IN THE SUPERIOR COURT OF FULTON COUNTY
STATE OF GEORGIA

	CIVIL ACTION NO. XX-XXXX
DELTA AIR LINES, INC., **Plaintiff,** **v.** **CROWDSTRIKE, INC.,** **Defendant.**	**Complaint** For: (1) Computer Trespass (O.C.G.A. §16-9-93) (2) Trespass to Personalty (O.C.G.A. §51-10-3) (3) Breach of Contract (4) Intentional Misrepresentation/Fraud by Omission (5) Strict-Liability: Product Defect (6) Gross Negligence (7) Deceptive and Unfair Business Practices Act (O.C.G.A. §10-1-391 et seq.) (8) Attorneys' Fees (9) Punitive Damages

Plaintiff, Delta Air Lines, Inc. ("Delta") brings this suit against CrowdStrike, Inc. ("CrowdStrike").

INTRODUCTION

1. Since its founding, CrowdStrike has advertised itself as the cybersecurity industry leader. But on July 19, 2024, CrowdStrike forced untested and faulty updates to its customers, causing more than 8.5 million Microsoft Windows-based computers around the world to crash, while also preventing many of them from being able to restart (the "Faulty Update"). These updates were pushed onto customers and their systems even when customers did not enable automatic update settings. The Faulty Update massively disrupted airlines, railroads, hospitals, emergency services, government agencies, banks, and hotels, among other businesses and

organizations, and negatively impacted millions of people across the globe. Commentators have characterized the Faulty Update as the "worst" and "largest" cyber event in history.

2. For Delta, the Faulty Update was catastrophic. Like many of CrowdStrike's other customers, Delta did not enable automatic updates. The Faulty Update disabled most of Delta's computers running on a Microsoft Windows operating system ("Microsoft OS"), crippled Delta's operations for several days, forced thousands of flight cancellations and delays, and adversely affected more than a million Delta customers. Delta estimates that it suffered over $500 million in out-of-pocket losses from the Faulty Update, in addition to future revenue and severe harm to its reputation and goodwill.

3. While CrowdStrike widely touts as part of its published "business ethics" that "we [CrowdStrike] do not cut corners" and that "[w]e are honest with our customers," nothing could be further from the truth. CrowdStrike caused a global catastrophe because it cut corners, took shortcuts, and circumvented the very testing and certification processes it advertised, for its own benefit and profit. If CrowdStrike had tested the Faulty Update on even one computer before deployment, the computer would have crashed.

4. To appreciate CrowdStrike's role in the worldwide disaster, one must understand that CrowdStrike intentionally created and exploited an unauthorized door within the Microsoft OS through CrowdStrike's Falcon software. CrowdStrike, as a certified Microsoft Windows Hardware Quality Lab ("WHQL") and Early Launch Antimalware ("ELAM") driver developer, is required to submit any deep-system "kernel-level" programming and data for rigorous testing and verification before deployment. To maintain the facade that it could safely deploy its solutions more rapidly than competitors, CrowdStrike touted compliance with operating system

requirements, while altering previously certified computer programming with uncertified and untested shortcuts that damaged and impaired its clients' systems and businesses.

5. Despite the fact that both CrowdStrike and its CEO previously subjected other customers to similar problems, the company rolled out the Faulty Update – which included a kernel-"access violation" – without the necessary quality assurance or client authorization. The kernel is the core of a computer.

6. In the aftermath of the Faulty Update, CrowdStrike conceded it did not subject its programming and data changes to even the most basic tests, and that it did not roll out the Faulty Update in staged deployments to customers commensurate with standard software development practices.

7. It is no wonder that CrowdStrike President, Michael Sentonas, personally accepted the "Most Epic Fail" award for the Faulty Update on CrowdStrike's behalf at the annual August 10, 2024 Las Vegas Def Con hacking conference. While accepting the award, CrowdStrike's President said it is "super important to own it when you do things horribly wrong, which we did in this case."[1] Delta files this lawsuit to hold CrowdStrike to its word: CrowdStrike must "own" the disaster it created.

THE PARTIES

8. Plaintiff Delta Air Lines, Inc. is a Delaware corporation with its headquarters, primary operations, and principal place of business at 1030 Delta Boulevard, Atlanta, Georgia 30354.

[1] Wes Davis, *CrowdStrike accepted a 'Most Epic Fail' award at Def Con hacking conference*, The Verge (Aug. 12, 2024, 7:44 AM), https://www.theverge.com/2024/8/12/24218536/crowdstrike-accepts-def-con-pwnies-award-most-epic-fail-global-windows-it-outage.

9. Defendant CrowdStrike, Inc. is a Delaware corporation with its principal executive office and principal place of business at 206 E 9th Street, Suite 1400, Austin, Texas 78701.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this action because the contract between the parties at issue expressly provides that the state courts situated in Fulton County, Georgia, shall have exclusive jurisdiction over the resolution of all disputes arising under the contract and because the acts or omissions giving rise to the claims occurred within Fulton County, Georgia.

11. This Court has personal jurisdiction over the Defendant because the contract at issue expressly provides that Plaintiff and Defendant have each irrevocably submitted to the personal jurisdiction of this Court, and because the acts or omissions giving rise to the claims occurred within Fulton County, Georgia, and the Defendant conducts business in Fulton County. For example, many of Delta's computers, networks, and data located in the State of Georgia were the subject of the unpermitted behavior at issue in this Complaint.

12. Venue is proper in this Court pursuant to O.C.G.A. § 9-10-30 and other applicable law, as the contract at issue was executed in Fulton County, Georgia, and the Defendant conducts business within Fulton County, Georgia. Additionally, the acts and omissions giving rise to the Plaintiff's claims occurred within Fulton County, Georgia.

13. This is an action for damages in excess of Fifteen Thousand Dollars ($15,000.00) exclusive of attorneys' fees and costs.

FACTUAL ALLEGATIONS

Delta Is a Market Leader and America's Most-Awarded Airline

14. Delta is one of the world's largest airlines and is traded on the NYSE as "DAL." Headquartered in Atlanta, Delta operates a global network of domestic and international routes with significant hubs and key markets in Amsterdam, Atlanta, Boston, Detroit, London-Heathrow, Los Angeles, Mexico City, Minneapolis-St. Paul, New York-JFK and LaGuardia, Paris-Charles de Gaulle, Salt Lake City, Seattle, Seoul-Incheon, and Tokyo. Delta proudly employs over 100,000 people, with over 4,000 daily flights globally using a large and diverse fleet of aircraft.

15. Delta is known for its customer service, reliability, and operational efficiency. Delta served over 190 million customers in 2023 and was recognized by J.D. Power in 2024 for being the number one airline in First, Business, and Premium Economy Passenger satisfaction.

