UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

_____, Individually and on behalf of all others similarly situated, Plaintiff, v. UNISYS CORPORATION, PETER A. ALTABEF, MICHAEL M. THOMPSON, and DEBRA MCCANN, Defendants.	**Case No:** **CLASS ACTION COMPLAINT FOR VIOLATIONS OF THE FEDERAL SECURITIES LAWS** JURY TRIAL DEMANDED

Plaintiff __ ("Plaintiff"), individually and on behalf of all other persons similarly situated, by Plaintiff's undersigned attorneys, for Plaintiff's complaint against Defendants (defined below), alleges the following based upon personal knowledge as to Plaintiff and Plaintiff's own acts, and information and belief as to all other matters, based upon, among other things, the investigation conducted by and through his attorneys, which included, among other things, a review of the Defendants' public documents, public filings, wire and press releases published by and regarding Unisys Corporation ("Unisys" or the "Company"), and information readily obtainable on the Internet. Plaintiff believes that substantial evidentiary support will exist for the allegations set forth herein after a reasonable opportunity for discovery.

NATURE OF THE ACTION

1. This is a class action on behalf of persons or entities who purchased or otherwise acquired publicly traded Unisys securities between February 26, 2021 and October 22, 2024, inclusive (the "Class Period"). Plaintiff seeks to recover compensable damages caused by

Defendant's violations of the federal securities laws under the Securities Exchange Act of 1934 (the "Exchange Act")

JURISDICTION AND VENUE

2. The claims asserted herein arise under and pursuant to Sections 10(b) and 20(a) of the Exchange Act (15 U.S.C. §§ 78j(b) and 78t(a)) and Rule 10b-5 promulgated thereunder by the SEC (17 C.F.R. § 240.10b-5).

3. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1331, and Section 27 of the Exchange Act (15 U.S.C. §78aa).

4. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b) and Section 27 of the Exchange Act (15 U.S.C. § 78aa(c)) as the alleged misstatements entered and the subsequent damages took place in this judicial district.

5. In connection with the acts, conduct and other wrongs alleged in this complaint, Defendants, directly or indirectly, used the means and instrumentalities of interstate commerce, including but not limited to, the United States mails, interstate telephone communications and the facilities of the national securities exchange.

PARTIES

6. Plaintiff ___, as set forth in the accompanying certification, incorporated by reference herein, purchased Unisys securities during the Class Period and was economically damaged thereby.

7. Defendant Unisys describes itself as follows:

> Unisys Corporation, a Delaware corporation (Unisys, we, our, or the company), ***is a global information technology (IT) solutions company that powers breakthroughs for the world's leading organizations***. ***Our clients rely on us to help solve many of their toughest business and technology challenges in highly complex, regulated and heterogeneous environments***. Our solutions and services are provided through global delivery capabilities, which allows us to execute large-scale, rapid technology migration and

> modernization projects. From our origins dating back to 1873 through the formation of Unisys in 1986, we have built a legacy of innovation and a reputation of trust.
>
> In recent decades, enterprise and government interactions with customers, suppliers, employees and citizens have shifted increasingly to digital channels. Cloud computing, artificial intelligence (AI), machine learning and quantum computing have pushed the required pace of innovation and led to a proliferation of data. At the same time, organizations face rising costs and complexity of managing IT infrastructure, data, security and compliance while integrating new technologies. We have a long track record of helping clients navigate technological change and architecting innovative solutions that simplify and accelerate digital transformation.
>
> (Emphasis added).

8. Unisys is incorporated in Delaware and its head office is located at 801 Lakeview Drive, Suite 100, Blue Bell, Pennsylvania 19422. Unisys' common stock trades on the New York Stock Exchange (the "NYSE") under the ticker symbol "UIS."

9. Defendant Peter A. Altabef ("Altabef") served as the Company's Chief Executive Officer ("CEO") and Chairman of the Board of Directors (the "Board") throughout the Class Period.

10. Defendant Michael M. Thompson ("Thompson") served as the Company's Chief Financial Officer ("CFO") and Senior Vice President from the beginning of the Class Period until May 2, 2022, and now serves as the Company's Chief Operating Officer and President.

11. Defendant Debra McCann ("McCann") has served as the Company's CFO and Executive Vice President from May 2022 to the present.

12. Defendants Altabef, Thompson, and McCann are collectively referred to herein as the "Individual Defendants."

13. Each of the Individual Defendants:

(a) directly participated in the management of the Company;

(b) was directly involved in the day-to-day operations of the Company at the highest levels;

(c) was privy to confidential proprietary information concerning the Company and its business and operations;

(d) was directly or indirectly involved in drafting, producing, reviewing and/or disseminating the false and misleading statements and information alleged herein;

(e) was directly or indirectly involved in the oversight or implementation of the Company's internal controls;

(f) was aware of or recklessly disregarded the fact that the false and misleading statements were being issued concerning the Company; and/or

(g) approved or ratified these statements in violation of the federal securities laws.

14. Unisys is liable for the acts of the Individual Defendants and its employees under the doctrine of *respondeat superior* and common law principles of agency because all of the wrongful acts complained of herein were carried out within the scope of their employment.

15. The scienter of the Individual Defendants and other employees and agents of the Company is similarly imputed to the Company under *respondeat superior* and agency principles.

16. Unisys and the Individual Defendants are collectively referred to herein as "Defendants."

SUBSTANTIVE ALLEGATIONS

Materially False and Misleading Statements Issued During the Class Period

17. On February 26, 2021, before market hours, Unisys filed with the SEC its annual

report on Form 10-K for the year ending December 31, 2020 (the "2020 Annual Report"). Attached to the 2020 Annual Report were certifications pursuant to the Sarbanes-Oxley Act of 2002 ("SOX") signed by Defendants Altabef and Thompson attesting to the accuracy of financial reporting, the disclosure of any material changes to the Company's internal control over financial reporting and the disclosure of all fraud.

