

CAUSE NO. 25-BC03A-0012

GOSECURE, INC.,	§	IN THE BUSINESS COURT OF TEXAS
	§	
<i>Plaintiff,</i>	§	
	§	
v.	§	THIRD DIVISION
	§	
CROWDSTRIKE, INC. and	§	
CROWDSTRIKE HOLDINGS, INC.	§	
	§	
<i>Defendants.</i>	§	TRAVIS COUNTY, TEXAS

PLAINTIFF’S ORIGINAL PETITION

Plaintiff GoSecure, Inc. (“GoSecure”) files this Original Petition against Defendants CrowdStrike, Inc. and CrowdStrike Holdings, Inc. (“CrowdStrike”) and for causes of action would show the following:

INTRODUCTION

1. GoSecure was founded in 2004 with the goal of revolutionizing the cybersecurity industry. At a time when other cybersecurity companies were focused on refining ineffective security strategies focused on protecting the perimeter of computer networks or defending computers against previously identified threats using static approaches, GoSecure recognized that evolving information technology (IT) security environments demanded more capable, rapid, real-time and proactive means to identify, understand, and defend against increasingly sophisticated threats.

2. While others were floundering with obsolete methods, GoSecure focused instead on the importance of developing critical endpoint security technology to ensure that each device connected to a network is protected. Unlike traditional security systems that only protect the perimeter, or common antivirus systems that require constant updating to ensure the software is

patched to block known threats, GoSecure developed an agile approach focused on monitoring activity and detecting threats on the endpoints that constitute the entry points for the many modern security threats.

3. GoSecure's revolutionary approach provided users visibility and highly-detailed insight into activity unfolding on their computing assets. Instead of requiring users to constantly update their antivirus software to receive patches, which are time-consuming and limited to addressing recently discovered and identifiable threats, GoSecure developed technology that preempts new threats, even those that have not previously been identified. By using behavioral analysis to identify and track previously unidentified threats, GoSecure's technologies improved the security of networks while simultaneously improving visibility on evolving threats, thereby allowing users to efficiently monitor and address security issues.

4. GoSecure's ability to monitor, detect, and respond to threats on endpoints connected to a network, while commonplace now, was a pipe dream when GoSecure developed it. GoSecure ignored the naysayers and bucked the trend to develop a platform that can monitor and respond to relevant activity on their endpoint devices. And GoSecure's technology quickly showed its value. Clients marveled at how quickly and illustratively GoSecure's platform could identify security threats, including threats that had not been caught by perimeter security or conventional anti-virus software.

5. Like other small startup companies, GoSecure sought partners and funding to help support the development of revolutionary technologies that would change the world of cybersecurity and help customers of all sizes protect themselves against cyberattacks that were expanding in number and increasing in sophistication.

6. Enter Mr. Dmitri Alperovitch and Mr. George Kurtz, two individuals who founded CrowdStrike, and who recognized early on the revolutionary nature of GoSecure's cybersecurity solutions. Feigning interest in helping GoSecure promote its technology and business goals, Mr. Alperovitch gained access to confidential information about GoSecure's technologies. Mr. Alperovitch even joined GoSecure's Board of Directors to act as the liaison between the Board and the company's engineering and development team. In that role, Mr. Alperovitch convinced GoSecure to hire Mr. Jeremy Gould so that Mr. Gould could obtain unfettered access to GoSecure's most valuable and confidential research and development.

7. Unbeknownst to GoSecure, Mr. Alperovitch and Mr. Gould were conspiring in an unlawful scheme to emulate GoSecure's highly valuable technology to benefit GoSecure's competitor, CrowdStrike. But CrowdStrike worked hard to cover its tracks. It was not until July 2024, when CrowdStrike suffered a well-publicized technical outage that affected millions of computers around the world and inflicted billions of dollars in losses for CrowdStrike's customers, that GoSecure was finally able to discover some of the hidden ways that CrowdStrike has misappropriated GoSecure's trade secrets and confidential information in its flagship Falcon Platform. These recent revelations show how CrowdStrike, with the help of Messrs. Gould and Alperovitch, leveraged GoSecure's trade secrets and confidential information to obtain a massive head start and leapfrog ahead of the competition by passing off as its own what it took GoSecure years to develop, thereby forcing GoSecure to compete against its own technology.

8. After discovering CrowdStrike's illegal activity, GoSecure promptly filed a lawsuit in California state court in November 2024, asserting causes of action for trade secret misappropriation against CrowdStrike and breach of contract against Mr. Gould. From day one, CrowdStrike stonewalled—refusing to participate in discovery at all unless compelled by court

order, knowing full well the California court's crowded docket would delay resolution of any such motion for nearly a year. Indeed, after nearly nine months of litigation in California, CrowdStrike had not produced a single document or substantively responded to a single interrogatory. Faced with CrowdStrike's calculated and absolute refusal to provide any discovery, GoSecure dismissed the California action without prejudice. GoSecure now brings these claims in Austin—CrowdStrike's "home court"—to obtain swift relief.

DISCOVERY CONTROL PLAN AND RULE 47 STATEMENT OF RELIEF

9. GoSecure intends that discovery be conducted under a Level 3 discovery control plan in accordance with Texas Rule of Civil Procedure 190.4.

10. GoSecure seeks monetary relief of over \$1,000,000 and non-monetary relief.

PARTIES

11. Plaintiff GoSecure, Inc. is a corporation organized and existing under the laws of the State of Delaware with its principal place of business in San Diego, California.

12. GoSecure was founded in 2004 and is one of the world's innovators in Endpoint Detection and Response (EDR), which allows companies of all sizes to identify, mitigate, and respond to cybersecurity threats before they can compromise sensitive data or business operations.

13. GoSecure's predecessor company, NeuralIQ, was founded in 2004 and relaunched as CounterTack in 2011. CounterTack then acquired GoSecure in 2018, and the newly merged company became GoSecure. GoSecure owns all rights and title to any and all property and/or rights previously possessed by NeuralIQ and CounterTack. GoSecure, CounterTack, and NeuralIQ are referred to herein as GoSecure.

14. GoSecure has launched multiple cybersecurity products that incorporate its highly valuable and secret information, including for example, the GoSecure Titan® Platform. GoSecure

provides its products to customers who operate throughout the United States and Canada, including within the state of Texas. GoSecure was recently declared by JMP Securities as one of the Elite 80 Hottest Privately Held Companies.

