David J. Jordan (#1751)
Email: djordan@foley.com
David L. Mortensen (#8242)
Email: dmortensen@foley.com
Tyler A. Dever (#15584)
Email: tdever@foley.com
FOLEY & LARDNER LLP
95 S. State Street, Suite 2500
Salt Lake City, UT 84111
Telephone: 801.401.8900

Attorneys for Plaintiff

IN THE UNITES STATES DISTRICT COURT IN AND FOR

THE DISTRICT OF UTAH, CENTRAL DIVISION

ALEGEUS TECHNOLOGIES, LLC, a Delaware limited liability company, Plaintiff, v. DIGICERT, INC., a Utah corporation, Defendant.	**VERIFIED COMPLAINT AND JURY DEMAND** Civil No. 2:24-cv-00534 The Honorable ________________

Plaintiff Alegeus Technologies, LLC ("Alegeus"), by and through its counsel, hereby complains and alleges against defendant DigiCert, Inc. ("DigiCert" or "Defendant") as follows:

INTRODUCTION

1. This action arises from DigiCert's abrupt decision to decertify Alegeus' SSL certificates for Alegeus' websites for is clients, which will result in severe damages to Alegeus and its many clients and their many millions of plan participants.

2. As set forth in greater detail below, Alegeus is a leading provider of a business-to-business, white-label funding and payment platform for healthcare carriers and third-party administrators to administer consumer-directed employee benefit programs, including HSAs,

FSAs, HRAs, COBRA, health and wellness programs, dependent care accounts and transportation accounts serving millions of U.S households (collectively, the "Health Accounts").

3. In addition, Alegeus is designated as a non-bank health savings trustee ("NBT") by the IRS. This designation allows it to serve as the custodian of Health Savings Accounts ("HSAs") through a direct custodial agreement with the HSA accountholders.

4. Alegeus contracts primarily with health plans and third-party administrators (the "Alegeus Clients") who manage these Health Accounts to provide a platform, where individuals with Health Accounts can manage their accounts by, among other things, paying health providers for medical services, submitting claims for reimbursement, checking account balances and making contributions. Alegeus provides unique websites and domain names for the Alegeus Clients (the "Alegeus Websites"). Alegeus' Clients in turn contract with employers to provide services related to the Health Accounts to the employers who make available the benefits of the Health Accounts to their employees. These employees are typically referred to as plan participants. Alegeus does not contract directly with employers or the plan participants.

5. A number of years ago, Alegeus entered into a Master Services Agreement and related agreements (collectively, the "Master Service Agreement") with DigiCert to provide digital security certificates for the Alegeus Websites. See Master Services Agreement, Ex. 1. Specifically, DigiCert provides public key infrastructure ("PKI") and validation required for issuing digital certificates or TLS/SSL certificates (collectively, the "Security Certificates") for the Alegeus Websites.

6. About thirty (30) days ago, Alegeus worked with DigiCert to update many of the Security Certificates for the Alegeus Websites. Alegeus followed DigiCert's instructions for updating the Security Certificates.

7. Following such updates, and without any interim notification of any issues, late on the afternoon of July 29, 2024, DigiCert sent an email to Alegeus stating that "DigiCert would be revoking [the Alegeus Websites]" unless it reissued/rekeyed and reinstalled the impacted certificates by 7:30 p.m. (Coordinated Universal Time) or 1:30 p.m. (Mountain Time) on July 30, 2024 (the "Revocation Notice"). *See* DigiCert Notice, Ex. 2. DigiCert asserted that the certificates needed to be revoked because they did not have a proper Domain Control Verification (DCV), which was because DigiCert "did not include the underscore prefix with the random value used in some CNAME-based validation cases." *Id.* In other words, DigiCert failed to properly validate the Alegeus Websites, and then suddenly and without any proper notice, gave Alegeus less than 24 hours to recertify each of the Alegeus Websites. Otherwise, each of the Alegeus Websites would be decertified.

8. Recertifying the Alegeus Websites requires Alegeus to coordinate with each of its Clients and cannot be completed for all of the Alegeus Websites by the DigiCert prescribed deadline. Accordingly, Alegeus requested three days to complete recertification of the Alegeus Websites. DigiCert has refused.

9. DigiCert's actions constitute a material breach of its agreement with Alegeus. Worse, if DigiCert decertifies the Alegeus Websites, it will cause Alegeus, Alegeus' Clients and each of the individual account holders severe and irreparable harm. Accordingly, Alegeus brings this action to obtain an injunction preventing DigiCert from decertifying the Alegeus Accounts

and to recover for the severe damages that result from such decertification, all caused by DigiCert's actions.