16. In January 2024, Delta won the Cirium Platinum Award for operational excellence for the third year. The award is given annually to airlines that show exemplary on-time performance while navigating complex operations and limiting the impact of disruptions to its customers.[2]

17. Delta also topped the Cirium rankings for being the most on-time airline in North America in January 2024. Cirium defines an on-time flight as one that arrives within 15 minutes of its scheduled gate arrival. In 2023, Cirium tracked 1,635,486 Delta flights, 84.72% of which arrived on time, which is up from 83.63% the previous year. Delta's on-time arrival rate far

[2] *Most on-time airline in North America: Delta wins Cirium Platinum Award*, Delta News Hub (Jan. 4, 2024, 11:00 AM), https://news.delta.com/most-time-airline-north-america-delta-wins-cirium-platinum-award.

exceeded the average of 74.45% for the North American top performers and also came in above the average of 83.67% for all global top performers.[3]

18. Delta was "America's most awarded airline" for multiple years, receiving numerous other rewards for reliability, leadership, and innovation in 2024:[4]

Organization:	**Award:**
Skytrax World Airline Awards	Delta received two **Skytrax World Airline Awards**, **Best Airline in North America** and **Best Airline Staff**, at the prestigious **2024 World Airline Awards** held in the U.K. It is the fourth year running that Delta has scooped the Best Airline in North America award, and third consecutive year for the best staff award.
The Points Guy	After compiling data across a diverse range of metrics, including operational reliability, customer experience, network, cost and loyalty offerings, The Points Guy recognized Delta as the **best U.S. airline for the sixth time since 2018**.
The145	Delta TechOps was named "**Best Total Solutions Provider**" by The145 in its 2024 Top Shop Awards.
Fortune	Delta's people-first culture continues to be recognized, earning the airline a spot on **Fortune's 100 Best Companies to Work For® list** for the fifth year. Delta is the only airline included on the 2024 list.
Aviation Week Network	Delta TechOps was honored with a **2024 Grand Laureate Award by Aviation Week Network** at its 66th Annual Laureate Awards ceremony. The award recognized TechOps' work with the APEX program – specifically how APEX is reimagining engine maintenance operations for Delta.
Fast Company	Delta earned a coveted spot on **Fast Company's list of the Most Innovative Companies**, climbing from its No. 8 spot in 2023 to **No. 2 in the travel category**. The airline was recognized for its Wi-Fi revolution that is working to ensure the future of travel is connected.
Air Transport World	Delta's outstanding operational performance, commitment to safety and premium customer service has earned **2024 Airline of the Year by aviation publication Air Transport World**.

[3] *Id.*
[4] *Delta: America's most-awarded airline*, Delta News Hub, https://news.delta.com/delta-americas-most-awarded-airline.

TIME	Delta landed on TIME's inaugural list of the "**World's Best Companies**," coming in at No. 12 – the only U.S. airline in the top 155. TIME's award is based on three criteria: employee satisfaction, revenue growth and sustainability. Delta earned the No. 5 spot in employee satisfaction and an overall score of 91.13.
Fortune	Delta was recognized by Fortune with a No. 11 placement on **Fortune's Top 50 Most Admired Companies** list. The company's strong management and commitment to providing elevated experiences and premium products also secured a No. 1 ranking out of the eight airlines on the list.
Wall Street Journal	Delta was named the **Top U.S. Airline of 2023 by the Wall Street Journal**, ranking No. 1 overall and in three of the seven categories, including on-time arrivals, low U.S. DOT complaints and involuntary bumping. Delta also ranked No. 2 in mishandled baggage and extreme delays.
OAG	**OAG Aviation Worldwide** announced Delta was the most on-time global airline in its 2023 rankings.

19. As part of its IT-planning and infrastructure, Delta has invested billions of dollars in licensing and building some of the best technology solutions in the airline industry. For cyber threat detection and response, Delta uses CrowdStrike, which many, prior to the Faulty Update, regarded as the best in its class. Delta uses Microsoft for some of its most mission-critical servers and most of its employee workstations, airport gate information screens, and productivity solutions. The Microsoft OS and Microsoft productivity solutions are regarded as among the best-in-class and are among the most widely used amongst Fortune 500 companies, including other major U.S. airlines.

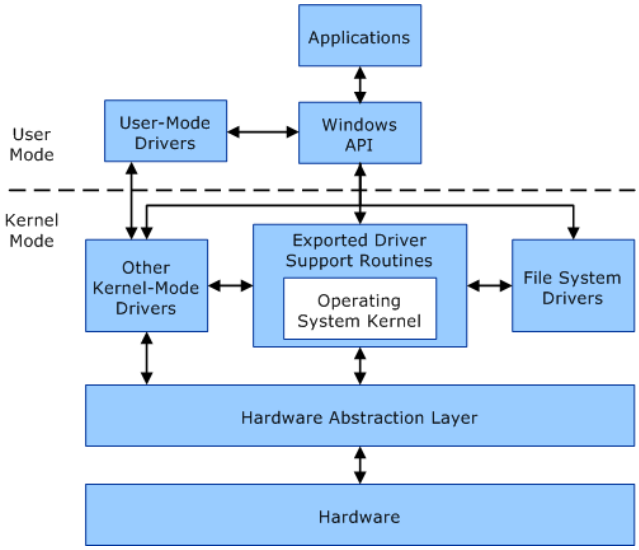
Microsoft's Kernel-Level Certification Process

20. The Microsoft OS separates programming into two distinct types: (1) kernel-level programming where the operating system runs, and (2) user-level programming where other software runs. Software in the kernel-level communicates directly with the hardware and devices, manages memory, and schedules programming processes. By contrast, the user-level typically

contains non-operating system applications. Outside of the kernel, all other software in the computer operates in user space. Application programming does not run in the kernel, and kernel programming never runs in user mode.

21. Generally, the kernel of a computer operating system is the core of the computer's software, the function of which is to manage the actual hardware of the computer. Unlike programming in the user space, any software running in the kernel operates with no restrictions and has full access privileges to manage the hardware. Because the kernel is the first level of software operations interfacing with hardware, if software crashes in the kernel, the entire computer crashes. Because of this, deploying unauthorized third-party kernel drivers[5] (or computer programming components that help to operate components at the kernel-level) is very dangerous for an operating system. It is far safer for developers, such as CrowdStrike, to operate in the user space because it is isolated from the kernel.

22. This is a Microsoft-visual graphic of its typical architecture:[6]



[5] *See Types of Windows Drivers*, Microsoft Ignite (Dec. 14, 2024), https://learn.microsoft.com/en-us/windows-hardware/drivers/kernel/types-of-windows-drivers.
[6] *User mode and kernel mode*, Microsoft Ignite (Sept. 27, 2024), https://learn.microsoft.com/en-us/windows-hardware/drivers/gettingstarted/user-mode-and-kernel-mode.

23. Beginning with Windows 10, Microsoft required that all kernel-level drivers be submitted to Microsoft for testing, verification, and certification.[7] During this certification process, Microsoft requires submission of the entire "driver package" for the kernel-file. As Microsoft explains: "A driver package includes all the software components that you must supply to ensure that your device is supported with Windows. Typically, a driver package contains the following components: INF file, Catalog file, Driver files, Other files (emphasis added)."[8] This means that any part of the driver package that can affect the behavior of the driver programming or system memory – such as "driver files" that have the "-.sys" extension[9] – must be included as part of the driver package for testing, verification, and certification.

24. Microsoft requires that drivers be certified by its Windows Hardware Quality Lab (WHQL) prior to being loaded by Windows OS. Specifically, "Early Launch Antimalware" (ELAM, or antimalware software intended to provide security protection for computers when they start up) certifications require:[10]

---

[7] *See Driver Signing changes in Windows 10*, Microsoft (Mar. 12, 2019, 7:10 AM), https://techcommunity.microsoft.com/t5/windows-hardware-certification/driver-signing-changes-in-windows-10/ba-p/364859

[8] *Components of a Driver Package*, Microsoft Ignite (June 19, 2024), https://learn.microsoft.com/en-us/windows-hardware/drivers/install/components-of-a-driver-package (emphasis added).

[9] *See id.* ("[t]ypically, a driver is a dynamic-link library (DLL) with the *.sys* file name extension.").

[10] *See ELAM Prerequisites*, Microsoft Ignite (May 12, 2023), https://learn.microsoft.com/en-us/windows-hardware/drivers/install/elam-prerequisites.

Early Launch Antimalware drivers must adhere to the following program requirements to be signed by **WHQL** and loaded by Windows.

