

ATTORNEY GENERAL OF THE STATE OF NEW YORK  
BUREAU OF INTERNET & TECHNOLOGY

---

In the Matter of

Assurance No. 23-069

**Investigation by**  
**LETITIA JAMES,**  
**Attorney General of the State of New York, of**

**REFUAH HEALTH CENTER, INC.,**

Respondent.

---

**ASSURANCE OF DISCONTINUANCE**

The Office of the Attorney General of the State of New York (“NYAG”) commenced an investigation pursuant to Executive Law § 63(12) and General Business Law (“GBL”) §§ 899-aa and 899-bb into a data breach at Refuah Health Center, Inc. (“Refuah”). This Assurance of Discontinuance (“Assurance”) contains the findings of the investigation and the relief agreed to by the NYAG and Respondent Refuah, whether acting through its respective directors, officers, employees, representatives, agents, affiliates, or subsidiaries (collectively, the “Parties”).

**NYAG FINDINGS**

1. Refuah is a New York-based federally qualified health center that receives federal funding for providing medical services to underserved communities. The company operates three facilities in New York, each of which provides a variety of medical services, and five mobile medical vans.

**The Data Breach**

2. In late May 2021, Refuah’s systems were targeted in an extortion scheme and

cyberattack by actors claiming to be the Lorenz Ransomware group. Attackers were able to gain access to a Refuah system used for viewing video from internal cameras monitoring the company's facilities. Access to this system was protected by a static four-digit code.

3. From this system, attackers were then able to remotely access Refuah's private network using login credentials for an administrative account that were stolen during the attack. The administrative credentials the attackers exploited to gain remote access were associated with a Refuah account used by a former IT vendor. The credentials had not been changed for at least 11 years. Further, despite the fact that the IT vendor had not worked with Refuah since 2014, the account used by the vendor had not been deleted or disabled. Multi-factor authentication was not enabled for the account.

4. Once on Refuah's network, the attackers had access to a variety of Refuah systems and data that contained patient information, including thousands of files stored on shared network space, employee emails, and a database associated with Refuah's dental practice. Many of these files were not encrypted at the file level and were available to an attacker who gained access to the shared network space.

5. Over the course of two days, the attackers exfiltrated files and data that contained patient information. The attackers also deployed ransomware that encrypted several of Refuah's systems, rendering them inaccessible without the decryption key held by the attackers.

6. Refuah discovered the attack on June 1, 2021. By that time, the attackers had exfiltrated approximately a terabyte of data. Refuah was unable to identify the files that had been taken, however, as Refuah did not have systems in place to log this activity, and system artifacts that might have indicated the scope of the breach were lost when systems were rebuilt to block

attackers' continued access and restore services and systems supporting Refuah's ongoing medical operations and patient care.

7. The attackers subsequently provided Refuah with information concerning the systems and data they had accessed, including a listing of thousands of files the attackers claimed to have taken, and a screenshot of a single page of patient information containing data consistent with the database. The attackers demanded a ransom payment to provide the decryption key to unlock the encrypted files and not publicly release the stolen information.

8. Refuah retained outside counsel to conduct an analysis to identify patients who had been impacted in the breach. Outside counsel promptly engaged a cybersecurity firm to conduct an investigation. The analysis focused on files stored in areas of the shared network space that the attackers had accessed.

9. Refuah did not, however, investigate whether attackers had accessed the database, even though: (a) the screenshot containing information on 34 patients that the attackers provided to representatives of the company contained information only found in the database and (b) the screenshot was not observed to originate from Refuah's electronic medical records system, but likely reflected data in an actor-controlled database that had originated from Refuah's electronic medical records system.

10. Refuah ultimately determined that attackers had access to files containing the information of more than 260,740 patients, 175,077 of which were New York residents. These files contained a variety of sensitive patient information. Different files contained different types of information, including patient names, addresses, phone numbers, Social Security numbers, driver's license numbers, state identification numbers, dates of birth, bank/financial account

information, credit/debit card information, medical treatment/diagnosis information, Medicare/Medicaid numbers, medical record numbers, patient account numbers, and health insurance policy numbers. Refuah concluded its analysis on March 2, 2022 and began providing notice of the breach to impacted patients on April 29, 2022. Refuah offered credit monitoring services to those individuals whose social security numbers had been impacted.

