IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

St. Jude Medical, Inc., Plaintiff, vs. Muddy Waters Consulting LLC, Muddy Waters Capital LLC, Carson C. Block, MedSec Holdings Ltd., MedSec LLC, Justine Bone and Dr. Hemal M. Nayak, Defendants.	Case No. 16-cv-03002 JURY TRIAL DEMANDED

COMPLAINT

St. Jude Medical, Inc. brings this action for false statements, false advertising, conspiracy and the resultant manipulation of the public markets against defendants (i) Muddy Waters Consulting LLC and Muddy Waters Capital LLC, (ii) MedSec Holdings, Ltd. and MedSec LLC, (iii) Carson C. Block, (iv) Justine Bone and (v) Dr. Hemal M. Nayak (collectively the "Defendants" and each a "Defendant"). Defendants' wrongful conduct conclusively demonstrates a total disregard for the patients whose lives depend on cardiac rhythm management devices and their conduct is indefensible. In further support, St. Jude states as follows:

NATURE OF THE ACTION

1. This action arises from Defendants' intentional, willful and malicious scheme to manipulate the securities markets for their own financial windfall through an unethical and unlawful scheme premised upon falsehoods and misleading statements initially contained in an August 25, 2016 Muddy Waters report concerning St. Jude's implantable cardiac rhythm management devices (also referred to as "CRM Devices"). The report and subsequent written and

oral assertions were willfully and intentionally designed and intended to influence and confuse patients and their doctors, by wrongfully defaming and disparaging St. Jude's lifesaving devices.

2. Defendants undertook their carefully orchestrated scheme with the express intent to interfere with efficient public markets by intentionally disseminating false information in order to depress the value of St. Jude's stock and profit from such depression in value by implementing a short-selling scheme. The sole purpose of this short-selling scheme was to enable Defendants to secure a quick and illegal financial windfall. Defendants purportedly claim they also wanted to inform users and physicians of risks associated with the use of St. Jude's CRM Devices, but this claim is belied by the fact that Muddy Waters had no experience in medical device security and purportedly relied on MedSec and its medical advisor and board member, Dr. Nayak, both of whom procured a financial interest in the short-selling scheme regarding St. Jude's stock value. The actions of each of the Defendants, individually and collectively, blatantly disregard ethical standard practices in the cybersecurity community and FDA Guidance, which call for a legitimately concerned party to first convey any security-related concerns about medical devices to the company itself and/or any relevant government agency or public health authority.

3. The motive for Defendants' approach is revealed in the first two sentences of the Muddy Waters report: "Muddy Waters Capital is short St. Jude Medical, Inc. (STJ US). There is a strong possibility that close to half of STJ's revenue is about to disappear for approximately two years." Thus, Defendants specifically intended to drive down the price of St. Jude's stock, which they had previously sold short. This insidious scheme to try to frighten and confuse patients and doctors by publicly disseminating false and unsubstantiated information in order to gain a financial windfall and thereby cause investors to panic and drive the St. Jude stock price down must be stopped and Defendants must be held accountable so that such activity will not be incentivized and

repeated in the future. Accordingly, the purpose of this action is to hold the Defendants, and each of them, fully accountable for their unlawful and inappropriate statements and scheme.

PARTIES

St. Jude

4. St. Jude Medical, Inc. is a global medical device company committed to transforming the treatment of expensive epidemic diseases. St. Jude Medical, Inc. and its affiliates (collectively "St. Jude") develop, manufacture, and distribute medical devices and services, including cardiac rhythm management medical devices. St. Jude Medical, Inc. is incorporated in the state of Minnesota, and maintains its global headquarters and principal executive offices at One St. Jude Medical Drive, St. Paul, Minnesota, 55117.

Muddy Waters

5. Muddy Waters Capital LLC manages hedge funds through a short-seller driven investment strategy. It was formed in Delaware and has offices in California.

6. Muddy Waters Consulting LLC (collectively with Muddy Waters Capital LLC, "Muddy Waters") is an affiliate of Muddy Waters Capital LLC. It was formed in Delaware.