Antimalware Vendor Participation Requirements

Microsoft requires that Early Launch Antimalware vendors be members of the Microsoft Virus Initiative (MVI). This membership ensures that the vendors are active antimalware community participants with a positive industry reputation. If you are not a member of the MVI program and believe you need use of ELAM, please reach out to mvi@microsoft.com for additional information.

Windows Hardware Quality Lab (WHQL) submission

- Submit your driver for verification as documented at ELAM Driver Submission
- The **WHQL** process will verify that the vendor is permitted to submit early launch drivers. Your submission will fail if you are not an MVI member.

25. Microsoft represents that it runs rigorous tests on a third-party kernel-driver before it may be allowed at the kernel level. It then assigns the driver a digital certification if the kernel-driver passes the verification process and is deemed by Microsoft to be trustworthy. This verification process is especially important for ELAM drivers.

26. An ELAM driver with new programming and logic cannot rely on a prior certification for an older set of programming, because the new programming and logic introduces new and different sets of system behavior in the kernel. Properly tested, vetted, and verified driver packages are critical to the maintenance and safeguarding of a stable operating system.

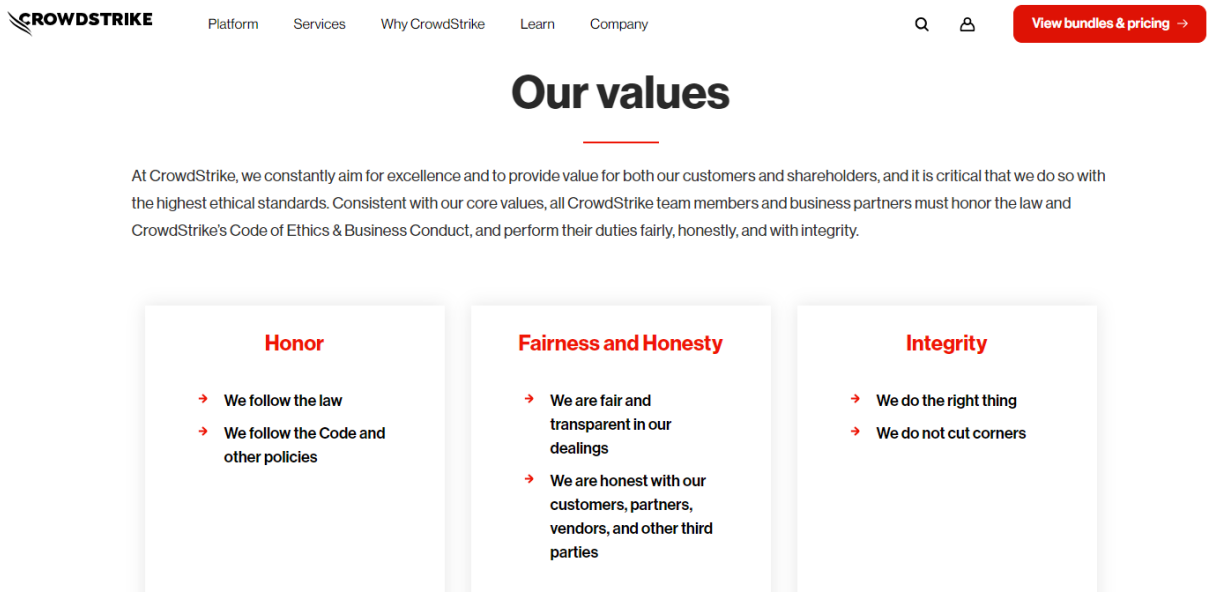
27. As further discussed herein, CrowdStrike repeatedly assured its customers that it adhered to the rigors and testing required by Microsoft, and that it never circumvented the ELAM/WHQL requirements. That assurance was broken as CrowdStrike exploited its privileged access to the Microsoft OS kernel in a manner its customers, including Delta, did not authorize.

CrowdStrike's Drive for Competitive Advantage and Its "Falcon System" Exploit

28. CrowdStrike claims that its name is derived from its mission to leverage the power of the "crowd" (i.e., collective clients) to combat cyber threats. It claims that by harnessing

collective intelligence and collaboration, CrowdStrike could create a more effective cybersecurity solution. Hence, it claims that it added "-strike" to its name to emphasize a proactive approach to identifying and neutralizing threats.

29. CrowdStrike can only harness the power of the "crowd," of course, if CrowdStrike has customers willing to share their threat intelligence and confidential information with CrowdStrike. To convince customers to do that, CrowdStrike portrays itself as reliable and trustworthy. As CrowdStrike touts in its "Code of Ethics & Business Conduct,"[11] its purported "core values" are "honor," "fairness and honesty," and "integrity," and CrowdStrike reassures customers that "we do not cut corners" and "we are fair and transparent in our dealings":



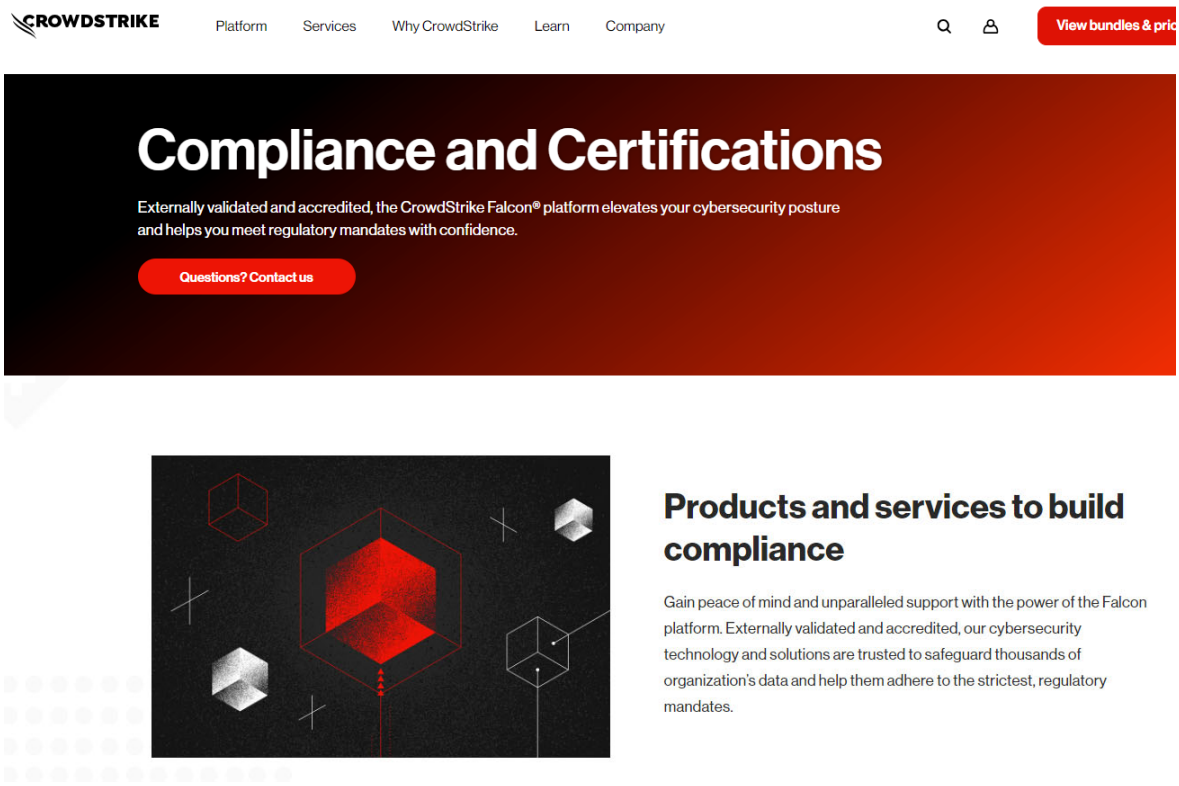
30. As CrowdStrike became more successful, however, its desire to use its customers' confidential information became less about its customers' benefit and more about putting profit ahead of protection and software stability. For example, CrowdStrike was particularly interested in maintaining a competitive advantage in providing security for the popular Microsoft OS. The

[11] *See CrowdStrike Ethics & Compliance*, CrowdStrike, https://www.crowdstrike.com/about-us/ethics-compliance/.