15. On information and belief, Defendant CrowdStrike Holdings, Inc. is a Delaware corporation with its principal executive office in Austin, Texas. On information and belief, Defendant CrowdStrike Holdings, Inc. is the parent of, and directly and wholly owns, Defendant CrowdStrike, Inc. Defendant CrowdStrike Holdings, Inc. may be served with process at 206 E 9th Street, Suite 1400 Austin, Texas 78701, or wherever else it may be found.

16. On information and belief, Defendant CrowdStrike, Inc. is a Delaware corporation with its current principal place of business located in Austin, Texas. Defendant CrowdStrike, Inc. may be served with process at 206 E 9th Street, Suite 1400 Austin, Texas 78701, or wherever else it may be found.

JURISDICTION AND VENUE

17. This Court has jurisdiction over this matter under the laws of the State of Texas, including Chapter 25A of the Texas Government Code, which governs the Texas Business Courts.

18. More specifically, this Court has jurisdiction over this matter under TEX. GOV. CODE § 25A.004(b)(3) because this is an action in which GoSecure is asserting a claim under trade regulation law against Defendants, who are organizations, and the damages sought are within the jurisdictional limits of the Court. GoSecure seeks monetary relief over \$5,000,000 exclusive of interest, statutory damages, exemplary damages, penalties, fees and costs, and non-monetary injunctive relief.

19. This Court has personal jurisdiction over CrowdStrike because, inter alia, CrowdStrike does business in Texas and is headquartered in Texas. *See* TEX. CIV. PRAC. & REM.

CODE § 17.042. CrowdStrike has purposely availed itself of doing business in the state of Texas, and this suit arises out of or relates to CrowdStrike's contacts in the state. Additionally, the exercise of personal jurisdiction over CrowdStrike would not offend traditional notions of fair play and substantial justice.

20. Venue is proper in this Division of the Business Court because CrowdStrike maintains its principal place of business in Travis County, and a substantial part of the events and omissions giving rise to these claims occurred within the Austin area, including Travis County. For example, CrowdStrike has been headquartered at 206 E 9th Street, Suite 1400, Austin, Texas since 2021, including when GoSecure discovered CrowdStrike's misappropriation in 2024. CrowdStrike has advertised that Austin is "CrowdStrike's largest office in the U.S." and, on information and belief, it employs hundreds of individuals there. As discussed in greater detail below, CrowdStrike engineers in Austin have been improperly using GoSecure's trade secrets and confidential information to develop its Falcon Platform for years.

FACTS

I. GoSecure Develops Novel Technologies to Protect Customers from Cyberattacks

21. GoSecure is a privately held company incorporated in 2004. From day one, GoSecure's purpose has been to develop and commercialize products and services that protect customers from novel cyberattacks, including attacks that have not been previously identified and for which there may be no other available defense. GoSecure currently provides first class Endpoint Detection and Response ("EDR") products and services to customers, including through its Titan® Platform. The Titan® Platform and GoSecure's other products and services rely on proprietary techniques developed by GoSecure, including its highly valuable and confidential trade secrets.

22. At the time of GoSecure's founding, the data security industry was struggling to keep up with evolving threats. GoSecure was the first to recognize that the threat prevention strategies that were available at the time were quickly becoming obsolete, which left companies of all sizes in a continuous state of compromise. By relying on firewalls that primarily focused on protecting a network's perimeter or intrusion detection systems ("IDS") and intrusion protection systems ("IPS") that relied on a binary approach that utilized static signatures libraries to identify software that had previously been diagnosed as malware, legacy security systems were fast becoming obsolete. These systems were inherently limited, either because they could not respond to threats that made it past the perimeter or were predicated on the use of a limited library of known signatures that could react only to previously identified malware. At a time when even the most sophisticated security systems could not keep up with rapid advancements in attack methodology, GoSecure conceptualized a revolutionary method that maximized security while optimizing performance.

23. More specifically, GoSecure recognized that as attacks became more sophisticated and numerous, conventional firewalls and antivirus software would no longer be able to keep up with the evolving and increasingly sophisticated attacks on a computer network, which became increasingly difficult to manage as the number of access points to a computer network expanded. In response, GoSecure developed innovative proprietary techniques to defend against increasingly sophisticated cyberattacks and quickly became the pioneer for EDR technology that can identify malicious behavior on a computer system, even after harmful vectors are able to evade perimeter security technologies and traditional antivirus software. This included, for example, strategies for gathering better intelligence and data to develop countermeasures to defend against unknown or

unaddressed vulnerabilities, against which conventional IDS/IPS solutions and traditional anti-virus systems were ineffective.

24. GoSecure is the owner of highly valuable and secret methods, techniques, assumptions, information, and data that have not been publicly disclosed and were developed at GoSecure over years of intensive and expensive development. These trade secrets have helped GoSecure develop products that enable organizations of all sizes to identify, assess, and quickly respond to advanced persistent and targeted attacks in order to arm defenders against attackers and stop advanced threats that could affect an organization on an enterprise-wide basis.

II. GoSecure's Asserted Trade Secrets and Confidential Information

25. GoSecure is the owner of highly valuable, proprietary, and secret source code, algorithms, architecture, technical specifications, product roadmaps, planning documents, and know-how for (i) compiling and analyzing substantial amounts of data reflecting how activity on an endpoint device can be used to perform threat detection and response; (ii) developing proprietary strategies to collect, filter, and analyze that data in “kernel mode”; and (iii) analyzing that data to, *inter alia*, identify potential threats, and alert other endpoints to the same (the “Asserted Trade Secrets”).

26. The Asserted Trade Secrets support significant aspects of the core functionality of GoSecure's cybersecurity products. These include in particular GoSecure's products relating to endpoint detection and response, such as GoSecure's Titan® Platform and its predecessors. As described below, the Asserted Trade Secrets are secret and not commonly known. In addition, GoSecure has taken reasonable measures under the circumstances to protect the secrecy of the Asserted Trade Secrets, which obtain independent economic value because they are secret, as

reflected in the fact that they have helped GoSecure secure and maintain hundreds of satisfied clients.

27. The development of GoSecure's Asserted Trade Secrets spanned multiple years and required substantial resources. GoSecure's engineers recognized more than a decade ago that rapid evolutions in malware required taking a new approach to detecting and responding to threats that can evade conventional anti-malware software to surreptitiously access networks through an increasing number of access points. To address these issues, GoSecure's new approach required: (i) compiling and analyzing substantial amounts of data reflecting how activity on an endpoint device can be used to perform threat detection and response; and (ii) developing proprietary strategies to collect, filter, and analyze that data. While the techniques and compilations of data underlying this approach comprise GoSecure's trade secrets, the conclusions GoSecure was able to reach from analyzing that data, and GoSecure's methods and strategies to improve its products based on those conclusions, also constitute highly valuable trade secrets that could (and in CrowdStrike's case, did) provide GoSecure's competitors a significant head start in developing their own copycat products.

