LATHAM & WATKINS LLP
Michael H. Rubin (SBN 214636)
michael.rubin@lw.com
505 Montgomery Street, Suite 2000
San Francisco, CA 94111-6538
Phone: (415) 391-0600
Fax: (415) 395-8095

Mary Rose Alexander (SBN 143899)
mary.rose.alexander@lw.com
330 North Wabash Avenue, Suite 2800
Chicago, IL 60611
Phone: (312) 876-7700
Fax: (312) 993-9767

Attorneys for Plaintiffs The Clorox Company and Clorox Services Company

SUPERIOR COURT OF CALIFORNIA

COUNTY OF ALAMEDA

THE CLOROX COMPANY and CLOROX SERVICES COMPANY, Plaintiffs, *v.* COGNIZANT WORLDWIDE LIMITED and COGNIZANT TECHNOLOGY SOLUTIONS U.S. CORPORATION, Defendants.	Case No. COMPLAINT FOR: 1. BREACH OF CONTRACT 2. BREACH OF THE COVENANT OF GOOD FAITH AND FAIR DEALING 3. GROSS NEGLIGENCE 4. INTENTIONAL MISREPRESENTATION JURY TRIAL DEMANDED **Public-Redacts Materials from Conditionally Sealed Record**

Plaintiffs The Clorox Company and Clorox Services Company ("Clorox") bring this suit against Defendants Cognizant Worldwide Limited ("Cognizant Worldwide") and Cognizant Technology Solutions U.S. Corporation ("Cognizant U.S.") (collectively, "Cognizant").

INTRODUCTION

1. For over a decade, Clorox entrusted Cognizant, a self-proclaimed leader in digital and cybersecurity services, to play critical roles in Clorox's cyber environment. One such task was as critical as it was fundamental: Cognizant helped guard the proverbial front door.

2. Cognizant provided the service desk ("Service Desk") that Clorox employees could contact when they needed password recovery or reset assistance. Cognizant's operation of the Service Desk came with a simple, common-sense requirement: never reset anyone's credentials without properly authenticating them first. Clorox made this easy for Cognizant by providing them with straight-forward procedures to follow *whenever* providing credential recovery or reset assistance.

3. Despite assuring Clorox that it was following these procedures, Cognizant's conduct on August 11, 2023, demonstrated spectacularly that it was failing to do so. Cognizant repeatedly gave a cybercriminal access to Clorox's network by handing them credentials without properly authenticating them or otherwise following Clorox's process.

4. Cognizant's failures resulted in a catastrophic cyberattack on Clorox ("Cyberattack").

5. Cognizant was not duped by any elaborate ploy or sophisticated hacking techniques. The cybercriminal just called the Cognizant Service Desk, asked for credentials to access Clorox's network, and Cognizant *handed the credentials right over*. Cognizant is *on tape* handing over the keys to Clorox's corporate network to the cybercriminal—no authentication questions asked:

Cybercriminal: *I don't have a password, so I can't connect.*

Cognizant Agent: *Oh, ok. Ok. So let me provide the password to you ok?*

Cybercriminal: *Alright. Yep. Yeah, what's the password?*

Cognizant Agent: *Just a minute. So it starts with the word "Welcome…"*

6. The cybercriminal then used those credentials, and others obtained that same day through similar calls to the Service Desk, to attack Clorox.

7. The resulting Cyberattack was debilitating. It paralyzed Clorox's corporate network and crippled business operations. And to make matters worse, when Clorox called on Cognizant to provide incident response and disaster recovery support services, Cognizant botched its response and compounded the damage it had already caused.

8. The root cause of the Cyberattack was Cognizant's blatant disregard for Clorox's credential support policies and procedures, industry standards, and the terms of the parties' Information Technology Services Agreement ("ITSA"). Clorox's policies were designed to protect against the very attack Cognizant facilitated. Inexplicably, Cognizant staff repeatedly ignored these policies on the calls with the cybercriminal, flinging open the otherwise secure gate to the Clorox network.