Microsoft OS dominates the enterprise operating systems market and is the operating system of choice for many Fortune 500 companies. Delta is informed, and on that basis alleges, that CrowdStrike leveraged its trusted position with clients and Microsoft to circumvent certification processes, and to maintain a competitive edge against its cybersecurity rivals.

31. Specifically, CrowdStrike never told its customers that to detect and prevent cyber-attacks, CrowdStrike would exploit its privileged kernel-level access in order to insert untested and uncertified programming or data. In fact, CrowdStrike offered its clients the ability to turn off automatic updates. While CrowdStrike swore to protect its customers' computer systems, networks, and programs, CrowdStrike circumvented and bypassed the controls and protections the developers of those systems created. CrowdStrike leveraged its expertise gained from crowdsourced information, to maintain an exploit of the Microsoft OS for its own expediency. CrowdStrike did this to sell more of its own products and services as "solutions." CrowdStrike knew that these unauthorized alterations and hacking of kernel-level controls and protections would upset and potentially damage CrowdStrike's customers, and it thus hid these tactics from customers, including Delta.

32. One of CrowdStrike's exploitations of Microsoft OS vulnerabilities was with its "Falcon" cybersecurity system. CrowdStrike claimed that Falcon was one of its top cybersecurity products and services and that it was "externally validated and accredited":



33. CrowdStrike assured customers that Falcon is "fully compliant" with rigorous certification standards, including Microsoft's ELAM/WHQL requirements for kernel driver programming and data for the Microsoft OS. For example, even in its Root Analysis Report on August 6, 2024, CrowdStrike touted its Microsoft certifications:[12]

> CrowdStrike certifies each new Windows sensor release through the Windows Hardware Quality Labs (WHQL) program, which includes extensive testing through all required tests in Microsoft's Windows Hardware Lab Kit (HLK) and Windows Hardware Certification Kit (HCK). The WHQL certification process marks the end of a comprehensive internal testing gauntlet involving functional tests, longevity tests, stress tests with fault injection, fuzzing and performance tests. During the testing required for the WHQL program, the sensors use the latest versions of channel files at the time of certification.

[12] *See External Technical Root Cause Analysis — Channel File 291*, CrowdStrike (Aug. 6, 2024), https://www.crowdstrike.com/wp-content/uploads/2024/08/Channel-File-291-Incident-Root-Cause-Analysis-08.06.2024.pdf.

34. As another example, in an August 9, 2024 blog,[13] CrowdStrike stated:

> ## Fully Compliant with the Most Rigorous Partner Certifications for Kernel Drivers
>
> CrowdStrike fully adheres to Microsoft's partner certification for kernel drivers and is a full member of the Microsoft Virus Initiative (MVI), which adds additional requirements. For each kernel driver release, CrowdStrike conducts extensive testing through all required tests in Microsoft's Hardware Lab Kit (HLK) and Microsoft's Hardware Certification Kit (HCK), and submits results to Microsoft Windows Hardware Quality Labs (WHQL) for certification.
>
> It is important to understand the difference between driver attestation (attestation signing) and WHQL verification, which CrowdStrike pursues. WHQL verification is far more rigorous than attestation signing and requires copious testing through the HCK/HLK process. This designation is embedded in the Microsoft signature attached to the kernel driver in the form of an Enhanced Key Usage (EKU). The differences in certification labeling should not be confused

35. CrowdStrike touted adherence to Microsoft's WHQL requirements as being one of its design requirements from "day one." In the same August 9 blog, CrowdStrike stated:

> As part of MVI, CrowdStrike must additionally respect additional requirements above and beyond WHQL testing in order to meet the strict performance and stability requirements that enable access to technologies such as ELAM.
>
> Finally, if the Falcon sensor recognizes that it is running on a version of the OS kernel that CrowdStrike has not fully tested against, the sensor disables certain functionality in the interest of stability and avoiding crashes. This is a fundamental part of the philosophy that has guided design of the Falcon architecture from Day One.

36. Contrary to what CrowdStrike represented, its Falcon programming and data did not adhere to WHQL/ELAM requirements. And CrowdStrike knew that. Instead, CrowdStrike designed Falcon to circumvent Microsoft's requirements, using Falcon as an unauthorized door and shortcut for CrowdStrike developers. After the Faulty Update and ensuing crippling of Delta's systems, CrowdStrike revealed to Delta for the first time that its "content updates" for its kernel

[13] *See* Alex Ionescu et al., *Tech Analysis: CrowdStrike's Kernel Access and Security Architecture*, CrowdStrike Blog (Aug. 9, 2024), https://www.crowdstrike.com/blog/tech-analysis-kernel-access-security-architecture/.

drivers alter computer programming and data for those drivers, including behavior and system memory, without further Microsoft verification. For example, CrowdStrike belatedly revealed that these updates included "-.sys" files that altered computer programming and system memory:[14]

> On Windows systems, Channel Files reside in the following directory:
>
> `C:\Windows\System32\drivers\CrowdStrike\`
>
> and have a file name that starts with "`C-`". Each channel file is assigned a number as a unique identifier. The impacted Channel File in this event is 291 and will have a filename that starts with "`C-00000291-`" and ends with a `.sys` extension. Although Channel Files end with the SYS

37. CrowdStrike altered and replaced the driver computer programming and data with new "content updates" through doors it had left in the Falcon software. That meant that the (unauthorized) updated driver packages behaved differently than the original certified-driver packages due to the new programming and data CrowdStrike placed and executed through the doors. As a result of this tactic, customers like Delta ended up with unverified and unauthorized programming and data running in kernel mode with each new "content update."[15] Delta would have never agreed to such a dangerous process had CrowdStrike disclosed it.

38. When the Faulty Update crashed millions of computers worldwide, CrowdStrike files were being directed to read from parts of the computer system that they were not supposed to. The CrowdStrike kernel package that had Microsoft ELAM certification defined only 20 fields.

---

[14] According to CrowdStrike's July 20 explanation of the Faulty Update, one problematic file was a "-.sys" file that was forcibly inserted into client systems, altering and replacing prior programming and data. *See Technical Details: Falcon Content Update for Windows Hosts*, CrowdStrike Blog (July 20, 2024), https://www.crowdstrike.com/en-us/blog/falcon-update-for-windows-hosts-technical-details/ ("[t]he impacted Channel File in this event is 291 and will have a filename that…ends with a .sys extension"). CrowdStrike deleted this blog sometime in August 2024. Although CrowdStrike claimed in this July 20 blog that "-.sys" files "are not kernel driver[]" programming and data, Microsoft developer guidelines state that they are. *See Components of a Driver Package*, Microsoft Ignite (June 19, 2024), https://learn.microsoft.com/en-us/windows-hardware/drivers/install/components-of-a-driver-package.

[15] It is currently unclear what Microsoft knew through the certification process and as a result of the Faulty Update.