Block

7. Carson C. Block ("Block") is the founder of, and research director for, Muddy Waters. Block resides in California.

MedSec

8. MedSec Holdings Ltd. claims to engage in cybersecurity research. It has an office in Florida.

9. MedSec LLC (collectively with MedSec Holdings Ltd., "MedSec") is an affiliate of MedSec Holdings Ltd.

Bone

10. Since July 2016, Justine Bone ("Bone") has been chief executive officer of MedSec Holdings Ltd. On information and belief, Bone resides in Florida.

Dr. Nayak

11. Dr. Hemal M. Nayak ("Dr. Nayak") serves as a director and advisor to MedSec. On information and belief, Dr. Nayak resides in Illinois.

12. Because Defendants acted in concert and conspired with each other in their scheme to defame and disparage St. Jude, they are jointly responsible for all misconduct, false and misleading statements, and harms as further set forth below.

JURISDICTION

13. This action arises under, and is brought pursuant to the Lanham Act, 15 U.S.C. § 1125, and also asserts claims for common law defamation and conspiracy, as well as Minnesota's deceptive trade practices act.

14. Subject matter jurisdiction is conferred upon this Court by 15 U.S.C. § 1125, and 28 U.S.C. §§ 1331, 1337, as the action arises under the laws of the United States.

15. Supplemental jurisdiction exists for state law claims pursuant to 28 U.S.C. § 1367.

VENUE

16. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(2), because a substantial part of the events giving rise to St. Jude's claims occurred in this judicial district.

17. To this end, each of the Defendants, both individually and collectively, committed wrongful acts for the purpose of having their consequences felt in Minnesota, where St. Jude resides and where a substantial part of the property that is the subject of the action is situated.

BACKGROUND

St. Jude's Devices

18. CRM Devices, including pacemakers and defibrillators, made by St. Jude save and improve lives every day. Studies have shown that remote monitoring of pacemakers and defibrillators can provide additional information to doctors to help improve patient care, reduce adverse events for patients and reduce mortality. *See* http://www.hrsonline.org/Policy-Payment/Clinical-Guidelines-Documents/Expert-Consensus-on-the-Monitoring-of-Cardiovascular-Implantable-Electronic-Devices/2015-Expert-Consensus-Statement-on-Remote-Interrogation-and-Monitoring-for-CIEDs. As shown throughout this Complaint, Defendants have attempted to scare patients into surrendering these demonstrated benefits by unplugging their St. Jude Merlin@home devices ("Remote Transmitters") based on false and misleading information.

19. As part of its efforts to protect the security of its devices, St. Jude enlists its employee experts and third party experts to assist in designing and testing security measures from its CRM Devices' design to market release and ongoing product enhancement, including software and security updates and regular risk assessment as prescribed by the FDA.

20. St. Jude provides remote automated security updates for Remote Transmitters. These security updates are designed to reach Remote Transmitters that are actively interfacing with patients' implants. Patient identifiable data transferred by St. Jude's Remote Transmitters to Merlin.net are sent over an encrypted channel.

21. Patients who have St. Jude's CRM Devices implanted may have a variety of cardiac conditions, including various cardiac arrhythmias. An arrhythmia is an abnormal heart rhythm that develops when congenital conditions, disease or injury causes the heart's electrical signals to change from normal to abnormal. The abnormal heart rhythm can cause the heart to beat too fast (tachycardia) or too slow (bradycardia) or, in patients with heart failure, inefficiently. Different types of implantable medical devices can be used in the treatment of tachycardia, bradycardia or heart failure as programmed and directed by a doctor. Some types of arrhythmias, such as ventricular fibrillation, a common cause of cardiac arrest, are fatal if not treated quickly. Others, such as atrial fibrillation, can be disabling and lead to stroke.