28. GoSecure's Asserted Trade Secrets enable, among other things, the use of a security agent to monitor a computer's activity by collecting data on an endpoint device and implementing an architecture that ensures the agent is readily deployable and functional. For example, to effectively perform its operations, GoSecure designed a proprietary security agent that operates in "kernel mode," which is a privileged level of a computer's operating system that provides direct access to the computer's hardware and system resources. By operating in kernel mode, GoSecure's security agents can monitor and respond to low-level system activities that are not detectable in "user mode," including operations related to data encryption on which users rely to

protect information and are thus capable of bypassing conventional anti-malware systems. In other words, by developing trade secrets that enabled GoSecure to monitor behavior at the core operating system layer, GoSecure was able to develop products that did not simply analyze surface-level behaviors but detected the previously undetectable.

29. But operating in kernel mode raises challenges that GoSecure was able to resolve using its trade secrets. For example, because kernel mode operation exists at the core of a computer's operating system, even minor bugs in drivers that operate in kernel mode can lead to significant system-wide crashes. In addition, security agents operating in kernel mode are exposed to voluminous amounts of raw activity data, much of which is benign, but the analysis of which can overload a security system, reduce the computer's performance, and increase the risk of security breaches given the sheer volume of data. GoSecure's paradigm-shifting trade secrets allowed GoSecure to protect endpoint devices while navigating the operating system in a way that did not result in a system crash or noticeably degrade system performance.

30. GoSecure developed secret techniques to deal with these challenges, which was a Herculean task because of the sheer volume of traffic within the kernel, making it difficult to develop code that could gather relevant data in kernel mode without causing the operating system to crash or slow to a crawl. GoSecure's secret and highly valuable implementation of its kernel-mode security agent overcame these (and other) issues.

31. Stated differently, GoSecure's trade secrets, some of which are embodied in the proprietary and confidential source code GoSecure was developing during Mr. Alperovitch and Mr. Gould's tenure at the company, allow GoSecure to collect, parse, filter, and package raw activity data into manageable parcels, analyze that data to generate useful insights, share those

insights to bolster defenses to constantly-evolving attacks, and provide users with interactive feedback regarding this end-to-end analysis.

32. GoSecure's trade secrets were being developed at GoSecure while Mr. Alperovitch and Mr. Gould were working for the company and had access to the company's research and development information, including valuable and highly confidential planning and research documents, the entirety of the company's source code, and detailed technical information gleaned from meetings with the GoSecure development team. These trade secrets allowed GoSecure to turn raw data into actionable insights that can be used to protect computer systems against more sophisticated cyberattacks while allowing GoSecure to become one of the only security companies that could offer real-time threat detection, intelligent malware analysis, continuous activity capture, and comprehensive system inspection.

33. Given the highly valuable and confidential nature of GoSecure's Asserted Trade Secrets, GoSecure employs numerous measures to control and limit access to its trade secret information and to protect against the theft or misuse of that information, as described below.

a. GoSecure employees are required to sign GoSecure's Proprietary Information and Invention Agreement ("PIIA"), pursuant to which they agree to protect and not to disclose GoSecure's confidential information. For example, Mr. Gould agreed, pursuant to the PIIA, "to hold in strictest confidence, and not to use, except for the benefit of the Company, except to the extent necessary to perform [Mr. Gould's] obligations to the Company" and not to "disclose to any person, firm, corporation or other entity without written authorization of the Board of Directors of the Company [] any Confidential Information of the Company which [he] obtain[ed] or create[d]." GoSecure's PIIA also required that, at the time of termination of his relationship with GoSecure, Mr. Gould

“deliver to the Company (and [] not keep in [his] possession, recreate or deliver to anyone else) any and all devices, records, data, notes, reports, proposals, lists, correspondence, specifications, drawings, blueprints, sketches, laboratory notebooks, materials, flow charts, equipment, other documents or property, or reproductions of any of the aforementioned items developed by” Mr. Gould pursuant to his relationship with GoSecure “or otherwise belonging to the Company, its successors or assigns.” On information and belief, Mr. Gould willfully breached these contractual obligations.

b. GoSecure further requires departing employees to participate in an exit process and to confirm that they have been provided access to GoSecure’s proprietary and trade secret information, have returned all such information to GoSecure upon departure, and have not maintained access to or copies of any digital or hard copy record of GoSecure.

c. GoSecure follows a principle of least privilege that limits access and sharing of confidential information to only those who need to know the information as part of the ordinary course of their business.

d. GoSecure’s proprietary and trade secret information is stored on a secure server and only certain GoSecure employees have access to such servers and databases. Access to these servers and databases is on a “need to know” basis and employees must be approved to obtain such access.

e. GoSecure also implements additional security measures to safeguard and protect sensitive information, including access restrictions, authentication, password protection, encryption, and physical protections.

f. GoSecure's systems and software are designed to prevent hacking or reverse engineering, and the company's systems are protected from external and internal cybersecurity threats.

g. GoSecure maintains secure offices, workspaces, and facilities and has controlled access into its buildings.

34. GoSecure's Asserted Trade Secrets also have substantial independent economic value and have helped GoSecure gain traction with key potential customers who also recognized the value GoSecure brings to the table. Industry stakeholders have recognized the value of GoSecure's products, and the trade secrets on which they rely, including by bestowing more than a dozen prestigious awards on GoSecure. Among the company's many accolades, GoSecure was named a Gartner Cool Vendor in 2014. In 2015, CRN named the company's solutions on their list of the year's 10 coolest network security products. In 2016, GoSecure was given a SANS Best of Award for Endpoint Detection and Response. And in 2017, GoSecure's patented Digital DNA technology was awarded a 5-star review by SC Media, and GoSecure was named to the JMP Securities Super 60 list of the hottest privately held internet security, network and storage companies four years in a row. In addition, the value of the Asserted Trade Secrets is reflected in the substantial unjust enrichment CrowdStrike has received by improperly using them.

III. CrowdStrike Seeks Out GoSecure's Highly Valuable Trade Secrets And Confidential Information

35. Like so many startup companies working to commercialize their innovative technologies, GoSecure sought investment from venture capitalists and sought out talented, knowledgeable individuals to work for GoSecure.