However, when deploying the Faulty Update, CrowdStrike, without authorization, added an additional field to the package, so that 21 fields were now included. After inserting this additional unauthorized parameter, CrowdStrike then changed the programming logic in the ELAM-certified package from "non-wildcard" (*i.e.*, logic looking for a total number of conditions together) to "wildcard" (*i.e.*, logic looking for any combination of various conditions) for the rogue 21st parameter. The addition of the 21st rogue field and the changes in logic caused the entire operating system to crash because the Falcon code now attempted to access deep system memory in the kernel that it was not authorized to access, which is why this type of fault is called an "access violation" or "out-of-bounds memory fault" by the technical community. This fault is the operating system's way of saying, "you are not supposed to be here."

39. Even computer programming novices would know that such fundamental alterations of programming logic required exhaustive testing and client authorization, particularly in the kernel. CrowdStrike did neither.

40. Microsoft reported in a blog on the Faulty Update, "CrowdStrike describes the root cause as a memory safety issue—specifically a read out-of-bounds access violation in the CSagent driver."

41. Indeed, CrowdStrike's own written analysis soon after the Faulty Update identified the problem as, "[o]pening the crash dump in the Windows kernel debugger and using the standard !analyze-v command for a quick summary, we see that a memory fault (also known as an **'access violation'**) bugcheck ha[d] occurred...."

42. CrowdStrike designed its kernel drivers to allow for these kinds of unauthorized alterations and replacements of existing programming and data. CrowdStrike used the "content updates" as shortcuts to avoid both the additional necessary permissions and authorization from

clients and the certifications and testing required by operating system developers like Microsoft, relying instead on old and outdated certifications. Again, Delta would have never agreed to such security shortcuts had CrowdStrike disclosed them. CrowdStrike's services contract with Delta expressly stated that CrowdStrike would not so alter Delta's systems without authorization, or build such doors:

> [CrowdStrike will] take commercially reasonable efforts to avoid the introduction, and [CrowdStrike] will not subsequently introduce into the Delta's computer systems where the Software is installed, any unauthorized 'back door,' 'time bomb,' 'Trojan horse,' 'worm,' 'drop dead device,' 'virus,' 'preventative routines' or other computer software routines designed to: (i) permit access to or use of Delta's computer systems by Service Provider or a third party not authorized by this Agreement; (ii) disable, modify, damage or delete the Customer Data and any data, software, computer hardware or other equipment operated or maintained by Delta; or (iii) perform any other such similar unauthorized actions.

Damages Inflicted on Delta's Computer Systems, Networks, and Programs

43. On July 19, 2024, CrowdStrike imposed the Faulty Update on most of its customers, without warning and without requesting consent. Indeed, like many other CrowdStrike customers, Delta had not enabled its automatic update settings for CrowdStrike, so that it could control installations and updates onto Delta's infrastructure.

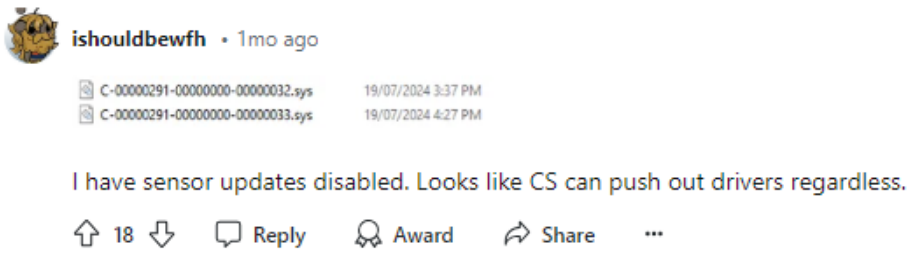
44. The Faulty Update pushed onto customers was done without any rollback capabilities, which meant that once it was deployed, there was no way for CrowdStrike to revert the customer back to where the customer was before the deployment. To make matters worse, CrowdStrike failed to implement the Faulty Update in a staged deployment, and instead recklessly deployed the update to customers. With a staged deployment, an update starts with only a small percentage of customers and reaches additional customers in stages so that failures can be identified before a widescale deployment. This mitigates the impact if the update fails and causes system crashes. And CrowdStrike failed to test the Faulty Update. If CrowdStrike had tested the

Faulty Update on even one computer before deployment, the computer would have crashed. As a result of CrowdStrike's failure to use a staged deployment and without rollback capabilities, the Faulty Update caused widespread and catastrophic damage to millions of computers, including Delta's systems, crashing Delta's workstations, servers, and redundancy systems.

45. But Delta, like many other customers, could not readily restart Microsoft OS for many of its computers because CrowdStrike's Faulty Update altered and hacked Microsoft OS programming and memory. This effectively forced the Microsoft OS on many devices to crash as soon as it read the faulty CrowdStrike programming and data at the kernel-level, needing another restart. The media referred to the crashed state as "the blue screen of death," because the computers would be frozen on a mostly Microsoft-blue screen. When Delta (and other CrowdStrike customers) tried to restart again, the Microsoft OS would again be forced to read CrowdStrike's faulty and contaminated programming and data, causing the operating system to crash again. Many Delta employees could not remediate the Faulty Update files from their computers for hours due to these problems.

46. For affected Delta computers that could restart, they also had to be remediated manually one at a time and could not be fixed remotely. The problems caused by the Faulty Update prevented administrators from being able to start affected Delta computers remotely or to remove the Faulty Update remotely. Contemporary computer networks, including Delta's, were designed to be able to be managed by administrators remotely, so that fixes and remediations can be done quickly and consistently across the entire inventory of computer workstations and terminals from a centralized location by the qualified technical personnel. Because the Faulty Update could not be removed remotely, CrowdStrike crippled Delta's business and created immense delays for Delta customers.

47. Notably, other CrowdStrike customers reported that they also could not prevent the Faulty Updates even when they tried to, such as by disabling automatic updates from CrowdStrike. Their systems crashed anyway. Giving one example online:



48. As Delta disclosed in its SEC 8K, filed on August 8, 2024, Item 7.01 Regulation FD Disclosure, Delta experienced operational disruption resulting from the CrowdStrike-caused outage on July 19.[16] The outage disrupted Delta's operations, causing approximately 7,000 flight cancellations over five days.[17] "An operational disruption of this length and magnitude is unacceptable, and our customers and employees deserve better. Since the incident, our people have returned the operation to an industry-leading position that is consistent with the level of performance our customers expect from Delta," said Ed Bastian, Delta's Chief Executive Officer.[18] "We are pursuing legal claims against CrowdStrike and Microsoft to recover damages caused by the outage, which total at least $500 million."[19]

[16] Delta Air Lines, Inc., Current Report (Form 8-K), item 7.01 (Aug. 8, 2024), https://d18rn0p25nwr6d.cloudfront.net/CIK-0000027904/073daaf9-c982-4c0a-bec4-841194f94c91.pdf.
[17] *Id.* at 2.
[18] *Id.*
[19] *Id.*

CrowdStrike Admits to Intentional and Reckless Conduct

49. On August 6, 2024, CrowdStrike published an "External Technical Root Cause Analysis – Channel File 291,"[20] which provided "further depth on the findings, mitigations, technical details and root cause analysis of the incident." Therein, CrowdStrike admitted that its programming and data changes "should have staged deployment," explaining that staged deployment mitigates impact if the changes cause failures such as system crashes. Further, CrowdStrike conceded that it should have "[p]rovide[d] customer[s with] control over the deployment of Rapid Response Content updates," and promised that it will do so going forward.

50. Indeed, CrowdStrike admitted that deployments of invasive techniques resulting in new programming and data should have been gradual (i.e., "staged"), such as on 1% of machines, then 10% of machines, before 100% of the machines. CrowdStrike itself explained the benefit of staged deployments, in its August 6 Root Cause Analysis report:[21]

> Staged deployment mitigates impact if a new Template Instance causes failures such as system crashes, false-positive detection volume spikes or performance issues. New Template Instances that have passed canary testing are to be successively promoted to wider deployment rings or rolled back if problems are detected. Each ring is designed to identify and mitigate potential issues before wider deployment. Promoting a Template Instance to the next successive ring is followed by additional bake-in time, where telemetry is gathered to determine the overall impact of the Template Instance on the endpoint.

