersecurity Program and who will report to the Audit Committee. The Audit Committee will thereafter report to Patelco's Board of Directors about the internal audit findings. Audit activities shall generally conform with the International Standards for the Professional Practice of Internal Auditing. Respondent's internal audit function shall audit the Cybersecurity Program, including incident response and business continuity functions. Independent testing shall follow a schedule that is prepared on a multi-year basis to ensure that applicable risk areas are tested with appropriate frequency. Critical and high-risk areas of the Cybersecurity Program shall be tested at least annually.

vi. Respondent's management shall report to the Audit Committee of the Board of Directors on the progress of appropriate corrective actions with respect to issues, findings, recommendations, and risks identified through the Risk Assessment set forth in paragraph 3.iii. above and independent testing set forth in paragraph 3.v. above as well as their timely and appropriate completion.

vii. Respondents shall have and maintain a training program that ensures all Patelco personnel at all levels understand Patelco's risk profile and compliance obligations and can implement the Cybersecurity Program effectively.

viii. Respondents shall exercise appropriate due diligence when selecting any service providers. Respondent shall require its service providers by contract to implement appropriate cybersecurity, incident response, and business continuity measures to meet the requirements of this Order.

ix. Respondent shall correct all apparent violations of laws or non-conformance with applicable rules and regulations within the timelines as set forth by the Commissioner following the investigation. In addition, the Respondent shall take all necessary steps to ensure future compliance with all such applicable laws and regulations.

4. Compliance Consultant. Within 90 days of the effective date of this Order, Patelco must engage a qualified, independent, and unaffiliated third-party compliance consultant ("Compliance Consultant") to support Respondent's efforts to augment its cybersecurity program and processes to complete the required corrective actions identified by the Commissioner following the investigation. The scope of the Compliance Consultant's engagement must include a quarterly written review of the progress taken to address all corrective action identified by the Commissioner following the investigation and as required by this Order. The scope of the Compliance Consultant's engagement must include, but is not limited to, quarterly reviews of Patelco's cybersecurity systems, and processes to ascertain compliance with applicable laws and regulations, as well as any corrective measures needed to ensure Respondent complies with this Order. The scope of the Compliance Consultant's engagement must also include, but is not limited to, quarterly independent testing of transaction data to verify the effectiveness of Patelco's internal controls and cyber security systems and processes. Respondent agrees to fully cooperate with the Compliance Consultant and support its work by, at minimum, providing the Compliance Consultant with access to relevant personnel, third-party service providers, facilities, files, reports, and records. A copy of the engagement letter for the Compliance Consultant must be submitted to the Commissioner within seven days of its execution. The Compliance Consultant must submit a copy of any reports issued to Patelco in connection with this engagement directly to the Commissioner contemporaneously. The obligation to have the Compliance Consultant engaged shall cease upon the Compliance Consultant's report that Respondent has fulfilled the requirements as identified by the Commissioner following the investigation.

5. Corrective Action Plan. To the extent that the Compliance Consultant identifies a

material deficiency in Respondent's Cybersecurity Program during the time of Compliance Consultant's engagement, Respondent must develop a plan to implement such measures (Corrective Action Plan). Respondent will provide the Corrective Action Plan to the Commissioner within sixty (60) days of the Compliance Consultant's written review. The Corrective Action Plan must appropriately incorporate the relative priority of each corrective measure as determined by the Compliance Consultant. The scope of the Compliance Consultant's engagement must include, but is not limited to, conducting a validation assessment of all corrective measures as identified by the Commissioner following the investigation and Corrective Action Plan and documenting findings in a validation report upon Respondent's determination that it has completed all corrective actions.

6. Penalty. Patelco agrees to pay a monetary penalty of $100,000.00 (penalty) pursuant to Financial Code § 4057 no later than thirty calendar days after the Effective Date of this Consent Order. The penalty must be made payable to "Department of Financial Protection and Innovation" in the form of a cashier's check, wire transfer or Automated Clearing House deposit to the Department of Financial Protection and Innovation, transmitted to the attention of Accounting – Litigation, at the Department of Financial Protection and Innovation, 2101 Arena Boulevard, Sacramento, California 95834. Notice of the payment must be concurrently sent to Paul Yee, Senior Counsel, Department of Financial Protection and Innovation, One Sansome Street, San Francisco, California 94104-4448, Paul.Yee@dfpi.ca.gov.

7. Waiver of Hearing Rights. Patelco acknowledges the Commissioner is ready, willing, and able to proceed with the filing of an administrative action on the charges contained in this Consent Order. Patelco hereby waives the right to any hearings, and to any reconsideration, appeal, or other right to review which may be afforded pursuant to the Financial Code, the California Administrative Procedure Act, the California Code of Civil Procedure, or any other provision of law. Patelco further expressly waives any requirement for the filing of an Accusation pursuant to California Government Code section 11415.60, subdivision (b). By waiving such rights, Patelco consents to this Consent Order becoming final.