22. St. Jude and its affiliates design, manufacture and sell a range of medical devices and systems for heart patients, including CRM Devices that treat and manage heart illnesses for a variety of patients. In addition to implantable cardioverter defibrillators ("ICDs") and pacemakers, St. Jude and its affiliates design, make and sell implantable cardiac resynchronization therapy pacemakers ("CRT-Ps"), and implantable cardiac resynchronization therapy defibrillators ("CRT-Ds"), as well as remote monitoring devices that allow pacemakers, ICDs and CRT devices to communicate with doctors without the need for a trip to the doctor's office and thereby reducing the need for in-person office visits.

23. A pacemaker can be implanted and programmed by a doctor to monitor and pace the heart when the patient's native heart rate is too slow. Pacemakers, unlike ICDs, do not have the ability to administer a therapeutic shock to the heart in the event of certain arrhythmias, including ventricular tachycardia or ventricular fibrillation, to restore a normal sinus rhythm. ICDs can be used to both pace the heart and to detect and administer therapy when certain arrhythmias

are detected, all as programmed by a doctor to customize therapy. ICDs, pacemakers, and CRT devices taken together are all CRM Devices.

24. Forty years ago, the U.S. Congress enacted the Medical Device Amendments ("MDA") to the Food, Drug, and Cosmetic Act ("FDCA"). The 1976 law granted the FDA authority to regulate medical devices in a comprehensive federal oversight regime. In enacting the MDA, Congress sought to ensure that medical devices would be readily available to treat patients in need of lifesaving or disability-averting care. Wary of differing state regulation, Congress has generally prohibited non-federal regulation of medical devices by incorporating an express-preemption clause into the MDA. That provision specifies that no state may impose "any requirement" relating to the safety or effectiveness of a medical device that "is different from, or in addition to, any requirement applicable … to the device" under federal law. 21 U.S.C. § 360k(a)(1). In the United States, St. Jude works closely with and is heavily regulated by the FDA in the design, testing, approval and ongoing post-market surveillance of its CRM Devices.

The Rigorous Premarket Approval Process for Class III Devices

25. Under the MDA, the FDA provides different levels of scrutiny depending on the type of device. Devices that "support" or "sustain" human life, or that "present a potential unreasonable risk of illness or injury," are "Class III" devices. Innovative Class III devices, such as the St. Jude CRM Devices at issue here, are subject to "the FDA's strictest regulation." Such devices must win FDA approval *before* they may be brought to market in the United States.

26. The premarket approval ("PMA") process is the most exacting kind of FDA medical device review, including analysis of clinical trial results. In order to approve the device, the FDA's thorough review must find a reasonable assurance of a device's "safety and effectiveness."

27. The FDA rigorously scrutinizes PMA applications. The average PMA application receives over *twelve hundred hours* of analysis. In this analysis, the FDA weighs a device's likely health benefits against the probable risk, if any, of illness or injury. The FDA has the authority and power to seek additional information and to compel manufacturers to make changes before it grants approval allowing commercial sales in the U.S.

The Rigorous Process for Changes to Approved Devices

28. Approval of a PMA application means the FDA generally "forbids" any and all subsequent device alterations that include design specifications, the manufacturing process, labeling, or any other attribute that would affect safety or effectiveness.

29. Only with additional FDA permission may such changes generally occur. The device maker must submit to another round of approval known as a "PMA Supplement." The same rigorous standards of review imposed during the initial PMA approval analysis apply, once again, to the PMA Supplement analysis, though typically without the need for a clinical trial.

30. Per the applicable guidance from the FDA, the FDA also receives from manufacturers Annual Reports for PMA devices where, among other things, changes that do not affect safety and effectiveness are reported and subject to FDA review.

Enforcement of FDA Requirements for Approved Devices

31. The FDA's enforcement authority is extensive *and exclusive*. By law, the FDA's enforcement conduct "shall be by and in the name of the United States." 21 U.S.C. § 337(a). Private citizens may make complaints to the FDA, but only the FDA may act on them. Private plaintiffs cannot sue under the FDCA.