51. Staged deployments and testing are basic and standard software development practices, as both CrowdStrike and its CEO are well aware.[22] When CrowdStrike's current CEO

---

[20] *External Technical Root Cause Analysis — Channel File 291*, CrowdStrike (Aug. 6, 2024), https://www.crowdstrike.com/wp-content/uploads/2024/08/Channel-File-291-Incident-Root-Cause-Analysis-08.06.2024.pdf.

[21] *Id*.

[22] *See* CNBC Television, *CrowdStrike CEO on global outage: Goal now is to make sure every customer is back up and running*, YouTube (July 19, 2024), https://www.youtube.com/watch?v=Dn7cN0sJhrI.

was the Chief Technology Officer of McAfee in 2010, that company released an antivirus software update that caused a worldwide meltdown for Microsoft Windows XP users by sending systems into a reboot loop and requiring tedious manual repairs very similar to CrowdStrike's recent Faulty Update. Similarly, just a few months before the Faulty Update, CrowdStrike released an update that caused similar problems for Linux operating systems.[23]

52. Any kernel-level computer programming and data that alters and changes the system programming and memory needed customer consent. Delta could not have been more clear in not allowing for automatic updates in the Falcon system. And CrowdStrike certainly knew that anything that affected system programming and memory needed to be well-tested and verified before deployment.

53. After the Faulty Update, CrowdStrike conceded in the Root Cause Analysis report that it always should have sought customer permission to deploy the schemes it ran with its Falcon system:[24]

> The Falcon platform has been updated to provide customers with increased control over the delivery of Rapid Response Content. Customers can choose where and when Rapid Response Content updates are deployed. We are continuing to enhance this capability to provide more granular control over Rapid Response Content deployments together with content update details via release notes, to which customers can subscribe.

---

[23] *See* Simon Sharwood, *CrowdStrike's Falcon Sensor also linked to Linux kernel panics and crashes*, The Register (July, 21, 2024, 11:51 PM), https://www.theregister.com/2024/07/21/crowdstrike_linux_crashes_restoration_tools/.

[24] *External Technical Root Cause Analysis — Channel File 291*, CrowdStrike (Aug. 6, 2024), https://www.crowdstrike.com/wp-content/uploads/2024/08/Channel-File-291-Incident-Root-Cause-Analysis-08.06.2024.pdf.

Delta Would Not Have Permitted Unauthorized Doors and Required Proper Testing

54. When CrowdStrike deployed the Faulty Update, CrowdStrike even forced its updates onto customers who had automatic updates disabled, such as Delta. Delta had not enabled the automatic update setting, because Delta wanted to maintain the proper type of change management controls over how updates could affect its computer systems and networks.

55. Delta would have never allowed the type of unauthorized and uncertified door that CrowdStrike implemented. Without proper testing, verification, and certification, Delta would not have allowed CrowdStrike to alter or replace kernel-level programming and data that affected Microsoft OS programming and memory. At all relevant times, CrowdStrike never disclosed its use of an unauthorized door, and Delta never gave CrowdStrike such permission.

56. CrowdStrike knew that any computer programming and data that it deployed that affected third-party systems' programming and memory required Delta testing as well. Otherwise, it could affect Delta's system stability and reliability. At no time did CrowdStrike inform Delta that its Falcon system would so affect the Microsoft OS. At minimum, Delta would have tested how such deployments affected Delta systems, including the Microsoft OS, in a staged environment, pursuant to customary software development practices.

57. CrowdStrike never disclosed that it deployed computer programming and data that circumvented certifications, verifications, and testing, and Delta never gave CrowdStrike such permission. Instead, at all times relevant, Delta was informed, and on that basis reasonably believed, that CrowdStrike already obtained the necessary compliance and certifications after rigorous and thoughtful testing.

58. When asked about the Faulty Update, the CEO for a leading cybersecurity provider, Sentinel One, stated on the record on July 30, 2024: "I haven't seen anybody update the kernel in

such a way [as CrowdStrike did] — and definitely not in a way that doesn't go through customer approval, as well. I mean, the other part here is, it's not just Microsoft in the process. It's customers. You're [supposed to be] giving customers the ability to control what's deployed, when it's deployed, what version is deployed, rollback capabilities, gradual rollout, phased deployments. All of those are kind of table stakes. So to see that with one push [of a] button, this gets immediately sent globally, causing the biggest IT security outage in history — it's not just a mistake. It's just architecture."

COUNT I:

COMPUTER TRESPASS (O.C.G.A. SECTION 16-9-93)

59. Plaintiff Delta restates, realleges, and incorporates herein by reference the preceding paragraphs 1 through 58, as if fully set forth herein.

60. In its contract with Delta, CrowdStrike specifically averred that "[CrowdStrike] will not subsequently introduce into Delta's computer systems any unauthorized 'back door,' 'time bomb,' 'Trojan horse,' 'worm,' 'drop dead device,' 'virus,' 'preventative routines' or other computer software routines designed to: (i) permit access to or use of Delta's computer systems by Service Provider or a third party not authorized by this Agreement; (ii) disable, modify, damage or delete the Customer Data and any data, software, computer hardware or other equipment operated or maintained by Delta; or (iii) perform any other such similar unauthorized actions."

61. By installing its exploit in Delta systems without Delta's permission or knowledge, CrowdStrike obstructed, interrupted, and interfered with Delta's use of its computer programs and computer networks. Further, by deploying its Faulty Update, which included an "access violation," CrowdStrike obstructed, interrupted, and interfered with Delta's use of its computer programs and computer networks.

62. By installing its exploit in Delta systems, and by deploying its Faulty Update with the access violation, CrowdStrike altered, damaged, and caused to malfunction Delta's computers, computer networks, and computer programs.

63. By installing its exploit in Delta systems, and by deploying its Faulty Update with the access violation, CrowdStrike deleted and removed previously certified computer programming or data, replacing them with what was unverified, untested, and unauthorized.

64. Delta did not authorize CrowdStrike to take these actions on Delta's systems, particularly any change in programming or data that affected or altered the behavior and memory of Delta's core systems, including the Microsoft OS on its computers and networks.

65. At all times relevant, CrowdStrike knew that its actions would—or that there was a very high likelihood that its actions could—cause Delta, its computers, its computer networks, and computer programs and data substantial harm.

66. CrowdStrike's unauthorized actions caused Delta, its computers, its computer networks, and its computer programs and data substantial harm.

67. Pursuant to O.C.G.A. Section 16-9-93, CrowdStrike is liable to Delta for damages sustained and costs of suit, including, without limitation, Delta's lost profits and expenditures, including attorneys' fees. Delta suffered over $500 million in out-of-pocket losses from the Faulty Update, in addition to reputational harm and future revenue loss.

COUNT II:

TRESPASS TO PERSONALTY (O.C.G.A. § 51-10-3)

68. Plaintiff Delta restates, realleges, and incorporates herein by reference the preceding paragraphs 1 through 67, as if fully set forth herein.

69. CrowdStrike abused, damaged, and interfered with Delta's personal property. As described herein, CrowdStrike replaced and altered Delta's computer programming or data, and interfered with and damaged Delta's computers and computer network, with the Faulty Update (including the "access violation") through the door CrowdStrike had left in its Falcon system and service for that purpose.