11. During the NYAG's subsequent investigation, Refuah determined that the database contained the data of approximately 195,974 to 233,575 patients, approximately 179,952 to 216,444 of which were New York residents. Approximately 72,000 to 79,000 of those New York residents did not receive notice.

#### Refuah's Risk Assessment in March 2017

12. In March 2017, a Refuah vendor conducted a HIPAA risk assessment for Refuah. This was the last HIPAA risk assessment conducted prior to the attack in May 2021.

13. The vendor identified several issues related to Refuah's data security program that were not resolved prior to the attack in 2021.

#### Refuah's Data Security Program in May 2021

14. At the time of the attack in May 2021, Refuah's data security program was deficient in several areas. These included:

- a. Evaluation: Refuah failed to conduct periodic evaluations of its security policies and procedures.
- b. Access Controls and Authentication: Refuah failed to implement and maintain appropriate controls to limit access to sensitive data, including by failing to decommission inactive user accounts, failing to rotate user account credentials, failing

to use multi-factor authentication, and failing to restrict employees' access to only those resources and data that were necessary for their business functions.

- c. Protection of Sensitive Information: Refuah failed to encrypt sensitive patient data maintained at rest.
- d. Audit Controls and Monitoring: Refuah failed to implement appropriate systems for recording, and reviewing records of, user activity on its network.
- e. Incident Response: Refuah failed to conduct an appropriate investigation to identify the patients whose information was accessed without authorization.
- f. Retention Policies: Refuah failed to maintain and adhere to a written policy governing the retention of patient data.

15. Respondent has represented that, following the attack, it has taken steps to improve its data security program, including (i) upgrading its network firewalls to models and services that employ behavioral based threat intelligence monitoring; (ii) installing an Endpoint Detection and Response (EDR) solution on endpoints, that uses machine learning to detect threats; (iii) configured firewall rules to reduce risk; (iv) contracting for an external cybersecurity vendor providing 24/7 Security Operations Center (SOC) services with threat alerts, including monitoring of account activity; (vi) implementing two factor authentication for remote access to internal systems; and (vii) adopting a cloud-based email system.

### **Respondent's Violations**

16. Refuah is a "covered entity" under the Health Insurance Portability and Accountability Act (HIPAA) subject to the HIPAA Security Rule, 45 C.F.R. Part 160 and Part 164 Subparts A and C, and the Breach Notification Rule, 45 C.F.R. Part 164 Subpart D. Refuah's

conduct violated both the HIPAA Security Rule and the Breach Notification Rule, including:

- a. § 164.308(a)(1)(i), which requires policies and procedures to prevent, detect, contain, and correct security violations;
- b. § 164.308(a)(1)(ii)(A) and (B), which require an accurate and thorough risk analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all ePHI, and implementation of security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a);
- c. § 164.308(a)(1)(ii)(D), which requires procedures to regularly review records of information system activity;
- d. § 164.308(a)(4)(i), which requires policies and procedures for authorizing access to ePHI;
- e. § 164.308(a)(4)(ii)(B) and (C), which require policies and procedures for granting access to ePHI, and establishing, documenting, reviewing, and modifying user's right of access based on access authorization policies;
- f. § 164.308(a)(5)(ii)(C) and (D), which require procedures for monitoring log-in attempts and reporting discrepancies, and procedures for creating, changing, and safeguarding passwords;
- g. § 164.308(a)(6)(i) and (ii), which require policies and procedures to address security incidents, and identifying and responding to suspected or known security incidents;
- h. § 164.308(a)(8), which requires periodic technical and nontechnical evaluations of a covered entity's security policies and procedures;
- i. § 164.312(a)(1) and (2)(iv), which require technical policies and procedures for systems that maintain ePHI to allow access to persons granted access rights, and a mechanism to encrypt ePHI;
- j. § 164.312(b), which requires controls for recording and examining activity in systems that contain or use ePHI;
- k. § 164.312(d), which requires procedures to verify that a person seeking access to

ePHI is the one claimed;

1. § 164.404, which requires notification of individuals whose unsecured PHI is accessed as the result of a breach.

17. Refuah's conduct also violated GBL § 899-aa, which requires disclosure of a data breach in the most expedient time possible and without unreasonable delay; and GBL § 899-bb, which requires implementation and maintenance of reasonable safeguards to protect consumer information.