18. The 2020 Annual Report contained the following statement regarding the Company's disclosure controls and procedures:

> As of the end of the period covered by this Annual Report, management performed, with the participation of the Chief Executive Officer (CEO) and the Chief Financial Officer (CFO), an evaluation of the effectiveness of the company's disclosure controls and procedures as defined in Rules 13a-15(e) and 15d-15(e) of the Securities Exchange Act of 1934 (the Exchange Act). In designing and evaluating the disclosure controls and procedures, management recognized that any controls and procedures, no matter how well designed and operated, can provide only reasonable assurance of achieving the desired control objectives. ***Based upon that evaluation, the CEO and the CFO concluded that, as of December 31, 2020, the company's disclosure controls and procedures were effective to provide reasonable assurance that information required to be disclosed in our Exchange Act reports is recorded, processed, summarized and reported within the time periods specified by the SEC, and that such information is accumulated and communicated to management, including the CEO and CFO, as appropriate, to allow timely decisions regarding required disclosure.***
>
> (Emphasis added).

19. The statement in ¶ 18 was materially false and misleading at the time it was made because the Company lacked adequate internal controls as a result of having no meaningful system for Company cybersecurity personnel to report cybersecurity incidents to senior management, which led to material cybersecurity events not being reported to investors in a timely manner.

20. The 2020 Annual Report contained the following risk disclosure:

> ***Cybersecurity breaches could result in the company incurring significant costs and could harm the company's business and reputation.***
>
> The company's business includes managing, processing, storing and transmitting proprietary and confidential data, including personal information, intellectual property and

> proprietary business information, within the company's own IT systems and those that the company designs, develops, hosts or manages for clients. ***Cybersecurity breaches*** involving these systems by hackers, other third parties or the company's employees, despite established security controls, ***could disrupt*** these systems or result in the loss or corruption of data or the unauthorized disclosure or misuse of information of the company, its clients or others. ***This could result in claims, investigations, litigation and legal liability for the company, lead to the loss of existing or potential clients and adversely affect the market's perception of the security and reliability of the company's services and products***. In addition, such breaches could subject the company to fines and penalties for violations of laws and result in the company incurring other significant costs. This may negatively impact the company's reputation and financial results.
>
> (Emphasis added).

21. The statement in ¶ 20 was materially false and misleading at the time it was made because the Company spoke of material cybersecurity breaches in hypothetical terms when, in actuality, the risk of a material cybersecurity breach had already materialized, resulting in heightened regulatory, reputational, and litigation risk to the company.

22. The 2020 Annual Report contained the following risk disclosure:

> ***A significant disruption in the company's IT systems could adversely affect the company's business and reputation.***
>
> ***We rely extensively on our IT systems to conduct our business and perform services for our clients***. ***Our systems are subject to damage or interruption from*** power outages, telecommunications failures, ***computer viruses and malicious attacks***, ***cybersecurity breaches*** and catastrophic events. If our systems are accessed without our authorization, damaged or fail to function properly, we could incur substantial repair or replacement costs, experience data loss and impediments to our ability to conduct our business, ***and damage the market's perception of our services and products. In addition, a disruption could result in the company failing to meet performance standards and obligations in its client contracts***, which could subject the company to liability, penalties and contract termination. This may adversely affect the company's reputation and financial results.
>
> (Emphasis added).

23. The statement in ¶ 22 was materially false and misleading at the time it was made because the Company spoke of cybersecurity breaches in hypothetical terms when, in actuality, the risk had already materialized. Specifically, Unisys network user accounts were compromised

between January 2020 and August 2021 by a hacking group associated with the Russian government.

24. On February 22, 2022, Unisys filed with the SEC its annual report on Form 10-K for the year ending December 31, 2021 (the "2021 Annual Report"). Attached to the 2021 Annual Report were certifications pursuant to SOX signed by Defendants Altabef and Thompson attesting to the accuracy of financial reporting, the disclosure of any material changes to the Company's internal control over financial reporting and the disclosure of all fraud.

25. The 2021 Annual Report contained the following statement regarding the Company's disclosure controls and procedures:

> As of the end of the period covered by this Annual Report, management performed, with the participation of the Chief Executive Officer (CEO) and the Chief Financial Officer (CFO), an evaluation of the effectiveness of the company's disclosure controls and procedures as defined in Rules 13a-15(e) and 15d-15(e) of the Securities Exchange Act of 1934 (the Exchange Act). In designing and evaluating the disclosure controls and procedures, management recognized that any controls and procedures, no matter how well designed and operated, can provide only reasonable assurance of achieving the desired control objectives. ***Based upon that evaluation, the CEO and the CFO concluded that, as of December 31, 2021, the company's disclosure controls and procedures were effective to provide reasonable assurance that information required to be disclosed in our Exchange Act reports is recorded, processed, summarized and reported within the time periods specified by the SEC, and that such information is accumulated and communicated to management, including the CEO and CFO, as appropriate, to allow timely decisions regarding required disclosure***.
>
> (Emphasis added).

26. The statement in ¶ 25 was materially false and misleading at the time it was made because the Company lacked adequate internal controls as a result of having no meaningful system for Company cybersecurity personnel to report cybersecurity incidents to senior management, which led to material cybersecurity events not being reported to investors in a timely manner.

27. The 2021 Annual Report contained the following risk disclosure:

Cybersecurity breaches could result in the company incurring significant costs and

could harm the company's business and reputation.

The company's business includes managing, processing, storing and transmitting proprietary and confidential data, including personal information, intellectual property and proprietary business information, within the company's own IT systems and those that the company designs, develops, hosts or manages for clients. ***Cybersecurity breaches*** involving these systems by hackers, other third parties or the company's employees, despite established security controls, ***could disrupt*** these systems or result in the loss or corruption of data or the unauthorized disclosure or misuse of information of the company, its clients or others. ***This could result in claims, investigations, litigation and legal liability for the company, lead to the loss of existing or potential clients and adversely affect the market's perception of the security and reliability of the company's services and products. In addition, such breaches could subject the company to fines and penalties for violations of laws and result in the company incurring other significant costs***. This may negatively impact the company's reputation and financial results.