32. The FDA uses its authority to investigate violations of the FDCA. The FDA's breadth of power permits—and encourages—a measured response. The FDA may seek to enjoin, fine, seize products of and/or pursue criminal charges against wrongdoers.

St. Jude Has Been Vigilant in Making Product Changes and Updates

33. Over the years, St. Jude followed applicable protocols for making product changes and updates, including those that have gone through the PMA-Supplement process as well as those implemented through Annual Report notifications. St. Jude has advised the FDA of security and software updates through, among other things, Annual Reports and PMA supplement applications.

34. St. Jude was an early supporter of the FDA's "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" issued on October 2, 2014. St. Jude was a key contributor to the Medical Device Privacy Consortium's Security Risk Assessment Framework for Medical Devices White Paper and has since incorporated a cybersecurity risk assessment as part of the St. Jude Quality System. Cybersecurity risk assessments have been completed and submitted to the FDA for recent new CRM Device product submissions and when there are significant changes to legacy CRM Devices. St. Jude has also been actively engaged in working with the FDA and other industry groups on the "Postmarket Management of Cybersecurity in Medical Devices" FDA guidance issued on January 22, 2016, including workshop participation. Among other things, and contrary to the MedSec and Muddy Waters scheme, the Draft Guidance recommends that a security researcher coordinate and collaborate with the manufacturer and relevant agencies before going public when a security researcher claims to have discovered a real or potential vulnerability.

35. St. Jude has worked with third-party experts, researchers, the FDA, the Department of Homeland Security and regulators in cybersecurity to develop appropriate safeguards for its

data and CRM Devices as part of its product development process and life cycle. Because cybersecurity is part of the St. Jude Quality System, ongoing product enhancement and evaluation includes formal risk assessments and, where appropriate, software updates and security updates to further strengthen St. Jude's products within the dynamic environment for assessing and improving cybersecurity. Specific to software updates and contrary to Defendants' statements that there have been "no significant security improvements since [2013]," St. Jude released seven different security updates alone to Merlin@home since 2013. St. Jude conducts regular risk assessments based on FDA guidance and performs penetration tests using internal and external experts. St. Jude continues to collaborate with industry and governmental organizations to help develop and improve standards and best practices, gain insight on recent trends and take appropriate action.

36. St. Jude's CRM Devices and security have been evaluated and assessed by internal audits and by several independent and third-party organizations and researchers. In particular, Merlin.net has been certified under the EU-US Privacy Shield and the US-Swiss Safe Harbor by St. Jude Internal Audit, comprising annual audits of key security controls, and has been reviewed and accepted by the U.S. Department of Commerce. St. Jude continues to adhere to the European Data Protection requirements by complying with strict privacy and security measures to protect the personal information of Merlin.net patients during transfers of personal information from the European Union to the United States. Since 2009, St. Jude's Merlin.net Patient Care Network ("PCN") has successfully achieved ISO 27001 certification, which includes an annual internal audit and the independent certification of third-party BSI, an internationally accredited management systems certification firm.

37. In addition, the Merlin.net PCN was the first cardiac device monitoring system to be awarded ISO/IEC 27001:2005 certification, a stringent worldwide information security

standard. This certification is audited, updated and current. Additionally, in 2015, St. Jude upgraded its remote monitoring system successfully to ISO 27001:2013 certification. St. Jude has launched programs to achieve a Report on Controls at a Services Organization (SOC2) for Merlin.net, which will be issued by an independent auditor and is also a pilot participant in the Underwriters Laboratories (UL) Cybersecurity Assurance Program.

38. As noted above, St. Jude openly encourages and has posted instructions on the St. Jude internet website (www.sjm.com) for anyone with product security questions to contact the company through a dedicated email at productsecurity@sjm.com. St. Jude also openly asks anyone who believes they have identified a potential cybersecurity vulnerability in a St. Jude product to contact the company at vulnerabilityreporting@sjm.com for further inspection and analysis to best ensure that St. Jude is able to investigate, validate and, if necessary and appropriate, communicate information in the interest of patient safety and develop any warranted security upgrades or software updates.