9. As a digital and cybersecurity services provider, Cognizant knows that the stakes are high at the Service Desk. In fact, Cognizant itself recognizes that "[e]very day, cyber and social engineering threats are actively targeting all aspects of the digital workplace…"[1]

10. The quality and training of Service Desk staff are crucial for ensuring the security of service desk operations, and Cognizant repeatedly represented to Clorox prior to the Cyberattack that it had properly trained its staff on Clorox's policies and procedures.

11. The Cyberattack exposed the fact that this was all a devastating lie. If Cognizant had properly trained its Service Desk staff on Clorox's policies and procedures or basic industry standards, the Cyberattack never would have happened.

12. Cognizant purportedly upholds a Code of Ethics to "maintain [its] culture of ethics and compliance," promising that it would "respect and protect the confidential and personal information [it] hold[s] on behalf of [its] clients, [its] associates, and third parties."[2]

---

[1] *Secure Workplace*, COGNIZANT, https://www.cognizant.com/en_us/services/documents/cognizant-mbg-secure-workplace-brochure-2023.pdf (last visited July 21, 2025).

[2] *Code of Ethics*, COGNIZANT, https://www.cognizant.com/en_us/about/documents/code-of-ethics.pdf (last visited July 21, 2025).

13. Quite the contrary, Cognizant's conduct in causing the Cyberattack starkly demonstrated its egregious lack of care for Clorox's confidential information.

14. The Cyberattack caused Clorox approximately $380 million in damages, including over $49 million in remedial costs alone to fix the damage caused by Cognizant's entirely preventable errors, and hundreds of millions of dollars in business interruption losses because the Cyberattack impeded Clorox's ability to ship orders and keep its products on the shelves of retailers. And as Cognizant acknowledges, "[t]he wreckage of a cyber attack extends beyond the immediate capital losses and financial consequences to brand credibility, with damages persisting over several years."[3]

15. Meanwhile, Cognizant "exited the year with momentum," reporting $20 billion in revenue for 2024 alone.[4] So while the Cyberattack paralyzed Clorox's network and crippled its business operations, Cognizant's reputation and profits have gone untarnished.

16. Clorox brings this action to hold Cognizant accountable for its failures, including its wholly inadequate performance under the parties' ITSA, breaches of the covenant of good faith and fair dealing, gross negligence, and intentional misrepresentations.

PARTIES

17. Plaintiff The Clorox Company is a Delaware corporation with its principal place of business in Oakland, California. The Clorox Company markets and sells a diverse portfolio of consumer household goods, including cleaning products, cat litter, and personal care products. Clorox's products are available for sale throughout this County, the State of California, the United States, and the world.

18. Plaintiff Clorox Services Company is a Delaware corporation with its principal place of business in Oakland, California. Clorox Services Company is a wholly-owned subsidiary of The Clorox Company.

---

[3] *Combating Cybersecurity Challenges with Advanced Analytics*, COGNIZANT (July 2019), https://www.cognizant.com/en_us/insights/documents/combating-cybersecurity-challenges-with-advanced-analytics-codex4588.pdf (last visited July 21, 2025).

[4] *Cognizant Reports Fourth Quarter and Full-Year 2024 Results*, COGNIZANT (Feb. 5, 2025), https://news.cognizant.com/2025-02-05-Cognizant-Reports-Fourth-Quarter-and-Full-Year-2024-Results (last visited July 21, 2025).

19. Defendant Cognizant Worldwide Limited is a private limited company incorporated in the United Kingdom with its principal place of business in London, England.

20. Defendant Cognizant Technology Solutions U.S. Corporation is a Delaware corporation with its principal place of business in Teaneck, New Jersey.

JURISDICTION AND VENUE

21. This Court has personal jurisdiction over Cognizant because it committed many of the acts that form the basis of Clorox's claims—including providing information technology services and other professional services—in California. Cognizant regularly and systematically transacts business in the State of California, including through employees who provide services at client locations, such as at Clorox's California offices. [redacted]

22. Venue is proper because the contract and events giving rise to the claims were performed in this County, including at Clorox's offices in Oakland and Pleasanton, California.