36. On or around September 20, 2011, GoSecure was introduced to Mr. Dmitri Alperovitch, who was then working at McAfee. Following that introduction, Mr. Alperovitch

expressed deep interest in GoSecure's technology, claiming that GoSecure was an extremely interesting opportunity and very relevant technology for the evolving cyber threat environment. Just a couple months later, around November 2011, Mr. Alperovitch began serving as a member of GoSecure's Board of Directors after signing a confidentiality agreement with GoSecure on November 4, 2011. Mr. Alperovitch held that position through May 2012, actively carving out a role as a technical liaison between GoSecure's Board and the company's engineering team. As part of that role, Mr. Alperovitch assumed responsibility for gathering substantial amounts of highly sensitive data from the company's engineering team under the guise of distilling that technical information into terms that non-technical members of the Board would understand.

37. While on the Board, Mr. Alperovitch recruited Mr. Gould to work at GoSecure as a senior engineer. After agreeing to maintain the confidentiality of GoSecure's confidential information pursuant to his employment agreement, Mr. Gould engaged with GoSecure's engineering team and received access to nearly all of GoSecure's research and development information, including all of GoSecure's confidential source code and other data, information, strategies, and methods that form the basis of GoSecure's Asserted Trade Secrets. During his time at GoSecure, Mr. Gould had access to GoSecure's entire repository of source code, including as reflected in logs of commits he made.

38. Mr. Alperovitch and Mr. Gould had access to GoSecure's most valuable and confidential information when GoSecure was at the forefront of the market and became privy to GoSecure's plans to develop user-friendly cybersecurity products that relied on GoSecure's trade secrets and confidential information.

39. Unbeknownst to GoSecure, Mr. Alperovitch and Mr. Kurtz had founded a new company called CrowdStrike to provide offerings that would misappropriate GoSecure's

technology. On or around February 22, 2012, Mr. Alperovitch informed GoSecure's CEO, Neal Creighton, that he and Mr. Kurtz had launched their new company—CrowdStrike. Then, in or around March 2012, while he was still a member of GoSecure's Board, Mr. Alperovitch recruited Mr. Gould to leave GoSecure and join CrowdStrike so that he could, on information and belief, work on CrowdStrike's copycat initiatives and products to unfairly compete against GoSecure. It was not until months later, in or around May 2012, that Mr. Alperovitch stepped down from the Board.

40. When Mr. Gould left GoSecure, GoSecure conducted an exit interview with Mr. Gould to confirm that he had been provided access to GoSecure's proprietary and trade secret information, had returned all such information to GoSecure upon departure, and had not maintained access to or copies of any digital or hard copy record of GoSecure, all consistent with GoSecure's standard procedure with departing employees. Mr. Gould indicated that he was unhappy with his compensation package but assured GoSecure that he would respect the confidentiality provisions in his employment agreement. GoSecure relied on Mr. Gould's assurances because Mr. Gould was a senior software engineer who was well-versed in codes of conduct in the industry. Indeed, despite coming to GoSecure directly from McAfee, Mr. Gould never attempted to divulge any confidential McAfee information to GoSecure.

41. When Mr. Alperovitch left GoSecure, Mr. Creighton met with Mr. Alperovitch to remind him of his fiduciary and contractual duty to the company to maintain confidentiality of GoSecure's trade secrets. In response, Mr. Alperovitch affirmatively represented to Mr. Creighton that there was no misuse of GoSecure's trade secret information at CrowdStrike and assured him that there would not be any such misuse in the future. Based on Mr. Alperovitch's representations, Mr. Creighton believed that Mr. Alperovitch and Mr. Gould would not use or divulge GoSecure's

confidential information to CrowdStrike or anyone else. Mr. Creighton had spent months getting to know Mr. Alperovitch and, in addition to their personal relationship, reasonably put stock in Mr. Alperovitch's reputation in the cybersecurity industry as a trustworthy individual. Mr. Creighton left his meeting with Mr. Alperovitch on good terms and reasonably believed Mr. Alperovitch would honor his legal commitments to GoSecure.

42. Over the ensuing decade-plus, GoSecure monitored public information about CrowdStrike's Falcon Platform but had no reason to suspect that either Mr. Gould or Mr. Alperovitch had been untruthful or that CrowdStrike was misusing GoSecure's trade secrets to develop a product, as opposed to having developed its own EDR solution. As a cybersecurity company, CrowdStrike was especially adept at disguising the operation of its Falcon Platform. Indeed, if it were possible to figure out the intricate details of how CrowdStrike's Falcon Platform worked by reverse engineering, hackers would have no problem circumventing it.

43. Moreover, even if GoSecure reasonably could have detected CrowdStrike's misappropriation through analysis of CrowdStrike's product (it could not), GoSecure would have been prohibited from doing so because CrowdStrike's Software Terms of Use specifically provide that users of its products may not "reverse engineer, decompile, disassemble or otherwise attempt to derive the source code for the Software," which is expressly defined to include the "Falcon Sensor." CrowdStrike has even previously initiated litigation based on its assertion that "use of the Falcon Platform for comparative testing through a CrowdStrike customer violated CrowdStrike's [sic] standard customer Terms and Conditions of service." *CrowdStrike, Inc. v. NSS Labs, Inc.*, No. 17-cv-146 (D. Del. 2017), Dkt. 35 ¶ 44.

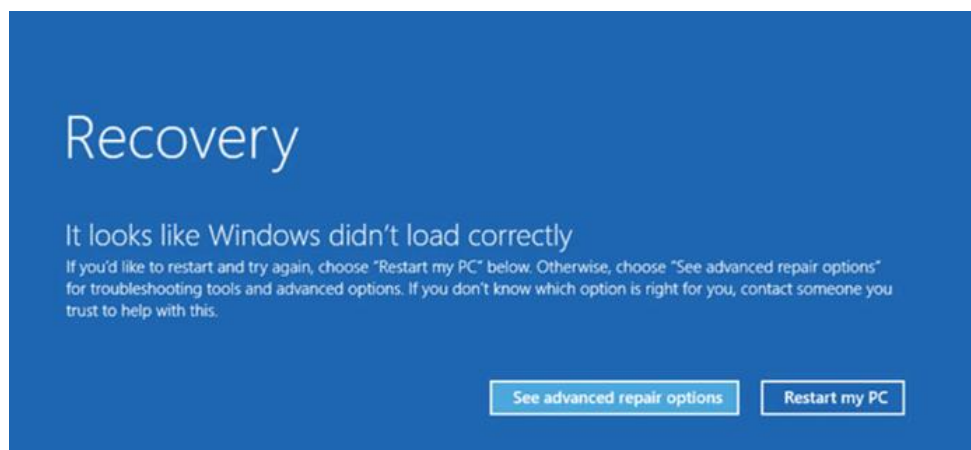
44. At CrowdStrike as its Chief Technology Officer and in collaboration with Mr. Gould until 2020, Mr. Alperovitch, on information and belief, was tasked with overseeing

technical operations, including those related to the design and development of the Falcon Platform. Mr. Gould worked at CrowdStrike as a Senior Cloud Engineer from March 2012 until February 2014, and again from October 2017 until April 2022 as a Senior Software Engineer, during which time he too would have been deeply involved with designing and developing CrowdStrike's Falcon Platform.