39. St. Jude's remote monitoring system for CRM Devices, Merlin.net PCN, is an award-winning system designed to improve outcomes for patients with pacemakers, ICDs and CRT devices. With rapid access to their patients' information through the secure Merlin.net PCN website, physicians can remotely monitor and assess patient device data and determine interventions that may be needed. Recent research has shown that remote monitoring can help doctors improve patient care and survival while reducing hospitalizations and health care utilization. *See* HRS ¶ 18 *supra.*

40. In 2008, St. Jude introduced the Merlin@home Remote Transmitter, which allows efficient remote monitoring and additional options for physicians to provide early intervention and

improve health care efficiency. All data transferred by Merlin@home to Merlin.net are transmitted over an encrypted channel.

41. Remote monitoring of cardiac patients has become a best-practice over the past decade. In 2015, the Heart Rhythm Society made remote monitoring the standard of care in its guidelines. *See* HRS ¶ 18 *supra*. St. Jude has pioneered this life-saving capability with the Merlin.net PCN and the Merlin@home patient system.

42. With respect to remote monitoring through use of Merlin@home transmitters, changes to therapeutic parameter settings on patients' devices require use of the in-clinic programming device and cannot be performed by the Merlin@home transmitters. The Remote Transmitter has no native applications with built-in programming capability to make such changes. Operating system access controls protect the Remote Transmitter from unauthorized access, and its lack of built-in programming helps ensure therapy selection is provided only by and as directed by the patient's physician. In addition, the limited wireless range of the 2.45 GHz wake-up function restricts accessibility of communications with the CRM Devices.

43. Over the last several years St. Jude made significant investments in improving the Merlin.net infrastructure, including implementation of full database encryption, implementation of next-generation firewalls, web-application firewalls, security monitoring and response capabilities. St. Jude added features to the Merlin.net application for patients such as two-factor authentication and access logging. St. Jude's cybersecurity efforts are active and ongoing.

THE SHORT-SALE SCHEME OF MUDDY WATERS AND MEDSEC

The Formation of the Scheme and Subsequent Reports

44. The short-sale scheme that emerged publicly on August 25, 2016, purportedly began some 18 months earlier when a group of unknown researchers funded by undisclosed

sources claims to have begun researching various medical devices made by several manufacturers. At some point, the strategy singled out St. Jude and turned toward making money as MedSec was formed. MedSec claims to have brought its "research"—not to St. Jude or even the FDA or U.S. Department of Homeland Security—but directly to Muddy Waters for the purpose of monetizing their claimed work with a hoped-for payday in the stock market. In July 2016, Bone became "CEO" and furthered the conspiracy and has, as shown below, furthered the plan jointly with Muddy Waters to profit from false and misleading information.

45. On August 25, 2016, Muddy Waters disseminated to media channels a document detailing what it claimed were security deficiencies in St Jude's CRM Devices and Remote Transmitters, including cardiac pacemakers (the "Muddy Waters Report") expressly based on the work of MedSec. That morning, Block appeared on Bloomberg TV to promote the Muddy Waters Report and Muddy Waters's short position in St. Jude's stock. Block told viewers that St. Jude's devices' "communication protocol has been compromised" amounting to "low hanging fruit for attackers to exploit."

46. Leaked minutes before Block's Bloomberg appearance, the Muddy Waters Report, based on MedSec's work, admits that Defendants expressly chose not to follow "standard practice" by contacting St. Jude about their supposed findings. Nevertheless, the document claims St. Jude's CRM Devices pose "unnecessary health risks" and should be "recalled" because they face "cyber attacks" that would "crash" them, "battery drain" them and cause "pacing at a potentially dangerous rate." Moreover, the Muddy Waters Report said, these and "numerous other types of attacks" purportedly "can be executed on a very large scale" courtesy of "keys to the castle" that St. Jude "literally distributed" by "the hundreds of thousands" by way of its Remote Transmitters. According to Defendants, these "keys to the castle" are "readily available on Ebay" to hackers

who, like Muddy Waters, need "no background in cybersecurity . . . to enable these attacks" because St. Jude's devices "are in fact compromised."