FACTUAL ALLEGATIONS

The 2013 Information Technology Services Agreement

23. Clorox and Cognizant's relationship began more than a decade ago.

24. On or around May 9, 2013, Clorox entered into a comprehensive Information Technology Services Agreement with Cognizant U.S., [redacted]. Cognizant U.S. continued to sign amendments to and statements of work under the ITSA.

25. The ITSA, as amended from time to time, set out Cognizant's commitments to Clorox. [redacted]

26. [redacted]

27. [redacted]

28. [redacted]

29. [redacted]

30. [redacted]

31. [redacted]

32. [redacted]

Clorox Had Comprehensive Credential Support Policies And Procedures

33. Cognizant operated the Service Desk for Clorox and provided IT support for Clorox employees, including employee credential recovery when needed.

34. [redacted]

35. Clorox had very specific and comprehensive procedures for credential support requests. These procedures were critical given that Clorox credentials are the keys to access the Clorox network. Clorox's procedures were designed to ensure that Cognizant's Service Desk Agents ("Agents") would authenticate a user requesting credential recovery—to confirm that the requestor is the user they say they are—*before* giving them access to Clorox's system.

Cognizant Knew About Clorox's Credential Support Policies And Procedures

36. Clorox ensured that Cognizant knew about its credential support policies and procedures and also required Cognizant to certify that its Agents were trained on these procedures.

37. For example, Clorox's internal Service Desk manager held weekly meetings with the managers of the Cognizant team staffed on the Service Desk ("Service Desk Leads") to discuss new procedures and action items. Clorox's internal Service Desk manager requested that his Cognizant counterpart provide email updates in a tracker confirming that action items had been completed.

38. On January 20, 2023, Clorox's internal Service Desk manager held a meeting with the Cognizant Service Desk Leads and reviewed Clorox's updated procedures for responding to network credential support requests. Under this procedure, upon receiving a network password reset request from a Clorox employee, an Agent was required to guide the employee toward using Clorox's verification and self-reset password tool, MyID; or if MyID was not available, to verify the employee's identity by (a) manager name and MyID user name before resetting the employee's

password, along with (b) required confirmation emails to the employee's Clorox email account and to the relevant manager after a reset.[5]

39. That same day, Clorox's internal Service Desk manager sent copies of the updated procedure to the Cognizant Service Desk Leads. Clorox's internal Service Desk manager requested that Cognizant share the documents with all Agents and noted under "Status" that this was "WIP," or a "W[ork] I[n] P[rogress]."

Item	Topic	Actions	Responsible one(s)	Comments	Status
1	New process starting on January 23rd Amherst Plant Pilot starts Monday 23rd (myID)	• Start with this new process in January 20th (Please read and share with all team all attached documents, specially the **myD Support Guide** one)	SD Leaders	MyID User Guide.docx MyID Support Guide.docx FW: Managing your passwords ... FW: MyID - Your phone number h...	WIP

40. Approximately one week later, after the February 3, 2023 meeting between Clorox's internal Service Desk manager and the Cognizant Service Desk Leads, Clorox's internal Service Desk manager sent another email, flagging "pending/open items from previous meeting(s)" and requested that the Service Desk Leads review and provide an update once completed. Listed below that request was the January 20, 2023 action item to share Clorox's credential support procedures with Agents—still showing a status of "WIP."

Jan 20th:

Item	Topic	Actions	Responsible one(s)	Comments	Status
1	New process starting on January 23rd Amherst Plant Pilot starts Monday 23rd (myID)	• Start with this new process in January 20th (Please read and share with all team all attached documents, specially the **myD Support Guide** one) • What if the user's manager calls on behalf of the user?	SD team Alejandro	MyID User Guide.docx MyID Support Guide.docx FW: Managing your passwords ... FW: MyID - Your phone number h...	WIP

41. On February 16, 2023, Clorox's internal Service Desk manager requested another update on open action items, including the updated credential support procedures. Finally, the Cognizant Service Desk Lead responded and confirmed that the credential support procedures action item had been completed with the comment "Educated the team," in past tense.

