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

In the Matter of

GOVERNMENT EMPLOYEES INSURANCE COMPANY

CONSENT ORDER

The New York State Department of Financial Services (the “Department” or “DFS”) and the Government Employees Insurance Company (hereinafter “GEICO” or the “Company”) agree to resolve the matters described herein without further proceedings.

WHEREAS, GEICO is licensed by the Department to sell property and casualty insurance in New York State;

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 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, in early 2021, threat actors conducted a widespread campaign to steal data from insurance companies that had access to consumer information such as drivers’ license numbers (“DLNs”);

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

WHEREAS, threat actors exfiltrated New Yorkers' nonpublic information ("NPI") via GEICO's information systems over multiple Cybersecurity Events;

WHEREAS, the Department initiated an investigation of these Cybersecurity Events and GEICO's compliance with the Cybersecurity Regulation; and

WHEREAS, based on its investigation, the Department has concluded that GEICO violated the following sections of the Cybersecurity Regulation: (1) 23 NYCRR § 500.2(b), which requires all DFS-regulated entities ("Covered Entities") to maintain a Cybersecurity Program that is based on the Covered Entity's risk assessment; (2) 23 NYCRR § 500.3(i) and (k), which require a Covered Entity to implement and maintain written cybersecurity policies that address systems and application development and quality assurance and customer data privacy; (3) 23 NYCRR § 500.5, which requires a Covered Entity not employing effective continuous monitoring to conduct annual penetration testing of the Covered Entity's electronic information resources ("Information Systems") each given year based on relevant identified risks in accordance with the risk assessment; (4) 23 NYCRR § 500.8(a), which requires a Covered Entity's Cybersecurity Program to include written procedures, guidelines, and standards designed to ensure the use of secure development practices for in-house developed applications utilized by the Covered Entity; (5) 23 NYCRR § 500.9(a), which requires a Covered Entity to conduct a periodic risk assessment of the Covered Entity's Information Systems, sufficient to inform the design of the Cybersecurity Program; (6) 23 NYCRR § 500.14(a), which requires a Covered Entity to implement risk-based policies, procedures, and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, NPI by such Authorized Users; and (7) 23 NYCRR § 500.17(b), which requires a Covered Entity to annually certify compliance with the Cybersecurity Regulation in the prior year;

NOW THEREFORE, to resolve this matter without further proceedings pursuant to the Superintendent's authority under Section 408 of the New York Financial Services Law, the Department finds as follows:

THE DEPARTMENT'S FINDINGS

Introduction

1. The Department is the insurance regulator of the State of New York, and the Superintendent of Financial Services 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.

2. 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.

3. To support this critical obligation, the Cybersecurity Regulation places on all Covered Entities an obligation to establish, implement, and maintain Cybersecurity Programs based on risk assessments and designed to protect the confidentiality and integrity of their Information Systems, as well as any consumer NPI contained therein. 23 NYCRR § 500.2(b).

4. The Cybersecurity Regulation contains requirements to protect Covered Entities' Information Systems from threat actors seeking to access and exploit NPI, including requiring that Covered Entities identify and assess risks to stored NPI and use defensive infrastructure and the implementation of policies and procedures to protect against unauthorized access, use, or other malicious acts. 23 NYCRR § 500.2(b).

5. The Cybersecurity Regulation requires that, as part of their Cybersecurity Programs, Covered Entities implement risk-based policies, procedures, and controls designed to monitor the activity of Authorized Users and detect unauthorized access or use of, or tampering with, NPI by such Authorized Users. 23 NYCRR § 500.14.

6. The Cybersecurity Regulation requires Covered Entities not employing effective continuous monitoring to conduct annual penetration testing of the Covered Entity's Information Systems each given year based on relevant identified risks in accordance with the risk assessment. 23 NYCRR § 500.5(a).

7. The Cybersecurity Regulation requires Covered Entities to periodically conduct a risk assessment, which should be updated as reasonably necessary to address changes to the Covered Entities' Information Systems, NPI, or business operations. 23 NYCRR § 500.9(a).

8. The Cybersecurity Regulation requires Covered Entities' Cybersecurity Program to include written procedures, guidelines, and standards designed to ensure the use of secure

development practices for in-house developed applications utilized by the Covered Entity. 23 NYCRR § 500.8(a).