70. CrowdStrike intentionally designed its applications and services to allow for the replacement, and alteration of Delta's programming or data, and to be able to interfere with Delta's computers and computer network. CrowdStrike had no authorization, contractual or otherwise, to interfere with Delta's software, data, networks, computers, and other property in this fashion. CrowdStrike never disclosed—and Delta never would have allowed—CrowdStrike's use of an unauthorized door to interfere with, replace, or alter kernel-level programming and data. This dangerous practice exceeded any authorization or access granted by Delta, and was in fact specifically prohibited by Delta.

71. CrowdStrike caused Delta substantial damage, including expenditures and lost profits, along with attorneys' fees and litigation expenses. Delta suffered approximately over $500 million in out-of-pocket losses, in addition to reputational harm and future revenue loss.

COUNT III:

BREACH OF CONTRACT

72. Plaintiff Delta restates, realleges, and incorporates herein by reference the preceding paragraphs 1 through 71, as if fully set forth herein.

73. Delta and CrowdStrike entered into contracts governing CrowdStrike's provision of products and services to Plaintiff, including a Subscription Services Agreement with an effective

date of June 30, 2022 (the "SSA"), and a Statement of Work with an effective date of July 1, 2022 (the "Falcon SOW").

74. The contracts between the parties, including the SSA and Falcon SOW, governed CrowdStrike's provision of its Falcon cybersecurity software and related services to Delta (the "Subscription Services") at all relevant times.

75. Under the SSA, CrowdStrike agreed to "host, maintain and support the Subscription Services and make them available to Delta and its Affiliates via the Internet or other data transmission system, pursuant to the terms and conditions" of the SSA and related agreements.

76. Under the SSA, CrowdStrike owed, *inter alia*, a duty to Delta and agreed that:

a. The Subscription Services would be "performed by qualified personnel in a thorough and workmanlike manner";

b. CrowdStrike must "take commercially reasonable efforts to avoid the introduction, and [CrowdStrike] will not subsequently introduce into the Delta's computer systems where the Software is installed, any unauthorized 'back door,' 'time bomb,' 'Trojan horse,' 'worm,' 'drop dead device,' 'virus,' 'preventative routines' or other computer software routines designed to: (i) permit access to or use of Delta's computer systems by Service Provider or a third party not authorized by this Agreement; (ii) disable, modify, damage or delete the Customer Data and any data, software, computer hardware or other equipment operated or maintained by Delta; or (iii) perform any other such similar unauthorized actions."

77. CrowdStrike breached its contractual promises in an intentional manner—or in a manner that was no less than grossly negligent—by:

a. Intentionally creating and exploiting an unauthorized door within Microsoft's OS via the Falcon software, without additional verification and certifications with each kernel-level update, including the Faulty Update;

b. Evading and exploiting a vulnerability in Microsoft's ELAM/WHQL certification standards and requirements by replacing and altering kernel-level programming or data without proper certification or authorization;

c. Implementing the Faulty Update, which included an "access violation," without minimal testing, and routine quality and assurance;

d. Deploying the Faulty Update without staged deployments, including installing the Faulty Update onto Delta's computers without its knowledge or consent; and

e. Deploying the Faulty Update without any rollback capabilities.

78. The agreement between Delta and CrowdStrike included an exchange of promises or value, including consideration. Delta agreed to and did pay for its products and services, including for subscriptions to use Defendant's Falcon cybersecurity software.

79. Delta performed all obligations and conditions required and expected of it and/or had a valid excuse for not performing any such obligations.

80. CrowdStrike knew that its actions would likely cause Delta, its computers, its computer networks, and computer programs substantial harm. Delta suffered over $500 million in out-of-pocket losses from the Faulty Update, in addition to the loss of future revenue and severe damage to Delta's reputation and goodwill.

COUNT IV:

INTENTIONAL MISREPRESENTATION/FRAUD BY OMISSION

81. Plaintiff Delta restates, realleges, and incorporates herein by reference the preceding paragraphs 1 through 80, as if fully set forth herein.

82. Delta purchased and renewed CrowdStrike's services and products between June 3, 2022 and 2024. Over the course of its ongoing relationship, interactions, and dealings, Delta placed immense trust and confidence in CrowdStrike, including because Delta relied on CrowdStrike for critical system-wide security and because CrowdStrike had the type of privileged access to Delta's systems that could—and did—cause a system-wide meltdown if mishandled.

83. CrowdStrike made the following misrepresentations during each of its sales pitches and renewals with Delta, on or around June 30, 2022, July 1, 2023, and March 30, 2024:

a. CrowdStrike did not take shortcuts;

b. CrowdStrike's Falcon product included various manufacturer and developer certifications, including Microsoft's WHQL certification;

c. CrowdStrike did not introduce into Delta's computer systems any unauthorized "back door", "time bomb", 'virus", "preventative routines" or other computer programming or data designed to permit access to or use of Delta's computer systems in an unauthorized matter; and

d. CrowdStrike does not disable, modify, damage or delete from the Delta computer systems and networks any data, software, computer hardware or other equipment operated or maintained by Delta, or perform any other such similar unauthorized actions.

84. CrowdStrike also omitted and suppressed numerous material facts throughout the Parties' relationship that CrowdStrike was under an obligation to communicate, including that:

a. CrowdStrike built dangerous doors into Delta's Microsoft OS systems, computers, and computer networks via the Falcon software, and CrowdStrike would use these doors to gain unauthorized access to those systems;

b. CrowdStrike evaded and exploited a vulnerability in Microsoft's ELAM/WHQL certification standards and requirements by providing "content updates" that altered and replaced kernel-level programming or data without proper certification, including "access violations";

c. CrowdStrike instituted deficient controls in its procedure for updating Falcon;

d. CrowdStrike was not adequately testing or appropriately rolling out updates to Falcon;

e. CrowdStrike's inadequate software testing and unauthorized deployments such as the Faulty Update may potentially cripple Delta's systems.

85. CrowdStrike was obligated to disclose (rather than hide) this information because of, among other things, its relationship of trust and confidence with Delta and because such disclosure was necessary to ensure that CrowdStrike's affirmative representations were not misleading and deceptive.

86. CrowdStrike made its misrepresentations willfully and/or recklessly and with the intent to deceive Delta into continuing to rely on CrowdStrike for crucial security. Delta relied on CrowdStrike's misrepresentations each time that Delta renewed the parties' relationship.

87. CrowdStrike knew that its actions would likely cause Delta, its computers, its computer networks, and computer programs substantial harm. Delta suffered over $500 million

in out-of-pocket losses from the Faulty Update, in addition to the loss of future revenue and severe damage to Delta's reputation and goodwill.

COUNT V:

STRICT-LIABILITY: PRODUCT DEFECT

88. Plaintiff Delta restates, realleges, and incorporates herein by reference the preceding paragraphs 1 through 87, as if fully set forth here.

89. The Falcon system and Faulty Update were defective, including how they bypassed Microsoft and customers' controls.

90. The defects in the Falcon system and Faulty Update existed at the time they were deployed by CrowdStrike onto Delta's systems.

91. The defects in the Falcon system and Faulty Update were proximate causes of injuries to Delta's property and goodwill. Delta suffered approximately over $500 million in out-of-pocket losses, in addition to reputational harm and future revenue loss.

COUNT VI:

GROSS NEGLIGENCE

92. Plaintiff Delta restates, realleges, and incorporates herein by reference the preceding paragraphs 1 through 91, as if fully set forth here.

93. CrowdStrike owed a duty of care to Delta. Delta relied on CrowdStrike for critical system-wide security, and CrowdStrike had the type of privileged access to Delta's systems that could—and did—cause a system-wide meltdown if mishandled. CrowdStrike was thus positioned to exercise a controlling influence over Delta's interests in the security, reliability and function of the computer systems vital to Delta's business. Moreover, for these reasons, CrowdStrike acted as a fiduciary and agent of Delta.