[5] Clorox's password support policy prior to 2023 also required the Agents to direct the user to MyID, or if not available, verify the user's identity using various techniques such as security questions.

Jan 20th:

Item	Topic	Actions	Responsible one(s)	Comments	Status
1	New process starting on January 23rd Amherst Plant Pilot starts Monday 23rd (myID)	• Start with this new process in January 20th (Please read and share with all team all attached documents, specially the **myD Support Guide** one) • What if the user's manager calls on behalf of the user?	SD team Alejandro	MyID User Guide.docx MyID Support Guide.docx FW: Managing your passwords ... FW: MyID - Your phone number h...	Educated the team
3	Return to Office plan	• Karthick to share an update on first week of February	Karthick		WIP

42. Cognizant Agents' calls with the cybercriminal exposed that this was a blatant lie.

Cognizant Failed To Follow Clorox's Policies And Procedures, Directly Resulting In A Devastating Cyberattack Against Clorox

43. Despite Cognizant's explicit acknowledgements and consistent reassurance that it was following Clorox's credential support procedures, its Agents failed to follow those processes (or even the processes that had been in place previously), which directly resulted in a significant Cyberattack against Clorox. Cognizant's substantial failures and breaches include the following:

Clorox Employee 1

44. On August 11, 2023, the cybercriminal first called the Service Desk requesting a reset of Employee 1's password "for Okta," which was an identity management tool Clorox used to authenticate access to its network. The Agent[6] responded by asking the cybercriminal to connect to Clorox's virtual private network ("VPN").

45. The cybercriminal stated that he could not connect to the VPN without a password, at which point the Agent unilaterally reset Employee 1's Clorox password without any further questioning or identity verification, in direct violation of Clorox's credential support procedures.

46. Following that success, the cybercriminal pushed further and told the Agent that his Microsoft multi-factor authentication ("MFA") was not working. Microsoft MFA is a security feature that requires employees to provide a form of secondary authentication beyond a password to verify their identity—such as accepting a push notification from an app—before accessing the Clorox network. This should have been an immediate red flag, as the combination of password

[6] Although more than one Agent spoke with the cybercriminal on August 11, 2023, Clorox refers to those Agents collectively as "Agent."

and MFA resets would effectively open the gate to the Clorox network. Instead of taking caution to verify the caller's identify in any way, the Agent simply proceeded with the MFA reset.

Cybercriminal:	*My Microsoft MFA isn't working.*
Cognizant Agent:	*Oh, ok...*
Cybercriminal:	*Can you reset my MFA? It's on my old phone ... [inaudible] old phone.*
Cognizant Agent:	*[Following a brief hold]. So thanks for being on hold, Alex. So multi-factor authentication reset has been done now. Ok. So can you check if you're able to login ...*
Cybercriminal:	*Alright. It let me sign in now. Thank you.*

47. Shortly thereafter on the same day, the cybercriminal called the Cognizant Service Desk a second time, again masquerading as Clorox Employee 1. Again, the cybercriminal requested that the Microsoft MFA associated with Employee 1's username be reset. And again, the Agent simply reset the user's MFA—never asking the caller to verify their identity as Employee 1.

48. Twenty minutes later, the cybercriminal called for the third time—again pretending to be Employee 1—and claimed that they needed their Okta credential reset yet again. And again, without verifying the caller's identity—or even questioning why the same employee would need their MFA credentials reset multiple times in short order—the Agent reset the credential again.

49. To peel off every layer of security protection that Clorox had concerning account credentials, the cybercriminal pushed further, requesting that the Agent also reset the phone number associated with Employee 1's user account for SMS MFA, which provided a separate authentication layer via a one-time password sent to a user's registered phone number in an SMS message. The Agent again reset it, allowing the cybercriminal to enter a phone number selected by the cybercriminal or leave the SMS protection feature completely turned off—no questions asked.

50. At no point during any of the calls did the Agent verify that the caller was in fact Employee 1. At no point did the Agent follow Clorox's credential support procedures—either the

pre-2023 procedure or the January 2023 update—before changing the password for the cybercriminal. The Agent further reset Employee 1's MFA credentials multiple times without any identity verification at all. And at no point did the Agent send the required emails to the employee or the employee's manager to alert them of the password reset.