9. Finally, the Cybersecurity Regulation requires Covered Entities to certify compliance with the Cybersecurity Regulation on an annual basis. 23 NYCRR § 500.17(b).

Events at Issue

First Cybersecurity Event

10. On January 23, 2021, GEICO reported a Cybersecurity Event to the Department (the "First Cybersecurity Event"). GEICO's notice to the Department stated that GEICO discovered the First Cybersecurity Event when it noticed a high number of "abandoned quotes" on its internally-developed customer-facing auto insurance application, Auto New Business Customer ("ANBC"), and initiated an internal investigation. An "abandoned quote" occurs when a prospective customer initiates a query for auto insurance pricing, but then does not follow through by purchasing the policy.

11. At the time of the First Cybersecurity Event, GEICO required a prospective customer who was interested in purchasing auto insurance to provide ANBC their name, address, and date of birth. These details were sent to a third-party pre-fill provider, which returned various data, including the prospective customer's DLN. ANBC attempted to display to the prospective customer their DLN, redacted to the last four digits. To do this, ANBC transmitted to the prospective customer's web browser a "JSON" file, a formatted set of data encoded in the JSON format, containing the customer's full unredacted DLN along with a copy of the DLN redacted down to the last four digits.

12. As a consequence of this architecture, threat actors were able to query ANBC with a stolen identity, then use developer tools to extract the full, unredacted DLN from the JSON.

13. Upon discovery of the First Cybersecurity Event, GEICO modified ANBC to cease sending DLNs, redacted or unredacted, to prospective customers.

Second Cybersecurity Event

14. On January 31, 2021, GEICO reported a second Cybersecurity Event (the "Second Cybersecurity Event") to the Department. At the time of the Second Cybersecurity Event, a user submitting an auto insurance claim to GEICO's auto claims website was provided a claims receipt, which ultimately gave the user access to their DLN in the claims system. Threat

actors seeking DLNs fraudulently applied for insurance policies using stolen identities and used fabricated bank account details to purchase these policies. Before GEICO's information systems could verify the validity of the bank accounts, threat actors submitted claims under the fraudulently purchased insurance policy. Upon receiving the fraudulent claims, GEICO's claims website sent the threat actors a claims receipt, which gave the threat actors access to the NPI of the individuals targeted, including unredacted DLNs in plain text.

15. On discovering the Second Cybersecurity Event, GEICO amended its claims website to redact customer DLNs server-side, prior to sending them to the claiming customer.

Third Cybersecurity Event

16. On January 28, 2021, the Department issued an informal alert to certain Covered Entities, including GEICO, stating that the Department "received reports from several sources that cybercriminals are conducting a widespread campaign to steal data from insurance company websites offering instant online automobile insurance premium quotes that display partial or redacted consumer information such as drivers' license numbers," and directing them to "immediately review customer-facing website security."

17. On February 16, 2021, the Department issued an industry-wide Cyber Fraud Alert, warning the auto insurance industry of a "systematic and aggressive campaign to exploit cybersecurity flaws in public-facing [instant quote] websites to steal NPI."

18. On March 4, 2021, GEICO reported a third Cybersecurity Event (the "Third Cybersecurity Event") to the Department. The Third Cybersecurity Event involved a number of issues surrounding an open application programming interface ("API"). An API is a gateway that accepts and transmits information between information systems. At the time of the Third Cybersecurity Event, this API was exclusively used by Auto Sales Agent ("ASA"), GEICO's portal for its insurance agents.

19. The threat actors involved in the Third Cybersecurity Event did not possess login information for ASA. However, the full URL, or address, of this API could be found in back-end source code that could be viewed by an attacker visiting GEICO's auto insurance purchase page. At the time of the Third Cybersecurity Event, ANBC did not use this API, and so there was no reason for ANBC's back-end source code to inform the public of the API's URL.

20. A threat actor could not use this API without the proper session ID and matching information from a variety of session cookies and headers. However, the API would accept either

the session ID a member of the general public received from using GEICO's auto insurance purchase page, or the session ID that could only be obtained by logging into ASA with a GEICO insurance agent's username and password. As they did not possess ASA login information, the threat actors used the session IDs from GEICO's auto insurance purchase page.