94. CrowdStrike failed to exercise the slight diligence or care of the degree that persons of common sense, however inattentive they may be, would use under the same or similar circumstances.

95. CrowdStrike failed to exercise even the slightest diligence and care by:

a. intentionally creating and exploiting an unauthorized door within Microsoft's OS via the Falcon software, without additional verification and certifications with each kernel-level update, including the Faulty Update;

b. Implementing the Faulty Update, which included an "access violation," without minimal testing, and routine quality and assurance;

c. Deploying the Faulty Update without staged deployments, including installing the Faulty Update onto Delta's computers without its knowledge or consent; and

d. Deploying the Faulty Update without any rollback capabilities.

96. CrowdStrike knew that its actions would likely cause Delta and Delta's property, including its computers, its computer networks, and computer programs, substantial harm. Delta suffered over $500 million in out-of-pocket losses from the Faulty Update, in addition to the loss of future revenue and severe damage to Delta's reputation and goodwill.

COUNT VII:

DECEPTIVE AND UNFAIR BUSINESS PRACTICES (O.C.G.A. § 10-1-391 et seq.)

97. Plaintiff Delta restates, realleges, and incorporates herein by reference the preceding paragraphs 1 through 96, as if fully set forth herein.

98. CrowdStrike engaged in unfair and deceptive practices in commerce by misleadingly advertising and describing its cybersecurity products and services as "[e]xternally

validated and accredited" and compliant with Microsoft's ELAM/WHQL certification standards and requirements for kernel driver programming or data.

99. CrowdStrike is an entity engaged in business involving computers, and specifically is engaged by Delta, among many others, to provide cybersecurity software and related services.

100. CrowdStrike, through both its marketing described above and the SSA, made numerous representations about the scope, quality, and reliability of its work in and relating to its cybersecurity software and Delta's computer and computer network.

101. These representations were shown to be false, and worked as a fraud and deceit upon Delta. Specifically, CrowdStrike contracted with Delta that:

a. the Subscription Services would be "performed by qualified personnel in a thorough and workmanlike manner";

b. CrowdStrike must "take commercially reasonable efforts to avoid the introduction, and [CrowdStrike] will not subsequently introduce into the Delta's computer systems where the Software is installed, any unauthorized 'back door,' 'time bomb,' 'Trojan horse,' 'worm,' 'drop dead device,' 'virus,' 'preventative routines' or other computer software routines designed to: (i) permit access to or use of Delta's computer systems by Service Provider or a third party not authorized by this Agreement; (ii) disable, modify, damage or delete the Customer Data and any data, software, computer hardware or other equipment operated or maintained by Delta; or (iii) perform any other such similar unauthorized actions."

102. Moreover, CrowdStrike marketing materials promised that:

a. CrowdStrike did not take shortcuts;

b. Its cybersecurity Falcon platform was "[e]xternally validated and accredited";

c. Falcon was compliant with Microsoft's ELAM/WHQL certification standards and requirements for kernel driver programming and data; and

d. CrowdStrike was "fair and transparent in [its] dealings," and was "honest with its customers, partners, vendors, and other third parties."

103. CrowdStrike violated these representations and broke these promises in connection with its work involving and using a computer and computer network, and, in violation of the Fair Business Practices Act, O.C.G.A. § 10-1-393.5(b), thereby operated a fraud against and deceived Delta intentionally, without Delta's knowledge or approval, by:

a. Intentionally installing and exploiting an unauthorized door within Microsoft's OS, and Delta's computers and computer networks, via the Falcon software and service, for which additional authorization, verification, and testing was not obtained with each kernel-level update, including the Faulty Update;

b. Evading and exploiting a vulnerability in Microsoft's ELAM/WHQL certification standards and requirements by providing "content updates" that in reality altered and replaced kernel-level programming or data without authorization and proper certification, including with "access violations";

c. Implementing the Faulty Update without even minimal testing, and routine quality and assurance;

d. Deploying the Faulty Update without staged deployments, including installing the Faulty Update onto Delta's computers without its consent.

104. CrowdStrike knew that its actions would likely cause Delta, its computers, computer networks, and computer programs substantial harm. Delta suffered over $500 million

in out-of-pocket losses from the Faulty Update, in addition to the loss of future revenue and severe damage to Delta's reputation and goodwill.

105. Delta has been injured and damaged in its business and property by CrowdStrike's violation of the Fair Business Practices Act, and thus Delta may recover its damages sustained pursuant to O.C.G.A. § 10-1-399(a).

106. Delta is entitled to exemplary damages pursuant to O.C.G.A. §10-1-339(a), because of CrowdStrike's intentional violation of the Fair Business Practices Act.

107. Delta complied with the 30-day notice provision under O.C.G.A. § 10-1-399(b) through a letter sent by counsel for Delta to counsel for CrowdStrike on July 29, 2024.

COUNT VIII

ATTORNEYS' FEES

108. Plaintiff Delta restates, realleges, and incorporates by reference the preceding paragraphs 1 through 107, as if fully set forth herein.

109. Through and in addition to the conduct described above, CrowdStrike had acted in bad faith, has been litigious, and has caused Delta unnecessary trouble and expense. As a result, Delta is entitled to recover its expenses of litigation, including attorney fees.

COUNT IX

PUNITIVE DAMAGES

110. Plaintiff Delta restates, realleges, and incorporates by reference the preceding paragraphs 1 through 109, as if fully set forth herein.

111. CrowdStrike's actions showed willful misconduct, malice, fraud, wantonness, oppression, and that entire want of care which would raise the presumption of conscious

indifference to consequences. Delta is therefore entitled to an award of punitive damages in an amount necessary to punish, penalize, and deter such conduct.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Delta is entitled to:

a. An award of money damages compensating Delta for the losses it has suffered as a result of CrowdStrike's Faulty Update;

b. An award of litigation expenses, including attorney fees, pursuant to O.C.G.A. §§ 16-9-93, 10-1-399(a), and 13-6-11;

c. An award of punitive damages pursuant to O.C.G.A. §§ 10-1-399(a) and 51-12-5.1; and

d. All other necessary and appropriate relief.

Dated: [insert]

Respectfully submitted,

_____

Frank M. Lowrey
Georgia Bar No. 410310
Jane "Danny" Vincent
Georgia Bar No. 380850
Michael R. Baumrind
Georgia Bar No. 960296
BONDURANT MIXSON & ELMORE, LLP
One Atlantic Center
Suite 3900
1201 West Peachtree Street NW
Atlanta, Georgia 30309
(404) 881-4100
lowrey@bmelaw.com
vincent@bmelaw.com
baumrind@bmelaw.com

David Boies (*pro hac vice* forthcoming)
BOIES SCHILLER FLEXNER LLP
55 Hudson Yards
20th Floor
New York, NY 10001
(914) 749-8200
dboies@bsfllp.com

Hsiao (Mark) C. Mao (*pro hac vice* forthcoming)
BOIES SCHILLER FLEXNER LLP
44 Montgomery Street
41st Floor
San Francisco, CA 94104
(415) 293-6800
mmao@bsfllp.com

James P. Denvir (*pro hac vice* forthcoming)
Michael S. Mitchell (*pro hac vice* forthcoming)

BOIES SCHILLER FLEXNER LLP
1401 New York Avenue, NW
Washington, DC 20005
(202)-237-2727
jdenvir@bsfllp.com
mmitchell@bsfllp.com

Counsel for Plaintiff Delta Air Lines, Inc.