51. Cognizant—displaying a shocking level of incompetence—failed over and over at the most basic level and enabled a cybercriminal to gain a foothold in Clorox's network.

52. Following the success of its first three calls, the cybercriminal continued to capitalize on Cognizant's ineptitude. The cybercriminal used Employee 1's compromised credentials to log into and gather information from the Clorox network. The cybercriminal then was able to target the credentials of Employee 2, who worked in IT security.

Clorox Employee 2

53. On August 11, 2023, the cybercriminal used the same amateur playbook to get access to Employee 2's credentials, and, again, it worked flawlessly. In a series of two calls, the Agent reset Employee 2's password, Okta MFA, and Microsoft MFA—again wholly ignoring Clorox's credential support policies and procedures at every turn.

54. First, the cybercriminal, now posing as Clorox Employee 2, called the Service Desk and requested a password reset. The Agent duly complied, without following the required authentication procedures.

Cognizant Agent:	*How can I help you today?*
Cybercriminal:	*Um my password on Okta was not working ...*
Cognizant Agent:	*I'm going to have your password reset from my end right away. Ok. And we'll see how it's going to work. Ok. [Following a brief hold] Thank you ... I'm extremely sorry for the long hold. So ... password is going to be Clorox@123.*
Cybercriminal:	*What's that?*
Cognizant Agent:	*Yeah it was Clorox@123...Ok.*
Cybercriminal:	*Yep.*
Cognizant Agent:	*Want me to wait over the phone while you are trying it?*

Cybercriminal: *Yes, yes, please.*

Cognizant Agent: *Sure ... sure.*

55. The cybercriminal then asked to have Employee 2's Okta MFA reset as well. The Agent informed the cybercriminal that she was seeing "two MFA applications" under Employee 2's account and volunteered to reset both—the Okta and Microsoft MFA. Unsurprisingly, the cybercriminal accepted the Agent's generous offer: "Yeah … reset both of them." It is illogical and inexcusable for an Agent to offer proactively to reset an MFA security tool that the cybercriminal had not even mentioned, and yet Cognizant's Agent did it anyway, again displaying a shocking level of incompetence, lack of common sense, and gross negligence.

56. The reset of Employee 2's credentials gave the cybercriminal privileged access to the Clorox network, and, once inside, the cybercriminal used Employee 2's credentials as a springboard to establish persistence and move laterally within the Clorox environment.

57. Clorox detected the cybercriminal's intrusion within three hours from the cybercriminal's initial activity in the Clorox environment, and Clorox took swift and effective containment actions in response that ejected the cybercriminal from its network within five days of the initial intrusion.

58. The Cyberattack caused devastating disruptions to Clorox's systems and operations. For example, to effectively stop the Cyberattack from further escalation, Clorox was forced to take its systems offline, pause manufacturing, and rely on manual order processing methods for weeks, resulting in product shortages for customers and significant lost sales for Clorox, as reported in Clorox's public disclosures since the Cyberattack. To date, Clorox's extensive damages total around $380,000,000. Had it not been for Clorox's decisive actions and mature business continuity plans, the impact could have been even more severe.

Cognizant's Post Incident Actions Exacerbated The Cyberattack And Further Exposed Cognizant's Incompetence

59. After opening the door to the Clorox environment for the cybercriminal, Cognizant's ongoing incompetence repeatedly impeded Clorox's real time incident response efforts.

60. Time is of the essence during a cyberattack, and every minute matters when trying to prevent a cybercriminal from escalating within an environment. As noted above, Clorox detected the cybercriminal's intrusion within three hours, and upon detection immediately called on Cognizant to deliver disaster recovery and incident response support services. But Cognizant compounded the damage it had already caused by botching its response in multiple ways.