21. If this API received a properly formatted request containing a targeted individual's name and address, it would automatically send back additional information, including the targeted individual's DLN.

22. Threat actors discovered this vulnerability and passed properly formatted requests based off stolen identities to the API, using the session ID from GEICO's auto insurance purchase page, receiving back the DLNs of the targeted individuals in an unencrypted and unredacted format.

23. GEICO did not discover the Third Cybersecurity Event until March 1, 2021, when it received communications from threat actors attempting to ransom back to GEICO stolen customer data, as well as separate communications from an individual describing a personal falling out with the threat actors and walking GEICO through precisely the steps taken to steal the customer data and what steps GEICO needed to take to solve the vulnerability.

24. Threat actors discovered this vulnerability as early as November 2020, but by January 22, 2021, had exploited it only about 75 times. By February 24, 2021, however, threat actors had found a way to automate the query, resulting in between 10,000 and 25,000 instances of exploitation per day until March 1, 2021, when GEICO discovered and mitigated the breach. In a subset of these instances, the threat actors were required to provide a legal match for name, address, and date of birth of an existing GEICO customer, before the threat actors were able to obtain the targeted individual's DLN.

25. GEICO resolved the Third Cybersecurity Event by disabling prefill and closing off the open API on March 1, 2021; its customer-facing website was back up and operational by March 4, 2021. Ultimately, GEICO replaced the entire system, including ANBC, with a different application.

GEICO's Cybersecurity Program

26. Although GEICO completed some risk assessments prior to the Cybersecurity Events, it did not perform a periodic risk assessment as required by Section 500.9 of the

Cybersecurity Regulation, nor did it base its Cybersecurity Program or cybersecurity policy on its risk assessment, as required by Sections 500.2(b) and 500.3.

27. Instead, leading up to the Third Cybersecurity Event, GEICO's principal assessment of its risks came in the form of a 2018 penetration test/risk assessment conducted by a third-party evaluator (the "Third-Party Test"). The Third-Party Test was limited in scope, and did not catalogue or consider "Nonpublic Information collected or stored" on GEICO's information systems, *see* 23 NYCRR § 500.9, nor did it evaluate GEICO's claims website or ASA. The Second Cybersecurity Event involved access to consumer NPI on GEICO's claims website. Despite the limited nature of the Third-Party Test, the warnings it did contain were not followed comprehensively.

28. For instance, the Third-Party Test flagged that sensitive information was not encrypted and recommended security improvements, including sanitization, for public-facing web servers and applications, which were only partially implemented. All three Cybersecurity Events involved the sending of unencrypted sensitive data, and the Third Cybersecurity Event involved an unsanitized web application that was sending out the URL of an open API that it did not use.

29. GEICO also failed to address another vulnerability identified by the Third-Party Test. Specifically, the Third-Party Test found that GEICO's public-facing websites might have been sending out IP addresses of internal GEICO servers. In response to this finding, GEICO management searched for the specific IP addresses mentioned by the Third-Party Test, rather than searching GEICO's public-facing applications as a whole for unintended addresses or data, such as the API URL found in ANBC. As such, GEICO management did not use a risk assessment as a basis for informing the architecture of GEICO's information systems, as required by Sections 500.2, 500.3, and 500.9 of the Cybersecurity Regulation.

30. Additionally, certain GEICO cybersecurity policies and procedures were under-implemented. For instance, GEICO implemented the Cybersecurity Regulation's application security requirements, *see* 23 NYCRR §500.8(a), by mandating GEICO developers follow the recommendations of the Open Web Application Security Project ("OWASP"). OWASP publishes a publicly available guide for securing web applications, which asks questions like, "Is any data transmitted in clear text?" and makes recommendations like, "Rate limit API and

controller access to minimize the harm from automated attack tooling." Those recommendations were not fully implemented.

31. The Cybersecurity Regulation requires that Covered Entities implement risk-based policies, procedures, and controls designed to monitor the activity of Authorized Users, *see* 23 NYCRR § 500.14(a)(1). Prior to the Third Cybersecurity Event, the API was used exclusively by Authorized Users: GEICO auto insurance agents. However, the session ID for GEICO's auto insurance purchase page was a valid identifier for accessing the API. As such, there were insufficient procedures and controls regarding the activity of Authorized Users.