45. On information and belief, Mr. Alperovitch, Mr. Gould, and CrowdStrike intentionally misled GoSecure, all the while improperly misappropriating GoSecure's trade secrets without GoSecure's knowledge. GoSecure reasonably expected that Mr. Alperovitch and Mr. Gould would comply with their confidentiality obligations to GoSecure when they left. GoSecure relied on Mr. Alperovitch's repeated assurances that CrowdStrike would not misappropriate GoSecure's trade secret information. But unbeknownst to GoSecure, CrowdStrike had in fact misappropriated GoSecure's trade secrets and confidential and proprietary information and unlawfully used that information to develop CrowdStrike's competing technologies.

IV. GoSecure Discovers CrowdStrike's Misappropriation

46. On July 19, 2024, millions of computer users around the world were confronted with an error message, written across a "Blue Screen of Death" ("BSOD") that noted that the Windows operating system on their computers had failed to load correctly.



47. News outlets across the globe began reporting on this “massive, far-reaching and sudden”¹ global outage that “disrupted operations across industries such as banks, hospitals and 911 call centers, plus grounded flights and hampered public transit systems.”² The global outage impacted “millions of users” and “touched almost every industry.”³ Experts referred to the catastrophe as “the largest IT outage of all time, and one estimate suggested the incident will cost U.S. Fortune 500 companies \$5.4 billion in total direct financial loss.”⁴ Within hours, “[m]ore than 2,000 flights originating or landing in the U.S. were canceled ... and more than twice that number were delayed.”⁵ As one internet security analyst remarked: “[t]his is basically what we were all worried about with Y2K, except it’s actually happened this time.”⁶

48. By 11:30 a.m. EDT on the day of the outage, the Cybersecurity and Infrastructure Security Agency, a division of the U.S. Department of Homeland Security, acknowledged that it was “aware of the widespread outage affecting Microsoft Windows hosts due to an issue with a recent CrowdStrike update.”⁷ CrowdStrike issued a press release confirming that it was “aware of reports of crashes on Windows hosts related to the Falcon Sensor,”⁸ which provides the data on which the Falcon Platform runs.

¹ <https://www.npr.org/2024/07/19/g-s1-12222/microsoft-outage-banks-airlines-broadcasters>

² <https://www.usatoday.com/story/money/2024/07/19/global-outage-communications-systems/74465953007/>

³ <https://www.wsj.com/tech/microsoft-reports-major-service-outage-affecting-users-worldwide-328a2f40>

⁴ <https://www.crn.com/news/security/2024/crowdstrike-microsoft-s-windows-kernel-update-process-was-followed>

⁵ <https://www.npr.org/2024/07/19/g-s1-12222/microsoft-outage-banks-airlines-broadcasters>

⁶ *Id.*

⁷ <https://www.cisa.gov/news-events/alerts/2024/07/19/widespread-it-outage-due-crowdstrike-update>

⁸ <https://www.crowdstrike.com/wp-content/uploads/2024/07/Tech-Alert-Windows-crashes-related-to-Falcon-Sensor-2024-07-19.pdf>

49. In the ensuing days and weeks, white-hat investigators around the world, and in particular China, began analyzing the BSOD event and publicly disclosing—for the benefit of the community—findings that provided new insight into the functionality of CrowdStrike’s Falcon Platform. GoSecure was closely monitoring these disclosures because GoSecure regularly monitors news pertaining to the cybersecurity industry. In the weeks after the BSOD event, GoSecure’s employees read different analyses to understand whether the update that caused the BSOD event could have any bearing on GoSecure’s customers or their systems.

50. Among those analyses, an August 2, 2024 analysis of a crash dump file (which was only available thanks to the outage) by Qihoo 360, a Chinese cybersecurity company, revealed that: (1) the BSOD event was caused by a read out-of-bounds access violation in the CSagent driver that created a null point exception; (2) the csagent.sys module is registered as a file system filter driver commonly used by anti-malware agents to receive notifications about file operations such as the creation or modification of a file; and (3) the File System filter driver API allows the driver to receive a call when named pipe activity (e.g., named pipe creation) occurs on the system that could enable the detection of malicious behavior. GoSecure obtained a translation of the 360 report shortly thereafter and, upon reading it, learned for the first time that CrowdStrike’s Falcon Platform had ripped off GoSecure. The original version of the report is available here: <https://mp.weixin.qq.com/s/uD7mhzyRSX1dTW-TMg4UhQ>.

51. The information in these public post-mortem analyses of the BSOD event was not previously available to GoSecure. The information showed, for the first time, that CrowdStrike built its Falcon Platform using illicitly obtained trade secrets from GoSecure. More specifically, analysis of the crash dump and csagent.sys files related to the BSOD event, along with CrowdStrike’s own statements as it attempted to perform damage control in the wake of the

catastrophic outage, showed that the end-to-end architecture underlying CrowdStrike's Falcon Platform relies on GoSecure's trade secrets.

52. Prior to the once-in-a-lifetime BSOD event, it would have been impossible for GoSecure to have investigated CrowdStrike's Falcon Platform to the level of detail required to suspect misappropriation. CrowdStrike is a sophisticated cybersecurity company whose entire existence is predicated on its ability to prevent attackers from accessing sensitive information, and its products make it impossible to detect what is going on from the outside in the absence of a global catastrophe.

53. Prior to the outage, CrowdStrike had publicly promoted its Falcon Platform's ability to update its detection logic and respond to emerging threats quickly. However, CrowdStrike had uniformly presented these updates as being restricted to user-mode data or scanning policies (e.g., dynamic signature and/or behavior-based rule updates). But the very fact that the outage occurred confirms that the "updates" CrowdStrike provides to its sensors (which CrowdStrike refers to as "Rapid Response Content") impact CrowdStrike's sensor at a deep technical level, which no one suspected before the outage. The fact that the outage occurred not only helped reveal CrowdStrike's misappropriation; it also demonstrated that cutting corners is part of CrowdStrike's culture. Rather than subjecting the Rapid Response Content to the full-scale validation typically required for any modification that might impact how a driver operates in kernel-mode, CrowdStrike relied on simple regular expression ("regex") and array-based parsing without full verification of the logic paths implicated by the update.