(Emphasis added).

28. The statement in ¶ 27 was materially false and misleading at the time it was made because the Company spoke of material cybersecurity breaches in hypothetical terms when, in actuality, the risk had already materialized. Specifically, Unisys network user accounts were compromised between January 2020 and August 2021 by a hacking group associated with the Russian government.

29. The 2021 Annual Report contained the following risk disclosure:

A significant disruption in the company's IT systems could adversely affect the company's business and reputation.

The company relies extensively on its IT systems to conduct its business and perform services for its clients. ***The company's systems are subject to damage or interruption from*** power outages, telecommunications failures, ***computer viruses and malicious attacks***, ***cybersecurity breaches*** and catastrophic events. If the company's systems are accessed without its authorization, ***damaged or fail to function properly, the company could incur substantial repair or replacement costs, experience data loss and impediments to its ability to conduct its business, and damage the market's perception of the company's services and products. In addition, a disruption could result in the company failing to meet performance standards and obligations in its client contracts***, which could subject the company to liability, penalties and contract termination. This may adversely affect the company's reputation and financial results.

(Emphasis added).

30. The statement in ¶ 29 was materially false and misleading at the time it was made because the Company spoke of material cybersecurity breaches in hypothetical terms when, in actuality, the risk had already materialized. Specifically, Unisys network user accounts were compromised between January 2020 and August 2021 by a hacking group associated with the Russian government.

31. On November 23, 2022, Unisys filed with the SEC its amended annual report on Form 10-K/A for the year ending December 31, 2021 (the "Amended 2021 Annual Report"). Attached to the Amended 2021 Annual Report were certifications pursuant to SOX signed by Defendants Altabef and McCann attesting to the accuracy of financial reporting, the disclosure of any material changes to the Company's internal control over financial reporting and the disclosure of all fraud.

32. The Amended 2021 Annual Report contained the following statement:

> **Disclosure Controls and Procedures (as restated)**
>
> As of the end of the period covered by this Annual Report, management performed, with the participation of the Chief Executive Officer (CEO) and the Chief Financial Officer (CFO), an evaluation of the effectiveness of the company's disclosure controls and procedures as defined in Rules 13a-15(e) and 15d-15(e) of the Securities Exchange Act of 1934 (the Exchange Act). At the time the company filed the original filing, the CEO and the CFO concluded that the company's disclosure controls and procedures were effective as of December 31, 2021.
>
> The company has reevaluated the effectiveness of the company's disclosure controls and procedures and identified material weaknesses in the company's disclosure controls and procedures and internal control over financial reporting. A material weakness is a deficiency, or a combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of a company's annual or interim financial statements will not be prevented or detected on a timely basis.
>
> Specifically, subsequent to the original filing, the CEO and CFO concluded that our disclosure controls and procedures were not effective as of December 31, 2021 ***as the company did not design and maintain effective formal policies and procedures over information being communicated by the IT function and the legal and compliance***

> ***function to those responsible for governance, including the CEO and CFO, to allow timely decisions related to both financial reporting, as further discussed in Management's Report on Internal Control Over Financial Reporting under Item 8, and other non-financial reporting in the reports that the company files or submits under the Exchange Act.***
>
> Notwithstanding the material weaknesses, the CEO and CFO have concluded that the company's consolidated financial statements included in the Annual Report were fairly stated in all material respects in accordance with generally accepted accounting principles in the United States of America for each of the periods presented.
>
> (Emphasis added).

33. The statement in ¶ 32 was materially false and misleading at the time it was made because while the Company did disclose that it had a material weakness in its internal controls, it omitted that this weakness had resulted in material cybersecurity breaches going unreported to senior management. In turn, those breaches went unreported to the Company's investors.

34. The Amended 2021 Annual Report contained the following risk disclosure relating to cybersecurity:

> ***Cybersecurity incidents could result in the company incurring significant costs and could harm the company's business and reputation.***
>
> The company's business includes managing, processing, storing and transmitting proprietary and confidential data, including personal information, intellectual property and proprietary business information, within the company's own IT systems and those that the company designs, develops, hosts or manages for clients. These systems are critical to the company's business activities, and shutdowns or disruptions of, and cybersecurity attacks on, these systems pose increasing risks. ***Cybersecurity incidents and network security incidents may include***, but are not limited to, attempts to access or unauthorized access of information, exploitation of vulnerabilities (including those of third-party software or systems), computer viruses, ransomware, denial of service and other electronic security incidents. Attacks also include social engineering and cyber extortion to induce customers, contractors, business partners, vendors, employees and other third parties to disclose information, transfer funds, or unwittingly provide access to systems or data. Cyberattacks from computer hackers and cyber criminals and other malicious internet-based activity continue to increase generally, and the company's services and systems, including the systems of the company's outsourced service providers, ***have been and may in the future continue to be*** the target of various forms of cybersecurity incidents such as DNS attacks, wireless network attacks, viruses and worms, malicious software, ransomware, cyber extortion, misconfigurations, supply chain attacks, application centric attacks, peer-to-peer

attacks, phishing attempts, backdoor trojans and distributed denial of service attacks.

The techniques used by computer hackers and cyber criminals to obtain unauthorized access to data or to sabotage computer systems change frequently and are growing in sophistication, and these new techniques generally are not detected until after an incident has occurred. Cybersecurity incidents involving the company's systems, despite established security controls, ***could result*** in disruption of the company's services, misappropriation, misuse, alteration, theft, loss, corruption, leakage, falsification, and accidental or premature release or improper disclosure or misuse of confidential or other information, including intellectual property and personal information (of the company, third parties, employees, clients or others). ***The company could be exposed to liability, litigation, and regulatory or other government action, as well as the loss of existing or potential customers, damage to the company's brand and reputation, damage to the company's competitive position, and other financial loss, any of which could have a material adverse effect on the company's business, financial condition and results of operations***. In addition, the cost and operational consequences of responding to cybersecurity incidents and implementing remediation measures could be significant. In the company's industry, security vulnerabilities are increasingly discovered, publicized and exploited across a broad range of hardware, software or other infrastructure, elevating the risk of attacks and the potential cost of response and remediation for the company.