61. ***Reinstalling a Cybersecurity Tool***. On the evening of the Cyberattack when Clorox detected suspicious activity on its network, Clorox immediately requested that Cognizant reinstall a critical cybersecurity tool that the cybercriminal had uninstalled. Despite the relayed urgency and seriousness of Clorox's request, Cognizant took over an hour to complete a task that should have taken less than 15 minutes. This inexplicable delay hindered Clorox's ability to slow down the cybercriminal's escalation within the Clorox environment when every minute was critical.

62. ***Additional Account Shutdown***. That same evening, Clorox detected suspicious activity from a specific Clorox account. Clorox immediately requested that Cognizant shut down the account. But Cognizant again delayed. Clorox later discovered the cybercriminal was using the account to escalate within the Clorox environment. Had Cognizant acted timely on this account per Clorox's request, Clorox might have been able to stop or slow the cybercriminal's escalation.

63. ***Incorrect Managed IP Addresses***. Cognizant was responsible for maintaining a list of specific IP addresses, which could be used to help limit and restrict access within the Clorox environment when necessary. When Clorox requested this list from Cognizant to contain the Cyberattack, Cognizant initially provided the wrong list and had to resend the correct list once the error was identified. This mistake resulted in an *eight-hour* delay in implementing this important containment measure and the unnecessary diversion of critical incident response resources.

64. Even following the initial crisis response, Clorox reasonably relied on Cognizant for support, given its decade of experience within the Clorox environment, but Cognizant's ongoing incompetence continued to hinder Clorox's recovery efforts.

65. ***Incompetent Cognizant Staff***. Cognizant already possessed much of the knowledge needed for Clorox's recovery given its prior IT support work and deep familiarity with the Clorox environment. However, the Cognizant personnel assigned to assist Clorox with recovery lacked individual skill and repeatedly failed to provide the deep expertise of the Clorox environment that was needed.

66. ***Cognizant Frustrated Database Recovery***. Again, the assigned Cognizant personnel were so lacking in technical competence and knowledge about Clorox's systems that they were unable to restore certain Clorox databases during recovery, despite the fact that Cognizant had supported those databases for years. Clorox was forced to seek replacement services from another vendor. The new vendor accomplished what Cognizant could not, further highlighting Cognizant's incompetence.

67. ***Cognizant Delayed Application Recovery***. In the days after the Cyberattack, Clorox attempted to rebuild certain applications, and this process exposed Cognizant's failure to maintain essential documentation required as part of its application management responsibilities. Information that an ordinary professional would expect to have been documented was conspicuously missing. Clorox was forced to recreate information that Cognizant agreed to maintain, further impeding Clorox's recovery efforts.

FIRST CAUSE OF ACTION

Breach of Contract

(By All Plaintiffs Against All Defendants)

68. Clorox realleges and incorporates by reference the allegations in paragraphs 1 through 67 as though fully set forth herein.

69. Clorox and Cognizant entered a valid written contract—the ITSA—on May 9, 2013. [redacted]

70. Cognizant breached the ITSA in multiple ways

71.

72.

73.

74.

Cognizant also sent personnel to assist with recovery efforts

who were so lacking in application support and infrastructure support skills that Clorox was forced to hire another vendor. [redacted]

75. [redacted]

76. Clorox has fully performed all of its obligations under the ITSA.

77. Cognizant's breaches caused direct damages to Clorox by failing to deliver the full bargained-for value of the breached provisions of the ITSA.

78. Cognizant's breaches proximately caused damage to Clorox, including but not limited to network remediation costs, loss of profits, property damage, goodwill, competitive advantage, and business opportunities.

79. [redacted]

SECOND CAUSE OF ACTION

Breach of the Covenant of Good Faith and Fair Dealing

(By All Plaintiffs Against All Defendants)

80. Clorox realleges and incorporates by reference the allegations in paragraphs 1 through 79 as though fully set forth herein.

81. Cognizant also owed Clorox a duty of good faith and fair dealing.

82. Clorox and Cognizant entered a valid written contract—the ITSA—on May 9, 2013. [redacted]

83. [redacted]

84. Cognizant's conduct—handing over the keys to Clorox's environment to the cybercriminal without any basic level of authentication—not only undermined but completely frustrated Clorox's rights [redacted], and therefore breached the duty of good faith and fair dealing.