PARTIES, JURISDICTION, AND VENUE

10. Alegeus is a Delaware limited liability company with its principal place of business at 1601 Trapelo Rd, Waltham, Massachusetts 02451. Alegeus is a wholly owned subsidiary of Alegeus Technologies Holding Corp., which is a Delaware Corporation with its principal place of business at 1601 Trapelo Rd, Waltham, Massachusetts 02451.

11. DigiCert is a Utah corporation with its principal place of business at 2801 North Thanksgiving Way, Suite 500, Lehi, Utah 84043-5803.

12. This Court has jurisdiction over this matter and the parties pursuant to 28 U.S.C. § 1332, because there exists complete diversity among plaintiff and defendant and the amount at issue is over $75,000 exclusive of costs and interest. This Court further has jurisdiction over this dispute because Alegeus and DigiCert agreed that state and federal courts located in Salt Lake County would have exclusive jurisdiction over any disputes arising from or related to the Master Services Agreement. *See* Master Services Agreement at § 9.8.

13. Venue is proper in this Judicial District pursuant to 28 U.S.C. § 1391, including because DigiCert is a resident of Utah. Venue is also proper in this Court because Alegeus and DigiCert agreed that state and federal courts located in Salt Lake County would have exclusive jurisdiction over any disputes arising from or related to the Master Services Agreement. *See* Master Services Agreement at § 9.8.

FACTUAL ALLEGATIONS

Aegeus

14. Alegeus is a leading provider of a business-to-business, white-label funding and payment platform for healthcare carriers and third-party administrators to administer consumer-directed employee benefit programs, including HSAs, FSAs, HRAs, COBRA, health and wellness programs, dependent care accounts and transportation accounts serving millions of U.S households (collectively, as defined above, the “Health Accounts”).

15. In addition, Alegeus is designated as a non-bank health savings trustee (“NBT”) by the IRS. This designation allows it to serve as the custodian of Health Savings Accounts (“HSAs”) through a direct custodial agreement with the HSA accountholders.

16. Alegeus provides separate websites (as defined above, the “Alegeus Websites”) for the Alegeus Clients.

DigiCert

17. DigiCert is a digital security company. It provides high-assurance SSL certificates to government agencies, financial institutions, educational and medical institutions, and companies worldwide.

18. DigiCert offers standard and wildcard SSL certificates, extended validation certificates, and unified communications certificates; and code signing certificate solutions that include Adobe, Apple, Java, and Microsoft code signing certificates. It also provides managed public key infrastructure solutions that allow organizations to take control of SSL certificate management, including issuing new certificates and reissuing, replacing, and revoking existing SSL certificates.

19. DigiCert is a voluntary member of the Certification Authority Browser Forum (CABF), which has bylaws stating that certificates with an issue in their domain validation must be revoked within 24 hours.

The Master Services Agreement

20. In order to obtain security certificates for the Alegeus Websites, Alegeus entered into the Master Services Agreement with DigiCert.

21. In the Master Services Agreement, DigiCert agreed to provide security certification services to Alegeus. In return, Alegeus agreed to pay for those services.

22. Specifically, the Master Services Agreement provides that:

> 2.1. Order Forms. Customer may purchase specific Services from DigiCert by entering into one or more mutually agreed upon quotes, purchase schedules, purchase orders, or order forms (whether online or electronic) that set forth the specific Services being procured by Customer under this Agreement, the term when each such Service is to be provided by DigiCert (the “Service Term”) and the related payment terms for such Service (each, an “Order Form”). Order Forms are considered “mutually agreed upon” either (i) when executed by both parties in writing, (ii) when Customer affirms its electronic acceptance of an Order Form that DigiCert has presented to Customer via electronic means (e.g., at https://www.digicert.com/order), or (iii) when DigiCert presents Customer with an Order Form and Customer affirms its acceptance by issuing a purchase order. Customer and DigiCert acknowledge and agree that each Order Form will be governed by and incorporated by reference into the terms of this Agreement.

23. In June or July 2024, Alegeus ordered and paid DigiCert to update several security certificates for the Alegeus Websites.

24. Within the last thirty (30) days from this Complaint, DigiCert provided updated security certificates for several of the Alegeus Websites.