Although the company continuously takes significant steps to mitigate cybersecurity risk across a range of functions, such measures can never eliminate the risk entirely or provide absolute security, and the company has experienced and expects to continue to experience cyberattacks on its information systems. ***While there have not been cybersecurity incidents or vulnerabilities that have had a material adverse effect on the company,*** there is no assurance that there will not be cybersecurity incidents or vulnerabilities that will have a material adverse effect in the future.

(Emphasis added).

35. The statement in ¶ 34 was materially false and misleading at the time it was made because the Company spoke of material cybersecurity breaches in hypothetical terms when, in actuality, the risk of a material hack had already taken place in 2021. In particular, Unisys network user accounts were compromised between January 2020 and August 2021 by a hacking group associated with the Russian government.

36. On March 1, 2023, Unisys filed with the SEC its annual report on Form 10-K for the year ending December 31, 2022 (the "2022 Annual Report"). Attached to the 2022 Annual Report were certifications pursuant to SOX signed by Defendants Altabef and McCann attesting

to the accuracy of financial reporting, the disclosure of any material changes to the Company's internal control over financial reporting and the disclosure of all fraud.

37. The 2022 Annual Report contained the following statement:

> As of the end of the period covered by this Annual Report, management performed, with the participation of the Chief Executive Officer (CEO) and the Chief Financial Officer (CFO), an evaluation of the effectiveness of the company's disclosure controls and procedures as defined in Rules 13a-15(e) and 15d-15(e) of the Securities Exchange Act of 1934 (the Exchange Act). In designing and evaluating the disclosure controls and procedures, management recognized that any controls and procedures, no matter how well designed and operated, can provide only reasonable assurance of achieving the desired control objectives***. Based upon that evaluation, the CEO and the CFO concluded that due to material weaknesses in our disclosure controls and procedures and in our internal control over financial reporting, the company's disclosure controls and procedures were not effective as of December 31, 2022 at the reasonable assurance level***. A material weakness is a deficiency, or a combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of a company's annual or interim financial statements will not be prevented or detected on a timely basis.
>
> The company did not design and maintain effective formal policies and procedures over information being communicated by the IT function and the legal and compliance function to those responsible for governance, including the CEO and CFO, to allow timely decisions related to both financial reporting as further discussed in Management's Report on Internal Control Over Financial Reporting under Item 8 of this Annual Report on Form 10-K, and other non-financial reporting in the reports that the company files or submits under the Exchange Act.
>
> To address the material weaknesses referenced above, the company performed additional analysis and performed other procedures in order to prepare the audited consolidated financial statements in accordance with generally accepted accounting principles (GAAP). Accordingly, management believes that the consolidated financial statements included in this Annual Report on Form 10-K fairly present, in all material respects, our financial condition, results of operations and cash flows for the periods presented.
>
> (Emphasis added).

38. The statement in ¶ 37 was materially false and misleading at the time it was made because while the Company did disclose that it had a material weakness in its internal controls, it omitted that this weakness resulted in cybersecurity breaches going unreported to senior management in 2020 and 2021, and in turn, those breaches were not reported to investors. Further,

in 2022, after another hack, the Company discovered that its "endpoint detection and response system was not set up properly to automatically send alerts to its centralized Security Information and Event Management system, which Unisys's policies and procedures required to be monitored regularly by cybersecurity personnel."

39. The 2022 Annual Report contained the following risk disclosure relating to cybersecurity:

> ***Cybersecurity incidents have occurred and may continue to occur and could result in the incurrence of significant costs and harm to our business and reputation.***
>
> Our business includes managing, processing, storing and transmitting proprietary and confidential data, including personal information, intellectual property and proprietary business information, within our own IT systems and those that we design, develop, host or manage for clients. These systems are critical to our business activities, and unauthorized access to or disruptions of, and cybersecurity attacks on, these systems pose increasing risks. Like other companies, we have experienced cybersecurity attacks and have had to expend increasing human and financial resources to respond. Cyberattacks from computer hackers and cyber criminals and other malicious internet-based activity continue to increase generally, and our services and systems, including the systems of our outsourced service providers, have been and may in the future continue to be the target of various forms of cybersecurity incidents such as DNS attacks, wireless network attacks, viruses and worms, malicious software, ransomware, cyber extortion, misconfigurations, supply chain attacks, application centric attacks, peer-to-peer attacks, phishing attempts, backdoor trojans and distributed denial of service attacks, among other cybersecurity threats. Attacks also may include social engineering and cyber extortion to induce customers, contractors, business partners, vendors, employees and other third parties to disclose information, transfer funds, or unwittingly provide access to systems or data. As a known provider of IT solutions, we pose an attractive target for such attacks.
>
> The techniques used by computer hackers and cyber criminals to obtain unauthorized access to data or to sabotage computer systems change frequently and are growing in sophistication, and these new techniques may not be detected until after an incident has occurred. Despite established security controls, cybersecurity incidents involving our systems could result in disruption of our services, misappropriation, misuse, alteration, theft, loss, corruption, leakage, falsification, and accidental or premature release or improper disclosure or misuse of confidential or other information, including intellectual property, personal information, and other confidential information (of the company, third parties, employees, clients or others). ***We could be exposed to liability, litigation, and regulatory or other government action, as well as the loss of existing or potential customers, damage to our brand and reputation, damage to our competitive position, and other financial loss, any of which could have a material adverse effect on our business,***

> ***financial condition and results of operations***. In addition, the cost and operational consequences of responding to cybersecurity incidents and implementing remediation measures could be significant. In our industry, security vulnerabilities are increasingly discovered, publicized and exploited across a broad range of hardware, software or other infrastructure, elevating the risk of attacks and the potential cost of response and remediation for us.
>
> Although we continuously take significant steps to mitigate cybersecurity risk across a range of functions, such measures can never eliminate the risk entirely or provide absolute security, and we have experienced and expect to continue to experience cyberattacks on our information systems.
>
> (Emphasis added).