47. It was no secret that Muddy Waters and MedSec had teamed up and would share profits if shares of St. Jude's stock *sank*. By day's end on August 25, 2016, there were dozens of strident media pronouncements about the Muddy Waters Report, major financial outlets and Minnesota media among them (for example, *St. Jude stock tumbles as report questions company's cybersecurity*, Minneapolis Star Tribune). By the next day, on August 26, 2016, media coverage of the Muddy Waters Report was mounting (e.g., *FDA joins investigation into security of St. Jude medical devices*, Minneapolis Star Tribune). The extreme and irresponsible language from both the Muddy Waters Report and its authors alike echoed through the blogosphere, just as Defendants planned.

48. On the afternoon of August 26, 2016, Bone appeared on CNBC to promote MedSec's investigation and conclusions set forth in the Muddy Waters Report. Bone told viewers there was a "complete absence of any security protections whatsoever in St. Jude Medical equipment" "across the whole ecosystem of their devices." She also claimed that "we can, remotely, cause these implants to cease to function." When asked about MedSec's financial alignment with Muddy Waters and their choice not to "go to the company [St. Jude]," Bone conceded that "standard operating procedures are to approach the manufacturer [St. Jude]" but that Defendants did not do so because, according to Bone, St. Jude supposedly has a "history of sweeping these issues under the carpet." Defendants have repeatedly stated—falsely—that St. Jude long ignored "fundamental" "security issues" and "put patients at risk." As Block put it, "Our assessment, as well as that of MedSec, is that for a number of years, in this area, St. Jude has been putting profit before patients."

49. Dr. Hemal Nayak, a physician at the University of Chicago Medicine, is an advisor to MedSec and sits on its Board of Directors. On information and belief, Dr. Nayak obtained and provided some of these devices to MedSec. Dr. Nayak also prepared and signed a letter to support Muddy Waters and MedSec's short-sale scheme which, among other things, recommended that patients disconnect their remote monitors based upon the cybersecurity allegations contained in the MedSec report attached to the Muddy Waters press release. Dr. Nayak did not purport to compare the known benefits of remote monitoring with the claimed risks he recounted in his letter and did not subject his views to peer review. Dr. Nayak also used University of Chicago Medicine letterhead to distribute the letter without any disclaimer that the university was not supporting his views; a disclaimer appeared only later in a subsequent version of the Muddy Waters Report. MedSec has admitted it sought advice from no physician other than Dr. Nayak, its own board member. Given that MedSec purportedly brought its research to Muddy Waters in May 2016, Dr. Nayak does not explain, in his letter or elsewhere, why—if he had any legitimate patient safety concerns—he waited about three months to share his supposed concerns for patient safety—none of which he raised with St. Jude or, on information and belief, with the FDA, prior to a letter—addressed to Dr. Nayak's "patients and colleagues"—distributed by short-seller Muddy Waters to investors.

50. Dr. Nayak, like MedSec's Bone, has an admitted interest in the profits that may result from Muddy Waters's short sale transactions. Muddy Waters, MedSec, Carson Block, Justine Bone and Hemal Nayak are concerned only about profiting from the short-sale plays and not patient safety. Dr. Nayak has a conflict of interest in providing medical care and treatment regarding St. Jude devices in that he, as a director of MedSec, owes MedSec duties which give him a personal financial incentive and interest in maintaining support for MedSec's unfounded

positions. Indeed, Defendants collectively are willing to risk patient safety by recommending disconnecting remote monitoring equipment to advance their collective interest in earning substantial profits in the stock market.

51. It was clear that if Defendants had "go[ne] to the company," as the CNBC interviewer suggested, Defendants' plan would crumble (just as their assertions have now begun to when subjected to scrutiny). Only driving down the stock price by defaming CRM Devices with market-bombshell scare tactics could make the short-positioned Defendants richer—with the very unfortunate (and despicable) concomitant result of fueling significant concern and fear in patients and their families.