DigiCert Abruptly Notices that It Intends to Revoke Alegeus’ Security Certificates

25. Around 6:41 p.m. (ET) on July 29, 2024, DigiCert sent the Revocation Notice to Alegeus stating that it intended to revoke the Security Certificates for each of the Alegeus Websites.

26. The Revocation Notice stated:

> We're writing to inform you that DigiCert must revoke your certificates, no later than JULY 30, 2024, at 19:30 UTC.
>
> To avoid disruption, you must reissue/rekey and reinstall the impacted certificates before they are revoked no later than JULY 30, 2024, at 19:30 UTC.

Revocation Notice at 1.

27. The Revocation Notice explained that <u>DigiCert's</u> error caused the need for Alegeus to reissue/rekey and reinstall the Security Certificates for the Alegeus Websites. *Id.* Specifically, it explained:

> DigiCert will be revoking certificates that did not have proper Domain Control Verification (DCV). Before issuing a certificate to a customer, DigiCert validates the customer's control or ownership over the domain name for which they are requesting a certificate using one of several methods approved by the CA/Browser Forum (CABF). One of these methods relies on the customer adding a DNS CNAME record which includes a random value provided to them by DigiCert. DigiCert then does a DNS lookup for the domain and verifies the same random value, thereby proving domain control by the customer.
>
> There are multiple valid ways to add a DNS CNAME record with the random value provided for this purpose. One of them requires the random value to be prefixed with an underscore character. The underscore prefix ensures that the random value cannot collide with an actual domain name that uses the same random value. While the odds of that happening are practically negligible, the validation is still deemed as non-compliant if it does not include the underscore prefix.
>
> **<u>Recently, we learned that we did not include the underscore prefix with the random value used in some CNAME-based validation cases.</u>** This impacted approximately 0.4% of the domain validations we have in effect. Under strict CABF rules, certificates with an issue in their domain validation must be revoked within 24 hours, without exception.

Id. (emphasis added).

28. As the Revocation Notice explained, DigiCert failed to properly include the underscore prefix with the random value in certain CNAME-based validation cases. As a result, of its error, DigiCert required that Alegeus reissue/rekey and reinstall its Security Certificates.

Despite it being entirely an error of DigiCerti's making, DigiCert suddenly threatened that, if Alegeus failed to reissue/rekey and reinstall its Security Certificates within less than 24 hours, the Security Certificates for the Alegeus Websites would be revoked.

29. Alegeus contacted DigiCert immediately in an attempt to resolve the matter within a reasonable commercial time period, including contacting its CEO. *See* Ex. 3. DigiCert's response is that there are no exceptions to extending the time period before revocation is to occur. *See id*.

30. On information and belief, DigiCert knew or should have known about its failure to properly complete the Security Certificates for Alegeus weeks ago. Despite that DigiCert has arbitrarily chosen this less than 24-hour window to replace defective certificates they themselves provided Alegeus just a few weeks ago.

31. DigiCert's failure to properly complete the Security Certificates constitutes a material breach of the Master Services Agreement, as well as negligence and gross negligence.

Alegeus Cannot Reissue and Reinstall the Security Certificates Within less than 24 Hours.

32. To Reissue and Reinstall the Security Certificates, Alegeus must work with and coordinate with its Clients, who are required to take steps to rectify the certificates. Alegeus has hundreds of such Clients. Alegeus is generally required by contract to give its clients much longer than 24 hours' notice before executing such a change regarding certification.

33. Consequently, due to the errors and delays of DigiCert alone, Alegeus cannot practically make all the required changes in such a short time period and will be faced with failing to meet the terms of its customer agreements.

Revocation of the Security Certificates for the Alegeus Websites Will Cause Alegeus Severe and Irreparable Harm.

34. If DigiCert revokes the Security Certificates for the Alegeus Websites, it will cause Alegeus severe and irreparable damages in an amount to be determined at trial.

35. Among other things, without the Security Certificates, plan participants will be unable to access and manage their accounts and a large number of participants will be unable to pay for medical services. Such a disruption (a) would impede consumers access to healthcare accounts, (b) would subject Alegeus to high penalties for failing to meet contractual SLAs, (c) could constitute a breach of Alegeus' agreements with its clients, opening Alegeus to a myriad of claims and lawsuits from its clients; (d) will harm Alegeus' goodwill and business reputation; and (e) cause Alegeus economic damages that cannot be readily calculated.

FIRST CAUSE OF ACTION
(Breach of Contract Against DigiCert)

36. Alegeus hereby incorporates by reference the allegations set forth in the preceding paragraphs as though fully set forth herein.