18. Respondent neither admits nor denies the NYAG's findings, paragraphs 1-17 above.

19. The NYAG finds the relief and agreements contained in this Assurance appropriate and in the public interest. THEREFORE, the NYAG is willing to accept this Assurance pursuant to Executive Law § 63(15), in lieu of commencing a statutory proceeding for violations of GBL §§ 899-aa and 899-bb, the HIPAA Security Rule, 45 C.F.R. Part 160 and Part 164 Subparts A and C, and the Breach Notification Rule, 45 C.F.R. Part 164 Subpart D.

IT IS HEREBY UNDERSTOOD AND AGREED, by and between the Parties:

**PROSPECTIVE RELIEF**

20. For the purposes of this Assurance, the following definitions shall apply:
  - a. "Consumer" shall mean any person residing in, or who has resided in New York.
  - b. "Consumer Personal Information" shall mean Private Information and PHI of a Consumer.
  - c. "Private Information" shall mean private information as defined in New York General Business Law § 899-aa(1)(b).

- d. "Protected Health Information" or "PHI" shall mean health information, as defined in section 160.103 of title 45 of the Code of Federal Regulations implementing the Health Insurance Portability and Accountability Act ("HIPAA").
- e. "Security Event" shall mean unauthorized access to or acquisition of Consumer Personal Information owned, licensed, or maintained by Respondent.

### **GENERAL COMPLIANCE**

21. Respondent shall comply with GBL §§ 899-aa and 899-bb, the HIPAA Security Rule, 45 C.F.R. Part 160 and Part 164 Subparts A and C, and the Breach Notification Rule, 45 C.F.R. Part 164 Subpart D in connection with its collection, use, and maintenance of Consumer Personal Information.

### **INFORMATION SECURITY PROGRAM**

22. Respondent shall maintain a comprehensive Information Security Program that is reasonably designed to protect the security, integrity, and confidentiality of Consumer Personal Information that Respondent collects, stores, transmits, and/or maintains. Respondent shall document in writing the content, implementation, and maintenance of the Information Security Program. The Information Security Program shall, at a minimum, include the following processes:

- a. Assess and document, not less than annually, internal and external risks to the security, integrity, and confidentiality of Consumer Personal Information;
- b. Design, implement, and maintain reasonable administrative, technical, and physical safeguards to control the internal and external risks Respondent identified that are appropriate to: (i) the size and complexity of Respondent's



operations; (ii) the nature and scope of Respondent's activities; and (iii) the volume and sensitivity of the Consumer Personal Information that Respondent collects, stores, transmits, and/or maintains.

- c. Assess, not less than annually, the sufficiency of any safeguards in place to address the internal and external risks Respondent identified, and modify the Information Security Program based on the results to ensure that the safeguards comply with (b) above;
- d. Test and monitor the effectiveness of the safeguards not less than annually, and modify the Information Security Program based on the results to ensure the safeguards comply with (b) above;
- e. Select service providers capable of appropriately safeguarding Consumer Personal Information, contractually require service providers to implement and maintain appropriate safeguards to protect Consumer Personal Information, and take appropriate steps to verify service providers are complying with the contractual requirements;
- f. Evaluate the Information Security Program not less than annually and adjust the Program in light of any changes to Respondent's operations or business arrangements, or any other circumstances that Respondent knows or has reason to know may have an impact on the effectiveness of the Program.

23. Respondent shall appoint a qualified employee to be responsible for implementing, maintaining, and monitoring the Information Security Program. The appointed individual shall have credentials, background, and expertise in information security appropriate to the level, size,

and complexity of the individual's role in implementing, maintaining, and monitoring the Information Security Program. The appointed individual shall report at a minimum semi-annually to the Chief Executive Officer and senior management, and shall report at a minimum semi-annually to the Board of Directors or equivalent governing body, or an appropriate committee thereof, concerning Respondent's security posture, the security risks faced by Respondent, and the Information Security Program.

24. Respondent shall provide notice of the requirements of the AOD to its management-level employees responsible for implementing, maintaining, or monitoring the Information Security Program and shall implement appropriate training of such employees. The notice and training required under this paragraph shall be provided to the appropriate employees within sixty (60) days of the effective date of the AOD, or within thirty (30) days of when an employee first assumes responsibility for implementing, maintaining, or monitoring the Information Security Program.