54. In other words, information that was not previously available, but that became available in July 2024—thanks to a once in a generation computer crash—finally gave GoSecure reason to suspect that CrowdStrike's Falcon Platform uses the same proprietary and secret methods

developed and used by GoSecure, all of which constitute information CrowdStrike and its founding employees could not have obtained from other sources except GoSecure, and without which CrowdStrike could not have independently developed essentially the same technological solution as is now apparent.

55. These public disclosures finally provided insight into how CrowdStrike was able to launch products that effectively competed with GoSecure's core offerings shortly after CrowdStrike's founding, when it took numerous skilled engineers at GoSecure years of research, implementation, and iteration to develop the same technology. GoSecure reasonably relied on Mr. Gould's assurances that he would comply with the legal obligations set forth in his employment agreement as well as Mr. Alperovitch's representation to Mr. Creighton that neither he nor Mr. Gould would disclose GoSecure's confidential or trade secret information and/or that CrowdStrike would not misappropriate any trade secrets. Without the BSOD event in July 2024 and the ensuing analysis by white-hat investigators, GoSecure would not have discovered that CrowdStrike had acted in concert with Mr. Alperovitch and Mr. Gould to misappropriate GoSecure's highly valuable trade secrets.

CAUSES OF ACTION

I. COUNT I – Misappropriation of Trade Secrets Under the Texas Uniform Trade Secrets Act ("TUTSA")

56. GoSecure realleges and incorporates by reference the allegations contained in each of the foregoing paragraphs as if fully set forth herein.

57. GoSecure is the sole and exclusive owner of confidential trade secret information, including, but not limited to, GoSecure's proprietary source code, algorithms, architecture, and know-how that support GoSecure's cybersecurity products relating to endpoint monitoring, threat

detection, and response, including GoSecure's Titan Platform and its predecessors. Such information constitutes trade secrets subject to protection under the law.

58. GoSecure's confidential, proprietary, and trade secret information is the result of substantial efforts and resultant expenses by GoSecure and would take a competitor considerable time and effort to duplicate. Accordingly, such information has great value to GoSecure and to its competitors, and GoSecure has taken reasonable measures under the circumstances to protect the secrecy of such trade secrets and confidential and proprietary information, including as described above, and specifically with respect to disclosures made to Mr. Alperovitch and Mr. Gould.

59. GoSecure's trade secrets derive economic value from the fact that such information is not generally known to persons who can obtain economic value from its disclosure or use, outside of GoSecure.

60. As described herein, CrowdStrike has misappropriated GoSecure's trade secrets by acquiring such information through improper means and improperly disclosing and using such information.

61. CrowdStrike has unlawfully used in the past, continues to use in the present, and will continue to use in the future, GoSecure's trade secrets to unlawfully and unfairly compete against GoSecure.

62. As a direct and proximate result of CrowdStrike's willful, malicious, improper, and unlawful misappropriation of GoSecure's confidential trade secret information, GoSecure has suffered and will continue to suffer damages including financial loss, loss of goodwill, loss of customers, loss of the confidentiality of the trade secrets, and other irreparable harm, while CrowdStrike has been unjustly enriched. GoSecure seeks damages including the actual loss caused by the misappropriation and any unjust enrichment resulting from CrowdStrike's

misappropriation. GoSecure also seeks to disgorge and/or impose a constructive trust on all wrongful gains received by CrowdStrike.

63. Because CrowdStrike's misappropriation was willful and malicious, GoSecure is also entitled to recover exemplary damages and attorneys' fees from CrowdStrike in an amount to be determined at trial under TEX. CIV. PRAC. & REM. CODE §§ 134A.004(b) and 134A.005(3). The statutory cap under TEX. CIV. PRAC. & REM. CODE § 41.008(b) is inapplicable because CrowdStrike's conduct is described as the felony of theft in the first degree. TEX. CIV. PRAC. & REM. CODE § 41.008(c)(13).

64. In addition, GoSecure has been and will continue to be irreparably harmed unless CrowdStrike is enjoined under TEX. CIV. PRAC. & REM. CODE § 134A.003 from further use and/or disclosure of GoSecure's confidential trade secret information. Accordingly, GoSecure seeks an injunction preventing CrowdStrike from further using or disclosing GoSecure's confidential trade information. *See* TEX. CIV. PRAC. & REM. CODE § 134A.003(a) ("Actual or threatened misappropriation may be enjoined . . .").

II. COUNT II – Misappropriation of Trade Secrets and Confidential Information Under Texas Common Law

65. GoSecure realleges and incorporates by reference the allegations contained in each of the foregoing paragraphs as if fully set forth herein.

66. GoSecure is the sole and exclusive owner of confidential trade secret information, including, but not limited to, GoSecure's proprietary source code, algorithms, architecture, and know-how that support GoSecure's cybersecurity products relating to endpoint monitoring, threat detection, and response, including GoSecure's Titan Platform and its predecessors.

67. GoSecure's confidential, proprietary, and trade secret information is the result of substantial efforts and resultant expenses by GoSecure and would take a competitor considerable

time and effort to duplicate. Accordingly, such information has great value to GoSecure and to its competitors, and GoSecure took reasonable measures under the circumstances to protect the secrecy of such trade secrets and confidential and proprietary information, including as described above, and specifically with respect to disclosures made to Mr. Alperovitch and Mr. Gould.

68. As described herein, CrowdStrike has misappropriated GoSecure's trade secrets by acquiring such information through improper means and improperly disclosing and using such information.

69. CrowdStrike has unlawfully used in the past, continues to use in the present, and will continue to use in the future, GoSecure's trade secrets to unlawfully and unfairly compete against GoSecure.

70. As a direct and proximate result of CrowdStrike's willful, improper, and unlawful misappropriation of GoSecure's confidential trade secret information, GoSecure has suffered and will continue to suffer financial loss, loss of goodwill, loss of customers, loss of the confidentiality of the trade secrets, and other irreparable harm in an amount to be proven at trial, while CrowdStrike has been unjustly enriched. GoSecure seeks damages including the actual loss caused by the misappropriation and any unjust enrichment resulting from CrowdStrike misappropriation. GoSecure also seeks to disgorge and/or impose a constructive trust on all wrongful gains received by CrowdStrike.