40. The statement in ¶ 39 was materially false and misleading at the time it was made because it omitted that a Russian-speaking ransomware organization had successfully hacked into Unisys's internal system in July 2022, that Unisys then mishandled the internal investigation into that hack, and then that "Unisys discovered that its endpoint detection and response system was not set up properly to automatically send alerts to its centralized Security Information and Event Management system, which Unisys's policies and procedures required to be monitored regularly by cybersecurity personnel."

41. The statements contained in ¶¶ 18, 20, 22, 25, 27, 29, 32, 34, 37, and 39 were materially false and/or misleading because they misrepresented and failed to disclose the following adverse facts pertaining to the Company's business, operations, and prospects, which were known to Defendants or recklessly disregarded by them. Specifically, Defendants made false and/or misleading statements and/or failed to disclose that: (1) Unisys had inadequate internal controls due to the lack of a system for reporting cybersecurity incidents to management; (2) as a result, Unisys did not disclose to its investors that it had been hacked multiple times, including by hackers with links to the Russian government; and (3) as a result, Defendants' statements about its business, operations, and prospects, were materially false and misleading and/or lacked a

reasonable basis at all times.

THE TRUTH BEGINS TO EMERGE

42. On October 22, 2024, the Securities and Exchange Commission posted an announcement on its website entitled "SEC Charges Four Companies With Misleading Cyber Disclosures", and also announced that Unisys had been charged with controls violations. The release further stated:

> The Securities and Exchange Commission today charged four current and former public companies – Unisys Corp., Avaya Holdings Corp., Check Point Software Technologies Ltd, and Mimecast Limited – with making materially misleading disclosures regarding cybersecurity risks and intrusions. The SEC also charged Unisys with disclosure controls and procedures violations. The companies agreed to pay the following civil penalties to settle the SEC's charges:
>
> - Unisys will pay a $4 million civil penalty[.]
>
> * * *
>
> The charges against the four companies result from an investigation involving public companies potentially impacted by the compromise of SolarWinds' Orion software and by other related activity.

43. Further, the announcement quoted Sanjay Wadhwa, Acting Director of the SEC's Division of Enforcement, as saying the following:

> As today's enforcement actions reflect, while public companies may become targets of cyberattacks, it is incumbent upon them to not further victimize their shareholders or other members of the investing public by providing misleading disclosures about the cybersecurity incidents they have encountered[.] Here, the SEC's orders find that these companies provided misleading disclosures about the incidents at issue, leaving investors in the dark about the true scope of the incidents.

44. On the same day, during market hours, the SEC issued an order instituting cease-and-desist proceedings, pursuant to Section 8A of the Securities Act of 1933 and Section 21C of the Securities Exchange Act of 1934, making findings, and imposing a cease-and-desist order (the "Order").

45. The Order stated the following about Unisys' business activities at the time of the misconduct outlined in this action:

> During the relevant time period, Unisys was a provider of technical and enterprise IT services and solutions to large commercial enterprises and public sector entities, including global non-profit organizations, foreign, state, and local governments, and, for a period, the U.S. government. It offered products and services for digital workplace solutions, cloud, applications and infrastructure solutions, and enterprise computing solutions.

46. The Order further stated the importance of Unisys's ability to protect information and data:

> As a provider of technical and enterprise IT services and solutions to large commercial enterprises and public sector entities, including global non-profit organizations; foreign, state, and local governments; and, for a period, the U.S. government, Unisys's ability to protect information and data stored on and transmitted over its network was critically important to its reputation and ability to attract and retain customers and to investors. Moreover, Unisys's information and data were of great interest to state-sponsored cyber threat actors, such as the threat actor likely behind the SolarWinds Compromise.

47. The Order gave the following background information regarding cybersecurity threats against Unisys:

> ***In December 2020***, Unisys identified one computer in its network that had a version of SolarWinds Orion software, which a likely nation-state threat actor infected with malicious code that could have allowed for unauthorized activity on affected computers and their networks ("SolarWinds Compromise"). Unisys also received notifications about and discovered compromises of its environment likely by the same threat actor. ***The compromises of Unisys's systems took place over a combined span of at least sixteen months starting in January 2020 and were persistent and impacted several parts of its corporate network and non-customer facing cloud environment***. Specifically, the activity involved the compromise of at least seven network credential[s] and 34 cloud-based accounts, including those with administrative privileges, repeated connections into Unisys's network with at least 33 gigabytes ("GB") of data transferred, and access to cloud-based shared files and mailboxes, including those of senior IT personnel. ***Unisys was aware that its investigations of the compromise involved significant gaps in its ability to identify the full scope of the unauthorized activity due to the lack of availability of the forensic evidence***.
>
> (Emphasis added).

48. The Order further revealed the following about the Company's investigation into the hacks, including that it turned down the recommendations of an outside service provider:

> In December 2020, Unisys identified an infected version of the SolarWinds software on at least one computer in its network. In a subsequent investigation, it learned that the infected software was loaded on seven dates (but found no evidence that the malicious implant was exploited by the SolarWinds threat actor) and that two other computers made one internet connection each to a known malicious command-and-control server via an internet browser (rather than an installation of the SolarWinds software). ***At the time of Unisys's investigation, its logs and forensic evidence of possible compromise were insufficient to rule out unauthorized activity for some of the installations***. The company retained ***a third-party service provider to review the available forensic evidence as well as additional forensic evidence the service provider maintained with respect to the Unisys network***. The service provider did not identify evidence of exploitation or other additional activity involving the SolarWinds software or through the internet connections on the two computers, ***but recommended that the company conduct a forensic review of the three computers with evidence of potentially unauthorized activity. Unisys determined that the level and nature of known activity on these computers did not necessitate such additional investigation***.
>
> (Emphasis added).