#### **PERSONAL INFORMATION SAFEGUARDS AND CONTROLS**

25. Access and Authentication Controls: Respondent shall establish, implement, and maintain policies and procedures to appropriately limit access to Consumer Personal Information. The policies and procedures shall require, at a minimum:

- a. Granting individuals and organizations access only to those resources and data that are necessary for their business functions; for the avoidance of doubt, this subparagraph includes resources and data maintained on Respondent's network;
- b. Promptly removing individuals' and organizations' access to resources and data

upon separation, or, upon an individual's change in responsibilities, promptly removing the individual's access to resources and data that are no longer needed to discharge those responsibilities;

- c. Requiring completion of multifactor authentication to remotely access resources and data;
- d. Regularly rotating credentials used to access resources and data; and
- e. Conducting an audit, not less than semi-annually, to ensure compliance with these policies.

Notwithstanding the foregoing, Respondent shall be deemed in compliance with subparagraph (c), (d), or (e) if, with respect to the subparagraph, it implements an equivalent, widely adopted industry measure and the person responsible for the Information Security Program: (1) approve(s) in writing the use of such equivalent measure, and (2) documents in writing how the measure is widely adopted and at least equivalent to the security provided by the subparagraph.

26. Account Audit: Within ninety (90) days of the effective date of this Assurance, Respondent shall conduct an audit to ensure compliance with subparagraphs 25(a) and (b).

27. Monitoring and Logging: Respondent shall implement controls to monitor and log all security and operational activity related to Respondent's networks, systems, and assets, and establish and maintain policies and procedures to regularly review appropriate records for anomalous activity. Respondent shall store logs of events that indicate anomalous activity for a period of time that is sufficient to detect, investigate, and respond to security incidents.

28. Encryption: Respondent shall encrypt Consumer Personal Information that it collects, stores, transmits, and/or maintains using an encryption method appropriate to the

sensitivity of the Consumer Personal Information.

### **INFORMATION SECURITY PROGRAM ASSESSMENTS**

29. Within one (1) year of the effective date of this Assurance, Respondent shall obtain a comprehensive assessment of the information security of Respondent's network conducted by an independent third-party assessor who uses procedures and standards generally accepted in the profession which shall be documented (a "Third-Party Assessment Report") and provided to the NYAG within two weeks of completion. Annually for five (5) years thereafter, Respondent shall obtain Third-Party Assessment Reports which Respondent shall maintain for seven (7) years from the date of each Third-Party Assessment Report and shall provide to the NYAG upon request. The Third-Party Assessment Reports shall:

- a. Identify the specific administrative, technical, and physical safeguards maintained by Respondent's Information Security Program;
- b. Document the extent to which the identified administrative, technical, and physical safeguards are appropriate considering Respondent's size and complexity, the nature and scope of Respondent's activities, the sensitivity of the Consumer Personal Information maintained on the network and the reasonably anticipated risks; and
- c. Assess the extent to which the administrative, technical, and physical safeguards that have been implemented by Respondent meet the requirements of the Information Security Program and the Assurance.

### **DATA RETENTION**

30. Respondent shall establish, implement, and maintain written policies and

procedures that govern the retention of Consumer Personal Information.

### **INCIDENT RESPONSE**

31. Respondent shall establish, implement and maintain, a comprehensive incident response plan. The incident response plan shall be documented in writing and include, at a minimum, the following policies:

- a. If Respondent has reason to believe a Security Event has occurred, Respondent shall promptly conduct a reasonable investigation to determine, at a minimum, whether Consumer Personal Information was accessed or acquired without authorization, and, if so, what Consumer Personal Information was accessed or acquired.
- b. If Respondent determines Consumer Personal Information has been, or is reasonably likely to have been, accessed or acquired without authorization, Respondent shall expediently provide each Consumer whose Personal Information has been, or is reasonably believed to have been, accessed or acquired without authorization, by email or letter or other legally valid forms of substitute notice established under New York law, material information concerning the Security Event that is reasonably individualized to the customer including, at a minimum, the timing of the Security Event, whether the Consumer's Personal Information was accessed or acquired without authorization, what Personal Information was accessed or acquired, and what actions have been taken to protect the Consumer. If necessary in order to provide expedient notice to Consumers, Respondent may provide more than one notice that collectively provide all material information.