71. Because CrowdStrike acted with malice, GoSecure is entitled to recover exemplary damages from CrowdStrike in an amount to be determined at trial under TEX. CIV. PRAC. & REM. CODE § 41.003(a)(2). The statutory cap under TEX. CIV. PRAC. & REM. CODE § 41.008(b) is inapplicable because CrowdStrike's conduct is described as the felony of theft in the first degree. TEX. CIV. PRAC. & REM. CODE § 41.008(c)(13).

72. In addition, GoSecure has been and will continue to be irreparably harmed unless CrowdStrike is enjoined from further use and/or disclosure of GoSecure's confidential trade secret information. Accordingly, GoSecure seeks injunctive relief to prevent CrowdStrike from further using or disclosing GoSecure's confidential, proprietary, and/or trade secret information.

III. COUNT III – Unfair Competition by Misappropriation

73. GoSecure realleges and incorporates by reference the allegations contained in each of the foregoing paragraphs as if fully set forth herein.

74. CrowdStrike's wrongful conduct constitutes an unlawful act that interfered with GoSecure's ability to conduct its business.

75. CrowdStrike's conduct is independently tortious, illegal, unfair, and contrary to accepted business ethics.

76. Specifically, CrowdStrike misappropriated and used, in competition with GoSecure, GoSecure's trade secrets and/or confidential information, which was created by GoSecure through its expenditure of labor, skill, and money.

77. As a direct and proximate result of CrowdStrike's willful, improper, and unlawful misappropriation of GoSecure's confidential and proprietary information, GoSecure has suffered and will continue to suffer damages in an amount to be proven at trial, while CrowdStrike has been unjustly enriched. GoSecure seeks damages including the actual loss caused by the misappropriation and any unjust enrichment resulting from CrowdStrike's misappropriation. GoSecure also seeks to disgorge and/or impose a constructive trust on all wrongful gains received by CrowdStrike.

78. Because CrowdStrike acted with malice, GoSecure is entitled to recover exemplary damages from CrowdStrike under TEX. CIV. PRAC. & REM. CODE § 41.003(a)(2). The statutory

cap under TEX. CIV. PRAC. & REM. CODE § 41.008(b) is inapplicable because CrowdStrike's conduct is described as the felony of theft in the first degree. TEX. CIV. PRAC. & REM. CODE § 41.008(c)(13).

IV. COUNT IV – Conversion

79. GoSecure realleges and incorporates by reference the allegations contained in the each of the foregoing paragraphs as if fully set forth herein.

80. GoSecure owned, possessed, or had the legal right to immediate possession of its trade secrets and/or confidential and proprietary information to the exclusion of CrowdStrike.

81. CrowdStrike wrongfully exercised dominion or control over GoSecure's property, including GoSecure's confidential and proprietary information and trade secrets, in denial of and/or inconsistent with GoSecure's rights, and has thereby converted GoSecure's property for CrowdStrike's own use.

82. CrowdStrike's improper exercise of dominion and control over GoSecure's property extended both to GoSecure's tangible personal property as well as GoSecure's intangible property, which was merged into tangible property.

83. As a direct and proximate result of CrowdStrike's willful, improper, and unlawful misappropriation of GoSecure's confidential and proprietary information, GoSecure has suffered and will continue to suffer damages in an amount to be proven at trial, while CrowdStrike has been unjustly enriched. GoSecure seeks damages including the actual loss caused by the misappropriation and any unjust enrichment resulting from CrowdStrike's misappropriation. GoSecure also seeks to disgorge and/or impose a constructive trust on all wrongful gains received by CrowdStrike.

84. GoSecure has suffered irreparable harm as a result of CrowdStrike's actions, and GoSecure is entitled to injunctive relief.

85. Because CrowdStrike acted with malice, GoSecure is entitled to recover exemplary damages from CrowdStrike under TEX. CIV. PRAC. & REM. CODE § 41.003(a)(2). The statutory cap under TEX. CIV. PRAC. & REM. CODE § 41.008(b) is inapplicable because CrowdStrike's conduct is described as the felony of theft in the first degree. TEX. CIV. PRAC. & REM. CODE § 41.008(c)(13).

V. COUNT V – Unjust Enrichment

86. GoSecure realleges and incorporates by reference the allegations contained in each of the foregoing paragraphs as if fully set forth herein.

87. CrowdStrike secured a benefit from GoSecure by fraud, duress, and/or taking an undue advantage.

88. CrowdStrike took an undue advantage by wrongfully securing the benefit of GoSecure's confidential, proprietary information and trade secrets and has unlawfully retained the benefit of this information.

89. There is no express contract governing the recovery of GoSecure's confidential, proprietary, and trade secret information from CrowdStrike.

90. As a direct and proximate result of CrowdStrike's willful, improper, and unlawful taking of an undue advantage through misappropriation of GoSecure's confidential, proprietary, and trade secret information, GoSecure has suffered and will continue to suffer damages in an amount to be proven at trial, while CrowdStrike has been unjustly enriched. GoSecure seeks damages including the actual loss caused by the misappropriation and any unjust enrichment

resulting from CrowdStrike's misappropriation. GoSecure also seeks to disgorge and/or impose a constructive trust on all wrongful gains received by CrowdStrike.

91. Because CrowdStrike acted with malice, GoSecure is entitled to recover exemplary damages from CrowdStrike under TEX. CIV. PRAC. & REM. CODE § 41.003(a)(2). The statutory cap under TEX. CIV. PRAC. & REM. CODE § 41.008(b) is inapplicable because CrowdStrike's conduct is described as the felony of theft in the first degree. TEX. CIV. PRAC. & REM. CODE § 41.008(c)(13).

VI. COUNT VI – Permanent Injunction

92. GoSecure realleges and incorporates by reference the allegations contained in each of the foregoing paragraphs as if fully set forth herein.

93. GoSecure requests a permanent injunction issue against CrowdStrike prohibiting CrowdStrike from using and disclosing GoSecure's confidential, proprietary, and trade secret information.

DAMAGES

94. GoSecure realleges and incorporates by reference the allegations contained in each of the foregoing paragraphs as if fully set forth herein.

95. Each of the unlawful acts alleged herein has, in addition to irreparable harm, directly and proximately caused damages to GoSecure. GoSecure has suffered and will continue to suffer direct and consequential actual damages, including without limitation: lost profits, damage to goodwill, loss of the benefits associated with exclusive possession of its property, and additional costs that GoSecure has incurred as a result of CrowdStrike's unlawful conduct.