32. GEICO was not conducting adequate continuous monitoring, as required by Section 500.5 of the Cybersecurity Regulation, nor implementing risk-based controls to detect unauthorized access of NPI, as required by Section 500.14. These failures are demonstrated by the fact that GEICO did not discover the full scope of the Third Cybersecurity Event via its internal processes, which might have mitigated the number of consumers whose NPI was exfiltrated by threat actors. At the height of the Third Cybersecurity Event, GEICO's open API received thousands of queries a day related to New Yorkers' NPI, a volume of traffic incompatible with the actual number of GEICO's New York-based auto insurance agents. GEICO did not have an appropriate system in place to detect such anomalous patterns of behavior and so was unable to react to the ongoing Cybersecurity Event. Rather, GEICO received notifications from an outside actor that there was a vulnerability in its information systems currently being exploited before GEICO was able to directly uncover the vulnerability.

33. GEICO was not conducting annual penetration testing, as required by Section 500.5 of the Cybersecurity Regulation in the absence of effective continuous monitoring, or other systems to detect, on an ongoing basis, changes in information systems that may create or indicate vulnerabilities. As previously noted, the Third-Party Test was the principal penetration test occurring between the implementation of the Cybersecurity Regulation and the Third Cybersecurity Event. GEICO was explicitly notified of this failing when it commissioned a third-party auditor (the "Auditor") to conduct an audit of GEICO's Cybersecurity Program. In its conclusion, the Auditor recommended that GEICO perform penetration testing against GEICO's most critical applications. Notwithstanding this recommendation, no such tests were performed.

GEICO's Part 500 Compliance Certification

34. Pursuant to 23 NYCRR § 500.17(b), Covered Entities are required to annually certify their compliance with the Cybersecurity Regulation.

35. GEICO certified compliance with the Cybersecurity Regulation for the 2017, 2018, 2019, 2020, and 2021 calendar years.

36. Although GEICO's certification filings referenced in paragraph 35 were largely timely and, the Company asserts, made in good faith when filed, in light of the foregoing findings, GEICO was not in compliance with the Cybersecurity Regulation at the time of the certifications.

37. Thus, GEICO's certification filings for the calendar years 2017 through 2021, attesting to its compliance with the Cybersecurity Regulation, were improper.

Violations of Law and Regulations

38. GEICO did not develop a risk-based Cybersecurity Program, in violation of 23 NYCRR § 500.2(b).

39. GEICO did not ensure the proper implementation of its cybersecurity policies, in violation of 23 NYCRR § 500.3(i) and (k).

40. GEICO did not conduct continuous monitoring or, in the absence of such continuous monitoring, annual penetration testing, in violation of 23 NYCRR § 500.5.

41. GEICO did not develop written procedures designed to ensure the use of secure development practices for in-house developed applications utilized by GEICO, in violation of 23 NYCRR § 500.8(a).

42. GEICO did not conduct a periodic risk assessment of its information systems sufficient to inform the design of its Cybersecurity Program, in violation of 23 NYCRR § 500.9(a).

43. GEICO did not implement effective monitoring of Authorized Users, in violation of 23 NYCRR § 500.14(a).

44. Because GEICO's Cybersecurity Program did not meet all the requirements of the Cybersecurity Regulation, GEICO's Certification of Compliance filings for the calendar years 2017 through 2021 were improper, in violation of 23 NYCRR § 500.17(b).

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

SETTLEMENT PROVISIONS

Monetary Penalty

45. No later than twenty (20) days after the Effective Date (as defined below) of this Consent Order, the Company shall pay a total civil monetary penalty pursuant to New York Financial Services Law § 408 to the Department in the amount of Five Million U.S. Dollars and 00/100 cents ($5,000,000.00). The payment shall be in the form of a wire transfer in accordance with instructions provided by the Department.

46. 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.

47. 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.

48. In assessing a penalty for failures in GEICO's cybersecurity compliance and required reporting, the Department has taken into account factors that include, without limitation: the extent to which GEICO 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.