8. Information Willfully Withheld. The Consent Order may be revoked if the Commissioner later finds out that Patelco knowingly or willfully withheld information used and

relied upon in the Consent Order.

9. Assisting Other Agencies. The Parties further acknowledge and agree that nothing in the Consent Order shall limit the Commissioner's ability to assist any other agency (city, county, state, or federal) with any prosecution, administrative, civil, or criminal, brought by any such agency against Patelco or any other person based upon any of the activities alleged in this matter or otherwise.

10. Third Party Actions. This Consent Order does not create any private rights or remedies against Respondents, serve as an admission by Respondent with regard to any third-party, create any liability for Respondents, or limit defenses of Respondents for any person or entity not a party to this Consent Order.

11. Headings. The headings to the paragraphs of the Consent Order are inserted for convenience only and will not be deemed a part hereof or affect the construction or interpretation of the provisions hereof.

12. Binding. The Consent Order is binding on all heirs, assigns, or successors in interest.

13. Reliance. Each of the Parties represents, warrants, and agrees that in executing the Consent Order, he/she/it has relied solely on the statements set forth herein and the advice of their own counsel. Each of the Parties further represents, warrants, and agrees that in executing the Consent Order it has placed no reliance on any statement, representation, or promise of any other party, or any other person or entity not expressly set forth herein, or upon the failure of any party or any other person or entity to make any statement, representation, or disclosure of anything whatsoever. The Parties have included this clause: (1) to preclude any claim that any party was in any way fraudulently induced to execute the Consent Order; and (2) to preclude the introduction of parol evidence to vary, interpret, supplement, or contradict the terms of the Consent Order.

14. Waiver, Amendments, and Modifications. No waiver, amendment, or modification of the Consent Order will be valid or binding unless it is in writing and signed by each of the Parties. The waiver of any provision of the Consent Order will not be deemed a waiver of any other provision. No waiver by each of the Parties of any breach of, or of compliance with, any condition or provision of the Consent Order by another party will be considered a waiver of any other condition

or provision or of the same condition or provision at another time.

15. Full Integration. This Consent Order is the final written expression and the complete and exclusive statement of all the agreements, conditions, promises, representations, and covenants among the Parties with respect to the subject matter hereof, and supersedes all prior or contemporaneous agreements, negotiations, representations, understandings, and discussions between and among the Parties, their respective representatives, and any other person or entity, with respect to the subject matter covered hereby.

16. Governing Law. This Consent Order will be governed by and construed in accordance with California law. Each of the parties hereto consent to the jurisdiction of such court, and hereby irrevocably waives, to the fullest extent permitted by law, the defense of an inconvenient forum to the maintenance of such action or proceeding in such court.

17. Counterparts. This Consent Order may be executed in one or more separate counterparts, each of which when so executed, shall be deemed an original. Such counterparts shall together constitute a single document.

18. Effect Upon Future Proceedings. If Patelco applies for any license, permit or qualification under the Commissioner's current or future jurisdiction or is the subject of any future action by such agency to enforce this Consent Order, then the subject matter hereof shall be admissible for the purpose of such application(s) or enforcement proceedings(s).

19. Voluntary Agreement. Patelco enters into this Consent Order voluntarily and without coercion and acknowledges that no promises, threats, or assurances have been made by the Commissioner, or any officer or agent thereof, about the Consent Order other than as reflected herein.

20. Notice. Any notices required under the Consent Order shall be provided to each party at the following addresses:

If to Patelco to:

Angela Jeffers, Esq.
General Counsel
Patelco Credit Union
3 Park Place
Dublin, California 94568
ajeffers@patelco.org

If to Commissioner to: Paul Yee, Senior Counsel
Department of Financial Protection and Innovation
One Sansome Street, Suite 600
San Francisco, California 94104-4448
(415) 972-8569
Paul.Yee@dfpi.ca.gov

21. Signatures. An electronic signature, or a faxed, photocopied, or scanned copy of an original signature, shall be deemed the same as an original signature.

22. Public Record. Patelco acknowledges that this Consent Order shall be a matter of public record.

23. Effective Date. The Consent Order shall become final and effective when signed by all Parties.

24. Authority to Sign. Each signatory hereto covenants that he/she possesses all necessary capacity and authority to sign and enter into this Consent Order and undertakes the obligations set forth herein.

IN WITNESS WHEREOF, the Parties hereto have approved and executed this Consent Order on the dates set forth opposite their respective signatures.

Dated: February 4, 2025 KHALIL MOHSENI
Acting Commissioner of Financial Protection and Innovation

By_____
MARY ANN SMITH
Deputy Commissioner
Enforcement Division

Dated: January 30, 2025 PATELCO CREDIT UNION

By_____
ERIN MENDEZ
President & Chief Executive Officer