96. The pecuniary value of the trade secret technologies and information that have been misappropriated by CrowdStrike, which are the fruit of years of development and hundreds of

millions of dollars in investment, is not subject to ready determination but is in any case in excess of \$5,000,000.

97. Because CrowdStrike's actions were willful, malicious, improper, and unlawful, CrowdStrike is also liable for exemplary damages under TEX. CIV. PRAC. & REM. CODE §§ 41.003(a)(2) and 134A.004(b).

ATTORNEYS' FEES

98. GoSecure realleges and incorporates by reference the allegations contained in each of the foregoing paragraphs as if fully set forth herein.

99. GoSecure has retained experienced legal counsel to represent it in this action and has agreed to pay reasonable and necessary attorneys' fees. GoSecure seeks recovery of their reasonable and necessary attorneys' fees pursuant to TEX. CIV. PRAC. & REM. CODE § 134A.005(3) and other applicable law.

CONDITIONS PRECEDENT

100. All conditions precedent to GoSecure's claim for relief have been performed, have occurred, or have otherwise been excused.

RULE 193.7 NOTICE

101. GoSecure hereby gives notice of intention to use items produced by all Parties in discovery at any pretrial proceeding or at trial of this matter, and the authenticity of such items is self-proven pursuant to Rule 193.7 of the Texas Rules of Civil Procedure.

DEMAND FOR JURY TRIAL

102. GoSecure hereby demands a trial by jury under Texas Rule of Civil Procedure 216 and Texas Government Code § 25A.015. Plaintiff is tendering the applicable jury fee to the clerk of the court as required by Texas Rule of Civil Procedure 216.

PRAYER FOR RELIEF

WHEREFORE, GoSecure respectfully prays for relief as follows:

1. Judgment in GoSecure's favor and against CrowdStrike on all causes of action;
2. Actual damages;
3. Exemplary damages, including pursuant to TEX. CIV. PRAC. & REM. CODE §§ 41.003, 134A.004(b), and as otherwise and to the extent provided by law;
4. Pre-judgment interest;
5. Post-judgment interest;
6. Attorneys' fees, including pursuant to TEX. CIV. PRAC. & REM. CODE § 134A.005(3) and as otherwise and to the extent provided by law;
7. An order awarding restitution of the monies CrowdStrike wrongfully acquired by their wrongful and illegal conduct;
8. Preliminary and permanent injunctive relief to prevent use by CrowdStrike of any of the trade secrets belonging to GoSecure or any information, strategies, business methods, or anything else derived from GoSecure's trade secrets;
9. An order requiring CrowdStrike to account for all gains, profits, and advantages derived from their misappropriation of GoSecure's confidential, proprietary, or trade secret information;
10. An order requiring CrowdStrike to disgorge all profits, in the past and in the future, earned from their unlawful conduct;
11. An order that CrowdStrike immediately assign, transfer, and return all right, title, and interest in the GoSecure trade secrets that they misappropriated and all other GoSecure confidential information that was improperly used by CrowdStrike, in all forms and in all manners in which they now exist, whether in electronic form, paper format, or in any other tangible or intangible entitlement or format, so that GoSecure retains all legal and equitable title in its trade secrets and confidential information;
12. An order awarding witness fees and litigation costs in an amount according to Proof;
13. An order awarding costs of suit incurred by GoSecure; and

14. Any further relief available at law or in equity to which GoSecure may be justly entitled and that this Court deems just and proper.

Dated: August 13, 2025

Respectfully submitted,

CLEVELAND | KRIST PLLC

/s/ Timothy Cleveland
Timothy Cleveland
State Bar No. 24055318
Austin H. Krist
State Bar No. 24106170
Lourdes Ortiz
State Bar No. 24134904
303 Camp Craft Rd., Suite 325
West Lake Hills, Texas 78746
(512) 689-8698
tcleveland@clevelandkrist.com
akrist@clevelandkrist.com
lortiz@clevelandkrist.com

CLEARY GOTTlieb STEEN & HAMILTON LLP

/s/ Giri Pathmanaban
S. Giri Pathmanaban (SBN 24074865)
gpathmanaban@cgsh.com
1841 Page Mill Road
Palo Alto, California 94304
Telephone: (650) 815-4100
Fax: (650) 815-4199

Thomas Yeh (*pro hac vice pending*)
tyeh@cgsh.com
650 California St., Suite 2400
San Francisco, California 94108
Telephone: (415) 796-4400
Fax: (415) 796-4499

Clement Naples (*pro hac vice pending*)
cnaples@cgsh.com
One Liberty Plaza
New York, New York 10006
Telephone: (212) 225-2000
Fax: (212) 225-3999

Daniel Todd (SBN 24135014)
dtodd@cgsh.com
2112 Pennsylvania Avenue, NW
Washington, DC 20037
Telephone: (202) 974-1500
Fax: (650) 815-4199

Attorneys for Plaintiff GoSecure, Inc.

Automated Certificate of eService

This automated certificate of service was created by the eFiling system. The filer served this document via email generated by the eFiling system on the date and to the persons listed below. The rules governing certificates of service have not changed. Filers must still provide a certificate of service that complies with all applicable rules.

Lourdes Ortiz on behalf of Tim Cleveland
Bar No. 24055318
lortiz@clevelandkrist.com
Envelope ID: 104344781
Filing Code Description: Petition
Filing Description: Original Petition
Status as of 8/13/2025 4:37 PM CST

Case Contacts

Name	BarNumber	Email	TimestampSubmitted	Status
Austin Krist		akrist@clevelandkrist.com	8/13/2025 4:23:20 PM	NOT SENT
Daniel Todd		dtodd@cgsh.com	8/13/2025 4:23:20 PM	NOT SENT
Clement Naples		cnaples@cgsh.com	8/13/2025 4:23:20 PM	NOT SENT
Thomas Yeh		yeh@cgsh.com	8/13/2025 4:23:20 PM	NOT SENT
Giri Pathmanaban		gpathmanaban@cgsh.com	8/13/2025 4:23:20 PM	NOT SENT
Sarah Prince		sprince@clevelandkrist.com	8/13/2025 4:23:20 PM	NOT SENT
Lourdes Ortiz		lortiz@clevelandkrist.com	8/13/2025 4:23:20 PM	NOT SENT
Timothy Cleveland		tcleveland@clevelandkrist.com	8/13/2025 4:23:20 PM	NOT SENT