85. Cognizant's breaches of the duty of good faith and fair dealing have caused damage to Clorox, including but not limited to network remediation costs, loss of profits, property damage, goodwill, competitive advantage, and business opportunities.

THIRD CAUSE OF ACTION

Gross Negligence

(By All Plaintiffs Against All Defendants)

86. Clorox realleges and incorporates by reference the allegations in paragraphs 1 through 85 as though fully set forth herein.

87. Clorox engaged Cognizant to provide professional services, including Service Desk support.

88. Cognizant, as a service provider with a special relationship to Clorox, had a duty to perform the services with reasonable care independent from its contractual obligations.

89. Cognizant breached its duty to Clorox when it failed to show even scant care and simply provided password and MFA credentials that allowed access to Clorox's network to a cybercriminal without verifying the caller's identity. This was an extreme departure from the ordinary standard of care and grossly negligent. Cognizant further breached its duty to Clorox by negligently, improperly, and recklessly impeding Clorox's response to the Cyberattack.

90. Cognizant was aware that its employees were not adequately trained. For example, in February 2023, Clorox met with Cognizant's Service Desk Leads to discuss issues with Cognizant's service and highlighted the need for regular training and evaluation. Cognizant was grossly negligent by not training its Agents to follow basic security procedures.

91. Cognizant's breach proximately caused damage to Clorox, including but not limited to network remediation costs, loss of profits, property damage, goodwill, competitive advantage, and business opportunities.

FOURTH CAUSE OF ACTION

Intentional Misrepresentation

(By All Plaintiffs Against All Defendants)

92. Clorox realleges and incorporates by reference the allegations in paragraphs 1 through 91 as though fully set forth herein.

93. Cognizant falsely and repeatedly represented to Clorox that it had properly trained its staff on Clorox's policies and procedures, including on February 16, 2023, when the Cognizant Service Desk Lead represented that Cognizant had "[e]ducated the team" on the updated credential support procedures.

94. Cognizant knew the representations it made to Clorox were false because Cognizant had not, in fact, properly trained its staff on Clorox's policies and procedures.

95. Multiple Agents failed on August 11, 2023, to follow Clorox's policies in performing credential resets. This reflects a systematic failure by Cognizant to train its staff. Clorox had sought repeated assurances that Cognizant's Agents had been trained appropriately. Given that passwords are the first line of defense against cyber intrusions, and given Cognizant's purported expertise in this field, Cognizant knew the stakes but nevertheless intentionally provided false assurances to Clorox that the team had been "[e]ducated," including in the February 16, 2023 email referenced above, all while knowing that this was false with respect to some—if not many or all—of its Agents. Cognizant made these misrepresentations with an intent to deceive Clorox and to induce Clorox to rely on such misrepresentations.

96. Clorox was more than justified in relying on Cognizant's misrepresentations that it had properly trained its staff on Clorox's policies and procedures—because Cognizant was a trusted managed service provider with whom Clorox had partnered for over a decade.

97. Cognizant's intentional misrepresentations caused damage to Clorox, including but not limited to network remediation costs, loss of profits, property damage, goodwill, competitive advantage, and business opportunities.

PRAYER FOR RELIEF

WHEREFORE, Clorox prays for judgment in its favor and against Defendants, inclusive, as follows:

1. Awarding damages as described in each of the above claims, in favor of Clorox and against Defendants, in an amount to be established according to proof at trial of approximately $380 million;
2. Awarding Clorox punitive damages;
3. Awarding Clorox pre- and post-judgment interest, attorneys' fees and costs, and other expenses incurred in this action; and
4. Granting Clorox such further relief as this Court deems just and proper.

JURY DEMAND

Clorox demands a jury trial for all issues triable by jury.

Date: July 22, 2025

Respectfully submitted,

LATHAM & WATKINS LLP

By

Michael H. Rubin
Mary Rose Alexander

Attorneys for Plaintiffs The Clorox Company and Clorox Services Company