49. The Order stated that the hack likely stemmed from Russia, stating the following:

> Throughout December 2020, Unisys learned that the threat actor behind the compromise of the SolarWinds Orion software was a hacking group likely associated with a nation-state. ***Public reports and commercial cybersecurity intelligence sources widely attributed the activity to the Russian Federation in late December 2020. On January 5, 2021, a joint public statement by the Federal Bureau of Investigation, the Office of the Director of National Intelligence, the National Security Agency, and the Cybersecurity and Infrastructure Security Agency attributed the attack to an intelligence gathering operation "likely Russian in origin."*** The event impacted thousands of SolarWinds' customers.
>
> (Emphasis added).

50. The Order further stated the following:

> On December 13, 2020, Unisys's then-senior cybersecurity personnel received credible information that likely the same threat actor had compromised Unisys's network and non-customer facing cloud environment using means other than SolarWinds software beginning in February 2020. ***The company's subsequent investigation uncovered evidence that the threat actor engaged in the following activities between January 2020 and February 2021: compromised at least three Unisys network user accounts and gained access to eight Unisys cloud-based user accounts, including accounts with global***

administrative privileges and the internal Unisys accounts of employees who serviced certain of the company's customers; repeatedly initiated and completed Virtual Private Network ("VPN") connections during ***which approximately 23GB of data was transferred to and approximately seven gigabytes was transferred from the company's network***; ***and accessed the contents of at least five cloud-based mailboxes, including high-level IT personnel and a Chief Information Officer for the company's then federal government business. Unisys took various remedial measures after investigating the activity***.

(Emphasis added).

51. The Report revealed the following about what the Company discovered in August 2021:

In August 2021, Unisys received credible information that the same threat actor accessed the company's VPN and non-customer facing cloud environment again between April and August 2021. The company's investigation identified evidence of additional persistent unauthorized activity, compromise of least four network user accounts and 28 cloud-based accounts, access to 14 systems, repeated VPN sessions, and access to approximately 27,000 email messages and 130 cloud-based shared files.

(Emphasis added).

52. The findings of the August 2021 investigation were not reported to senior management. The Order stated the following:

Unisys's policies did not include adequate escalation procedures in the event of a cybersecurity incident, and Unisys cybersecurity personnel did not report this activity to senior management. Unisys also failed to review the contents of the messages and shared files until 2022, by which point only half of these documents remained available. Between April and August 2021, the threat actor exploited information obtained in 2020 about the Unisys network and at least one persistence mechanism the threat actor established in 2020, an authorization certificate for facilitating authorization for cloud-based applications, which the company failed to identify during its review of the 2020 activity.

(Emphasis added).

53. The Order stated the following about the Company's controls:

Unisys's materially misleading statements resulted in part from the company's failure to design controls and procedures to ensure (1) that information about potentially material cybersecurity incidents was timely recorded, processed, summarized and reported, within the time period specified as appropriate in the Commission's rules and forms, and (2) that

> information was accumulated and communicated to the company's management to allow timely decisions regarding required disclosures. As a result, decision makers failed at the time to reasonably assess the materiality of these events and new risks arising thereform.

54. The Order noted that, separately from the events described above relating to the SolarWinds attack, in July 2022, a "separate threat actor—a Russian-speaking ransomware group—successfully compromised Unisys's network and [exfiltrated] certain cybersecurity and product and platform code for products the company offers to its customers." (the "July 2022 Cybersecurity Event").

55. The Order gave the following further detail about the July 2022 Cybersecurity Event:

> Between July 7 and 12, 2022, Unisys's internal cybersecurity systems issued at least 10 alerts about the presence and execution of powerful password-stealing malware, Mimikatz, on seven computers in its non-customer facing software development network. Unisys's cybersecurity personnel were not sufficiently familiar with the format of the alerts and erroneously believed that the malware was deployed on only one machine and only on July 7, 2022. ***The company's cybersecurity personnel also assigned a low priority to the activity because one of the alerts stated that the malware was quarantined. As a result, no cybersecurity personnel took steps to investigate the activity until July 13, almost a week after the initial alert.***
>
> Unisys's cybersecurity personnel determined on July 14, 2022 that the malware was not in fact quarantined, and it conducted additional investigation and identified an active intrusion by another threat actor, a Russian-speaking ransomware group. The next day, Unisys took the compromised lab network off the internet. ***However, during the eight days between the initial alerts and Unisys's disconnection of the network, the threat actor exfiltrated certain cybersecurity and product and platform software code for products the company offers to its customers. Unisys notified criminal law enforcement as part of its incident response.***
>
> By July 22, 2022, Unisys identified evidence of this code exfiltration and in fact found a copy of the code on a threat actor-controlled server on the internet. Unisys cybersecurity personnel initially believed that they were able to remove the code from the threat actor-controlled server. However, on July 25 and 30, 2022, the threat actor provided evidence to Unisys that it still had a copy of the code. In addition, on August 3, 2022, in an effort to pressure Unisys into paying a ransom, the threat actor briefly posted on its darkweb site a message alleging that it had exfiltrated all of Unisys's code. The post was up for less than one hour and did not receive media coverage.

(Emphasis added).

56. The Order stated the following about what Unisys discovered about its own reporting systems during the July 2022 Cybersecurity Event:

> In the course of the incident, ***Unisys discovered that its endpoint detection and response system was not set up properly to automatically send alerts to its centralized Security Information and Event Management system***, ***which Unisys's policies and procedures required to be monitored regularly by cybersecurity personnel***. Unisys was unable to determine how long the misconfiguration persisted and how many alerts were not reviewed by cybersecurity personnel as a result.
>
> (Emphasis added).