## **NOTICE AND CREDIT MONITORING**

32. Within ninety (90) days of the effective date, Respondent shall provide notice of the 2021 Security Event to all Consumers whose information was contained within the database associated with Refuah's dental practice and who were not previously provided notice. Where multiple Consumers are members of a single household residing at the same address, notice may be provided to a single household. Such notice shall be provided in a manner consistent with the requirements of GBL § 899-aa and the HIPAA Breach Notification Rule.

33. Respondent shall offer identity theft protection services to all Consumers whose information was contained within the database associated with Refuah's dental practice, who were not previously offered identity theft protection services, and whose social security number was impacted. Such offer shall be for services at least reasonably equivalent in length and coverage as the offers previously made to Consumers to whom Respondent has previously offered identity theft protection services.

## **MONETARY RELIEF**

34. Respondent shall pay to the State of New York four hundred and fifty thousand dollars (\$450,000) in penalties and costs as follows:

- a. a first payment of one hundred seventeen thousand dollars (\$117,000) shall be paid in full by January 31, 2024;
- b. a second payment of one hundred seventeen thousand dollars (\$117,000) shall be paid in full by June 30, 2024;
- c. a third payment of one hundred sixteen thousand dollars (\$116,000) shall be paid in full by January 31, 2025;

d. one hundred thousand dollars (\$100,000) shall be suspended; provided however, that the suspended amount will be immediately due and payable if the NYAG finds that Respondent's Fiscal Year 2022 financial statement submitted to the NYAG contains material misstatements or Respondent fails to spend \$1.2 million dollars (\$1,200,000) to develop and maintain its information security program between Fiscal Year 2024 and Fiscal Year 2028.

35. Payments shall be made by wire transfer in accordance with instructions provided by a NYAG representative and shall reference Assurance No. 23-069.

#### **MISCELLANEOUS**

36. Respondent expressly agrees and acknowledges that NYAG may initiate a subsequent investigation, civil action, or proceeding to enforce this Assurance, for violations of the Assurance, or if the Assurance is voided pursuant to paragraph 43, and agrees and acknowledges that in the event the Assurance is voided pursuant to paragraph 43:

- a. any statute of limitations or other time-related defenses are tolled from and after the effective date of this Assurance;
- b. the NYAG may use statements, documents or other materials produced or provided by Respondent prior to or after the effective date of this Assurance;
- c. any civil action or proceeding must be adjudicated by the courts of the State of New York, and that Respondent irrevocably and unconditionally waives any objection based upon personal jurisdiction, inconvenient forum, or venue; and
- d. evidence of a violation of this Assurance shall constitute prima facie proof of a violation of the applicable law pursuant to Executive Law § 63(15).

37. If a court of competent jurisdiction determines that Respondent has violated the Assurance, Respondent shall pay to the NYAG the reasonable cost, if any, of obtaining such determination and of enforcing this Assurance, including without limitation legal fees, expenses, and court costs.

38. This Assurance is not intended for use by any third party in any other proceeding. This Assurance is not intended, and should not be construed, as an admission of liability by Respondent.

39. All terms and conditions of this Assurance shall continue in full force and effect on any successor, assignee, or transferee of Respondent. Respondent shall include in any such successor, assignment or transfer agreement a provision that binds the successor, assignee or transferee to the terms of the Assurance. No party may assign, delegate, or otherwise transfer any of its rights or obligations under this Assurance without the prior written consent of NYAG. Notwithstanding the forgoing, nothing herein waives or limits any immunity, supremacy or other authority applicable or assertable by or on behalf of the federal government or any agency thereof.

40. Nothing contained herein shall be construed as to deprive any person of any private right under the law.

41. Any failure by the NYAG to insist upon the strict performance by Respondent of any of the provisions of this Assurance shall not be deemed a waiver of any of the provisions hereof, and the NYAG, notwithstanding that failure, shall have the right thereafter to insist upon the strict performance of any and all of the provisions of this Assurance to be performed by Respondent.