49. The Department acknowledges GEICO's cooperation throughout this investigation. The Department also recognizes and credits GEICO's efforts to remediate the shortcomings identified in this Consent Order. Among other things, GEICO has demonstrated its commitment to remediation by devoting significant financial and other resources to enhance its Cybersecurity Program, including through changes to its policies, procedures, systems, and governance structures.

Remediation

50. GEICO shall continue to strengthen its controls to protect its information systems and consumers' NPI in accordance with the relevant provisions and definitions of the Cybersecurity Regulation.

a. Cybersecurity Risk Assessment. Within thirty (30) days of the Effective Date of this Consent Order, GEICO shall conduct a Cybersecurity Risk Assessment of its information systems consistent with 23 NYCRR § 500.9. The Cybersecurity Risk Assessment shall contain:

i. the reasonably necessary changes GEICO plans to implement to address changes to GEICO's information systems, NPI or business operations;

ii. any and all plans for revisions of controls to respond to technological developments and evolving threats, which shall consider the particular risks of GEICO'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;

iii. any and all plans for updating (or creating additional) written policies and procedures to include:

1. criteria for the evaluation and categorization of identified cybersecurity risks or threats facing GEICO;
2. criteria for the assessment of the confidentiality, integrity, security, and availability of GEICO's information systems and NPI, including the adequacy of existing controls in the context of identified risks; and
3. requirements describing how identified risks will be mitigated or accepted based on the Risk Assessment and how the Cybersecurity Program will address the risks.

b. Action Plan. Within sixty (60) days of the Effective Date of this Order, GEICO shall submit the results of the Cybersecurity Risk Assessment to the Department, together with a detailed Action Plan describing what steps GEICO plans to take to address any substantial risks or material issues identified in the Cybersecurity Risk Assessment. The Department's approval of the Action Plan shall not be unreasonably withheld.

c. Penetration Test. Within one hundred twenty (120) days of the Effective Date of this Order, GEICO shall conduct penetration test(s) of its information systems based on relevant identified risks in accordance with the Cybersecurity Risk Assessment, if such penetration test(s) have not been conducted in the past fiscal year (starting January 1, 2024). Within sixty (60) days of the completion of the final of such penetration test(s), GEICO shall submit the results of all such penetration test(s) to the Department.

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.

Waiver of Rights

52. 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

53. 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.

54. 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. Furthermore, no further action will be taken by the Department against the Company for conduct in connection with the Department's investigation described in this Consent Order.

55. 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 presentations or written materials submitted to the Department by the Company in connection with this matter.

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

Breach of Consent Order

57. 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.

58. The Company understands and agrees that its failure to make the required showing within the designated time period set forth in Paragraph [57] 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 State Financial Services Law, the New York State Insurance Law, and any other applicable laws, and may use any evidence available to the Department in any ensuing hearings, notices, or orders.

59. All notices, reports, requests, certifications, and other communications to the Department regarding this Consent Order shall be in writing and shall be directed as follows:

For the Department:

Christina Glekas
Assistant Deputy Superintendent
Consumer Protection and Financial Enforcement Division
New York State Department of Financial Services
One State Street
New York, NY 10004

For GEICO:

Government Employees Insurance Company
5260 Western Avenue Chevy Chase, MD 20815
Attention: Tracey Laws, Head of Government and Regulatory Affairs

with an electronic copy simultaneously sent to:

GEICORegulatoryNotices@geico.com

Miscellaneous

60. 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.

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

62. 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.

63. 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.

64. 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.

65. 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.

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

67. Except with regard to the enforcement of this Consent Order, the Company's consent to the provisions of this Consent Order is not intended to bar, estop, waive, preclude, or otherwise prevent the Company from taking any positions of law or fact or raising any defenses in any action taken by any federal or state agency or department, or in any civil action brought by any party against the Company.

68. 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/ David A. Casler
DAVID A. CASLER
Senior Assistant Deputy Superintendent
Consumer Protection and Financial Enforcement

November 18, 2024

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

November 20, 2024

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

November 20, 2024

GOVERNMENT EMPLOYEES INSURANCE COMPANY

By: /s/ Tangela Richter
TANGELA RICHTER
Chief Legal Officer

November 4, 2024

THE FOREGOING IS HEREBY APPROVED. IT IS SO ORDERED.

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

November 25, 2024