37. The Master Services Agreement is a valid and enforceable agreement.

38. Alegeus performed its obligations under the Master Services Agreement by ordering and paying for the Security Certificates for each of the Alegeus Websites.

39. DigiCert breached the Master Services Agreement by (a) failing to properly complete the Security Certificates for the Alegeus Websites; (b) failing to provide notice of its failure to properly complete the Security Certificates for the Alegeus Websites; and (c) threatening to revoke and/or revoking the Security Certificates for the Alegeus Websites with less than 24 hours' notice.

40. DigiCert's actions constitute a material breach of the Master Services Agreement.

41. As a result of DigiCert's breach, Alegeus has suffered or will suffer severe and irreparable damages in amount to be determined at trial, plus interest, costs and attorneys' fees to the fullest extent allowed by law.

42. Because DigiCert's actions will cause Alegeus irreparable harms, Alegeus is entitled to an injunction prohibiting DigiCert from revoking the Security Certificates for the Alegeus Websites until Alegeus is able to obtain the properly rekey and reissue the Security Certificates.

SECOND CAUSE OF ACTION
(Breach of the Implied Covenant of Good Faith and Fair Dealing Against DigiCert)

43. Alegeus hereby incorporates by reference the allegations set forth in the preceding paragraphs as though fully set forth herein.

44. DigiCert's conduct as alleged above constitutes a breach of the implied covenant of good faith and fair dealing.

45. According to Utah law, every contract has an implied covenant of good faith and fair dealing. This covenant requires that neither party to a contract do anything that injures the right of the other to receive benefits of the contract.

46. Despite its implied obligation, DigiCert has breached its obligations by, among other things, (a) failing to properly complete the Security Certificates for the Alegeus Websites; (b) failing to provide notice of its failure to properly complete the Security Certificates for the Alegeus Websites; and (c) threatening to revoke and/or revoking the Security Certificates for the Alegeus Websites with less than 24 hours' notice.

47. As a result of DigiCert's breach, Alegeus has suffered or will suffer severe and irreparable damages in amount to be determined at trial, plus interest, costs and attorneys' fees to the fullest extent allowed by law.

48. Because DigiCert's actions will cause Alegeus irreparable harms, Alegeus is entitled to an injunction prohibiting DigiCert from revoking the Security Certificates for the Alegeus Websites until Alegeus is able to obtain the properly rekey and reissue the Security Certificates.

THIRD CAUSE OF ACTION
(In the Alternative, Negligence and Gross Negligence)

49. Alegeus hereby incorporates by reference the allegations set forth in the preceding paragraphs as though fully set forth herein.

50. As set forth above, negligently failed to properly complete the Security Certificates for the Alegeus Websites.

51. In doing so, DigiCert acted negligently and/or grossly negligently.

52. As a result of DigiCert's negligence, Alegeus has suffered or will suffer severe and irreparable damages in amount to be determined at trial, plus interest, costs and attorneys' fees to the fullest extent allowed by law.

53. Because DigiCert's actions will cause Alegeus irreparable harms, Alegeus is entitled to an injunction prohibiting DigiCert from revoking the Security Certificates for the Alegeus Websites until Alegeus is able to obtain the properly rekey and reissue the Security Certificates.

PRAYER FOR RELIEF

WHEREFORE, Alegeus pray for judgment against DigiCert as follows:

1. On all Causes of Action, for direct and consequential damages in an amount determined at trial, plus interest and attorneys' fees and costs.

2. On all Causes of Action, for an injunction prohibiting DigiCert from revoking the Security Certificates for the Alegeus Websites until Alegeus is able to obtain the properly rekey and reissue the Security Certificates.

3. On all Causes of Action, for such other and further relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Alegeus demands a trial by jury for all issues so triable.

Dated this the 30th day of July, 2024.

FOLEY & LARDNER LLP

/s/ *David Mortensen*
David J. Jordan
David Mortensen
Tyler A. Dever

Attorneys for Alegeus

VERIFICATION

I, Derek Holmes, I am the Chief Information Office for Alegeus Technologies, LLC ("Alegeus") and have been authorized by Alegeus to make this verification on behalf of Alegeus. I hereby verify that I have read the foregoing Verified Complaint and that the facts recited therein are true and correct insofar as they concern the acts and deeds of Alegeus, and are believed by me to be true insofar as they concern the acts and deeds of any other person or entity. This verification is made under the penalty of perjury.

Dated: July 30, 2024

/s/ Derek Holmes
Derek Holmes
Alegeus Technologies, LLC