57. Despite these issues, the Order notes that "[b]efore ***December 2022, Unisys's incident response policies did not reasonably require cybersecurity personnel to report information to Unisys's disclosure decision makers and contained no criteria for determining which incidents or information should be reported outside the information security organization***." (Emphasis added). As a result, "Unisys's senior cybersecurity personnel repeatedly failed to report the above incidents to executive management and the legal department in a timely manner."

58. The Order stated the following about how the Company's cybersecurity risk profile changed as a result of the aforementioned cybersecurity events:

> Unisys's cybersecurity risk profile changed materially as a result of the SolarWinds Compromise-related activity for the following reasons: (1) a persistent and reportedly nation-state-supported threat actor compromised the company's environment; (2) ***the threat actor persisted in the environment unmonitored for a combined span of at least sixteen months***; and (3) the company's investigation of the activity suffered from gaps that prevented it from identifying the full scope of the compromise.
>
> (Emphasis added).

59. After Unisys discovered these events, the Order stated that it did the following:

> ***Unisys filed with the Commission annual reports on Form 10-K for fiscal years ended December 31, 2020 and 2021 that included cybersecurity risk disclosures that were***

> ***materially misleading and not sufficiently tailored to its particular risks and incidents***. In these disclosures, Unisys inaccurately described the existence of successful intrusions and the risk of unauthorized access to data and information in hypothetical terms, despite knowing that the above-described intrusions had actually happened and in fact involved unauthorized access and exfiltration of confidential and/or proprietary information.
>
> (Emphasis added).

60. The Order stated the following about Unisys's failure to maintain disclosure controls and procedures:

> Unisys's cybersecurity personnel failed to report the 2020 and 2021 activity to disclosure decision-makers until a year after discovering it, and the 2022 extortion incident until the hackers' public statement. At the time of these events, Unisys did not maintain effective controls requiring escalation of potentially material incidents to senior management and disclosure decision-makers. At the same time, Unisys did not have controls and procedures designed to ensure that its disclosure decision-makers reviewed cybersecurity incident information in Unisys's possession in order to determine which information about the incident may be required to be disclosed in Commission filings. Accordingly, despite the importance of data integrity and confidentiality to Unisys, the company failed to maintain disclosure controls and procedures designed to ensure that information around material cybersecurity incidents was, among other things, reported to management responsible for disclosures and therefore timely reported to investors. Specifically, Unisys's deficient controls contributed to Unisys's materially misleading risk factor disclosures for the years ending 2020 and 2021.

61. On this news, Unisys's stock fell $0.59, or 8.6%, to close at $6.25 on October 22, 2024. The next day, it fell a further $0.58, or 9.28%, to close at $5.67 on October 23, 2024.

62. As a result of Defendants' wrongful acts and omissions, and the precipitous decline in the market value of the Company's common shares, Plaintiff and the other Class members have suffered significant losses and damages.

PLAINTIFF'S CLASS ACTION ALLEGATIONS

63. Plaintiff brings this action as a class action pursuant to Federal Rule of Civil Procedure 23(a) and (b)(3) on behalf of a class consisting of all persons other than defendants who acquired Unisys securities publicly traded on the NYSE during the Class Period, and who were damaged thereby (the "Class"). Excluded from the Class are Defendants, the officers and

directors of the Company, members of the Individual Defendants' immediate families and their legal representatives, heirs, successors or assigns and any entity in which Defendants have or had a controlling interest.

64. The members of the Class are so numerous that joinder of all members is impracticable. Throughout the Class Period, the Company's securities were actively traded on the NYSE. While the exact number of Class members is unknown to Plaintiff at this time and can be ascertained only through appropriate discovery, Plaintiff believes that there are hundreds, if not thousands of members in the proposed Class.

65. Plaintiff's claims are typical of the claims of the members of the Class as all members of the Class are similarly affected by Defendants' wrongful conduct in violation of federal law that is complained of herein.

66. Plaintiff will fairly and adequately protect the interests of the members of the Class and has retained counsel competent and experienced in class and securities litigation. Plaintiff has no interests antagonistic to or in conflict with those of the Class.

67. Common questions of law and fact exist as to all members of the Class and predominate over any questions solely affecting individual members of the Class. Among the questions of law and fact common to the Class are:

- whether the Exchange Act was violated by Defendants' acts as alleged herein;
- whether statements made by Defendants to the investing public during the Class Period misrepresented material facts about the business and financial condition of the Company;

- whether Defendants' public statements to the investing public during the Class Period omitted material facts necessary to make the statements made, in light of the circumstances under which they were made, not misleading;
- whether the Defendants caused the Company to issue false and misleading filings during the Class Period;
- whether Defendants acted knowingly or recklessly in issuing false filings;
- whether the prices of the Company's securities during the Class Period were artificially inflated because of the Defendants' conduct complained of herein; and
- whether the members of the Class have sustained damages and, if so, what is the proper measure of damages.

68. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. Furthermore, as the damages suffered by individual Class members may be relatively small, the expense and burden of individual litigation make it impossible for members of the Class to individually redress the wrongs done to them. There will be no difficulty in the management of this action as a class action.

69. Plaintiff will rely, in part, upon the presumption of reliance established by the fraud-on-the-market doctrine in that:

- the Company's securities met the requirements for listing, and were listed and actively traded on the NYSE, an efficient market;
- as a public issuer, the Company filed public reports;
- the Company communicated with public investors via established market communication mechanisms, including through the regular dissemination of press

releases via major newswire services and through other wide-ranging public disclosures, such as communications with the financial press and other similar reporting services;

- the Company's securities were liquid and traded with moderate to heavy volume during the Class Period; and
- the Company was followed by a number of securities analysts employed by major brokerage firms who wrote reports that were widely distributed and publicly available.