42. All notices, reports, requests, and other communications pursuant to this Assurance



must reference Assurance No. 23-069, and shall be in writing and shall, unless expressly provided otherwise herein, be given by hand delivery; express courier; or electronic mail at an address designated in writing by the recipient, followed by postage prepaid mail, and shall be addressed as follows:

If to Respondent Refuah, to:

Alexandra Khorover, Esq.  
Chief Strategic Officer & General Counsel  
728 North Main Street  
Spring Valley, NY 10977

If to NYAG, to:

Jordan Adler, Senior Enforcement Counsel, or in his absence,  
to the person holding the title of Bureau Chief  
Bureau of Internet & Technology  
28 Liberty Street  
New York, NY 10005

43. NYAG has agreed to the terms of this Assurance based on, among other things, the representations made to NYAG by Respondent and its counsel and NYAG's own factual investigation as set forth in the Findings, paragraphs 1-17 above. Respondent represents and warrants that neither it nor its counsel have made any material representations to NYAG that are inaccurate or misleading. If any material representations by Respondent or its counsel are later found to be inaccurate or misleading, this Assurance is voidable by NYAG in its sole discretion.

44. No representation, inducement, promise, understanding, condition, or warranty not set forth in this Assurance has been made to or relied upon by Respondent in agreeing to this Assurance.

45. Respondent represents and warrants, through the signature below, that the terms and conditions of this Assurance are duly approved.

46. Unless a term limit for compliance is otherwise specified within this Assurance, the Respondent's obligations under this Assurance are enduring. Nothing in this Agreement shall relieve Respondent of other obligations imposed by any applicable state or federal law or regulation or other applicable law.

47. Respondent agrees not to take any action or to make or permit to be made any public statement denying, directly or indirectly, any finding in the Assurance or creating the impression that the Assurance is without legal or factual basis. Nothing in this paragraph affects Respondent's right to take legal or factual positions in defense of litigation or other legal proceedings to which the NYAG is not a party.

48. Nothing contained herein shall be construed to limit the remedies available to NYAG in the event that Respondent violates the Assurance after its effective date.

49. This Assurance may not be amended except by an instrument in writing signed on behalf of the Parties to this Assurance.

50. In the event that any one or more of the provisions contained in this Assurance shall for any reason be held by a court of competent jurisdiction to be invalid, illegal, or unenforceable in any respect, in the sole discretion of NYAG, such invalidity, illegality, or unenforceability shall not affect any other provision of this Assurance.

51. Respondent acknowledges that it has entered this Assurance freely and voluntarily and upon due deliberation with the advice of counsel.

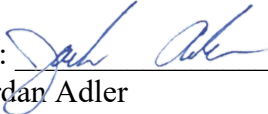
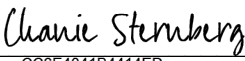
52. This Assurance shall be governed by the laws of the State of New York without regard to any conflict of laws principles.

53. The Assurance and all its terms shall be construed as if mutually drafted with no

presumption of any type against any party that may be found to have been the drafter.

54. This Assurance may be executed in multiple counterparts by the Parties hereto. All counterparts so executed shall constitute one agreement binding upon all Parties, notwithstanding that all Parties are not signatories to the original or the same counterpart. Each counterpart shall be deemed an original to this Assurance, all of which shall constitute one agreement to be valid as of the effective date of this Assurance. For purposes of this Assurance, copies of signatures shall be treated the same as originals. Documents executed, scanned and transmitted electronically and electronic signatures shall be deemed original signatures for purposes of this Assurance and all matters related thereto, with such scanned and electronic signatures having the same legal effect as original signatures.

55. The effective date of this Assurance shall be December 29, 2023.

<p><b>LETITIA JAMES</b> <b>ATTORNEY GENERAL OF THE</b> <b>STATE OF NEW YORK</b></p> <p>By:  _____ Jordan Adler Bureau of Internet and Technology New York State Attorney General 28 Liberty St. New York, NY 10005 Phone: (212) 416-8433 Fax: (212) 416-8369</p> <p><u>1/5/2024</u> Date</p>	<p><b>REFUAH HEALTH CENTER, INC.</b></p> <p><small>DocuSigned by:</small> By:  _____ <small>CC6E4041B4414ED...</small> Chanie Sternberg President &amp; CEO Refuah Health Center, Inc. 728 N. Main Street Spring Valley, NY 10977</p> <p><u>12/29/2023</u> Date</p>
---	---