70. Based on the foregoing, the market for the Company securities promptly digested current information regarding the Company from all publicly available sources and reflected such information in the prices of the common units, and Plaintiff and the members of the Class are entitled to a presumption of reliance upon the integrity of the market.

71. Alternatively, Plaintiff and the members of the Class are entitled to the presumption of reliance established by the Supreme Court in *Affiliated Ute Citizens of the State of Utah v. United States*, 406 U.S. 128 (1972), as Defendants omitted material information in their Class Period statements in violation of a duty to disclose such information as detailed above.

COUNT I
For Violations of Section 10(b) And Rule 10b-5 Promulgated Thereunder
Against All Defendants

72. Plaintiff repeats and realleges each and every allegation contained above as if fully set forth herein.

73. This Count asserted against Defendants is based upon Section 10(b) of the Exchange Act, 15 U.S.C. § 78j(b), and Rule 10b-5 promulgated thereunder by the SEC.

74. During the Class Period, Defendants, individually and in concert, directly or indirectly, disseminated or approved the false statements specified above, which they knew or deliberately disregarded were misleading in that they contained misrepresentations and failed to disclose material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading.

75. Defendants violated §10(b) of the 1934 Act and Rule 10b-5 in that they:

- employed devices, schemes and artifices to defraud;
- made untrue statements of material facts or omitted to state material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; or
- engaged in acts, practices and a course of business that operated as a fraud or deceit upon plaintiff and others similarly situated in connection with their purchases of the Company's securities during the Class Period.

76. Defendants acted with scienter in that they knew that the public documents and statements issued or disseminated in the name of the Company were materially false and misleading; knew that such statements or documents would be issued or disseminated to the investing public; and knowingly and substantially participated, or acquiesced in the issuance or dissemination of such statements or documents as primary violations of the securities laws. These defendants by virtue of their receipt of information reflecting the true facts of the Company, their control over, and/or receipt and/or modification of the Company's allegedly materially misleading statements, and/or their associations with the Company which made them privy to confidential proprietary information concerning the Company, participated in the fraudulent scheme alleged herein.

77. Individual Defendants, who are or were senior executives and/or directors of the Company, had actual knowledge of the material omissions and/or the falsity of the material statements set forth above, and intended to deceive Plaintiff and the other members of the Class, or, in the alternative, acted with reckless disregard for the truth when they failed to ascertain and disclose the true facts in the statements made by them or other Company's personnel to members of the investing public, including Plaintiff and the Class.

78. As a result of the foregoing, the market price of the Company's securities was artificially inflated during the Class Period. In ignorance of the falsity of Defendants' statements, Plaintiff and the other members of the Class relied on the statements described above and/or the integrity of the market price of the Company's securities during the Class Period in purchasing the Company's securities at prices that were artificially inflated as a result of Defendants' false and misleading statements.

79. Had Plaintiff and the other members of the Class been aware that the market price of the Company's securities had been artificially and falsely inflated by Defendants' misleading statements and by the material adverse information which Defendants did not disclose, they would not have purchased the Company's securities at the artificially inflated prices that they did, or at all.

80. As a result of the wrongful conduct alleged herein, Plaintiff and other members of the Class have suffered damages in an amount to be established at trial.

81. By reason of the foregoing, Defendants have violated Section 10(b) of the 1934 Act and Rule 10b-5 promulgated thereunder and are liable to the plaintiff and the other members of the Class for substantial damages which they suffered in connection with their purchase of the Company's securities during the Class Period.

COUNT II
Violations of Section 20(a) of the Exchange Act
Against the Individual Defendants

82. Plaintiff repeats and realleges each and every allegation contained in the foregoing paragraphs as if fully set forth herein.

83. During the Class Period, the Individual Defendants participated in the operation and management of the Company, and conducted and participated, directly and indirectly, in the conduct of the Company's business affairs. Because of their senior positions, they knew the adverse non-public information about the Company's business practices.

84. As officers of a public business, the Individual Defendants had a duty to disseminate accurate and truthful information with respect to the Company's financial condition and results of operations, and to correct promptly any public statements issued by the Company which had become materially false or misleading.

85. Because of their positions of control and authority as senior executives and/or directors, the Individual Defendants were able to, and did, control the contents of the various reports, press releases and public filings which the Company disseminated in the marketplace during the Class Period concerning the Company's results of operations. Throughout the Class Period, the Individual Defendants exercised their power and authority to cause the Company to engage in the wrongful acts complained of herein. The Individual Defendants therefore, were "controlling persons" of the Company within the meaning of Section 20(a) of the Exchange Act. In this capacity, they participated in the unlawful conduct alleged which artificially inflated the market price of Company securities.

86. By reason of the above conduct, the Individual Defendants are liable pursuant to Section 20(a) of the Exchange Act for the violations committed by the Company.

PRAYER FOR RELIEF

WHEREFORE, plaintiff, on behalf of himself and the Class, prays for judgment and relief as follows:

(a) declaring this action to be a proper class action, designating plaintiff as Lead Plaintiff and certifying plaintiff as a class representative under Rule 23 of the Federal Rules of Civil Procedure and designating plaintiff's counsel as Lead Counsel;

(b) awarding damages in favor of plaintiff and the other Class members against all defendants, jointly and severally, together with interest thereon;

(c) awarding plaintiff and the Class reasonable costs and expenses incurred in this action, including counsel fees and expert fees; and

(d) awarding plaintiff and other members of the Class such other and further relief as the Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury.

Dated: **THE ROSEN LAW FIRM, P.A.**

Jacob A. Goldberg
101 Greenwood Avenue, Suite 440
Jenkintown, PA 19046
Telephone: (215) 600-2817
Fax: (212) 202-3827
Email: jgoldberg@rosenlegal.com

Phillip Kim, Esq.
275 Madison Avenue, 40th Floor
New York, New York 10016
Telephone: (212) 686-1060
Fax: (212) 202-3827
Email: philkim@rosenlegal.com

Counsel for Plaintiff