52. The day after Defendants' media blitz to depress the price of St. Jude's stock, St. Jude categorically and emphatically denied the findings and conclusions in the Muddy Waters Report. The FDA *contradicted* Defendants' medical advice to St. Jude device recipients, recommending patients *not* unplug remote monitoring at this time. In the face of this rebuke and that of other concerned physicians, Dr. Nayak did not retract his purported medical advice and the other Defendants remarkably continued their campaign of fear and continued their intentional or reckless disregard for patients. Facing potentially mammoth losses, Muddy Waters instead released another report on August 29, doubling down on its false and misleading statements, this one entitled "STJ: Still Not Secure" (the "Second MW Report"). This time, Defendants claimed that "the hundreds of thousands of" St. Jude device recipients "who sleep near their" remote monitoring technology for their cardiac implants "would obviously be vulnerable to a large-scale attack."

53. On top of Defendants' latest round of wild accusations aimed at heart patients, Defendants claimed they possessed additional information about St. Jude's device technology that did not appear in the Muddy Waters Report or the Second MW Report.

54. The same day Defendants released the Second MW Report, they publicly posted a video, purportedly of a St. Jude device, on the website vimeo.com. According to Defendants, the video showed their "crash attack on a [St. Jude] pacemaker," evidenced by "red error messages," which sends St. Jude pacemakers "into a state of malfunction" that was "likely" to cause a doctor to "explant" the device. The clear implication: Defendants' "attack" was intended to be so devastating that heart patients would be prompted to undergo surgery to remove pacemakers (and perhaps other cardiac devices) made by St. Jude from their bodies.

55. Muddy Waters posted the video—supposedly the product of months of investigation by MedSec—at approximately 9:45 a.m. EST on August 29, 2016.

The Scheme Starts to Unravel

56. Roughly 24 hours after the August 29 video was posted publicly, on the morning of August 30, 2016, a team of University of Michigan researchers—whose work the Muddy Waters Report purported to invoke—debunked it, concluding that the Muddy Waters Report and Defendants' purported "crash attack" video had "major flaws" because "the evidence does not support their conclusions." According to the University of Michigan researchers, MedSec had not caused any "crash" or malfunction.

57. No surgery would have been required as the device appears to have been functioning. Defendants' claims to the contrary were fiction, and Defendants' video a completely bogus and inappropriate attempt to scare patients.

58. One of the University of Michigan researchers dismissed fears over the "error messages" from Defendants' so-called attack and explained that "we believe the pacemaker is acting correctly." The researcher observed that "to the armchair engineer it may look startling, but to a clinician it just means you didn't plug it in. In layman's terms, it's like claiming that hackers took over your computer, but then later discovering that you simply forgot to plug in your keyboard."

59. In sum, the University of Michigan researchers said they "reproduced [Defendants'] experiments that led to the allegations and came to strikingly different conclusions." Referring to Defendants, one researcher cautioned that "claiming the sky is falling is unproductive. Health care cybersecurity is about safety and risk management, and patients who are prescribed a medical device are far safer with the device than without it."

60. The University of Michigan researchers' conclusions echoed the FDA's rejection of Defendants' findings that users of CRM Devices and Remote Transmitters should "unplug" or "explant" them. In response to the Muddy Waters Report, the FDA advised that at this time "patients should continue to use their devices as instructed and not change any implanted device" and that "if a patient has a question or concern they should talk with their doctor."

61. St. Jude also reviewed the findings and conclusions of the Muddy Waters Report, the Second MW Report and the media statements of Block and Bone. St. Jude concluded that Defendants' statements and communications about St. Jude's device technology are untrue, misleading and irresponsible. St. Jude publicly stated that its long and robust history of working with "third-party experts, researchers, government agencies and regulators in cybersecurity to develop appropriate safeguards" for its devices includes "regular risk assessments based on FDA guidance," "penetration tests" performed by "external experts" and collaborations with

"governmental organizations to gain insight on recent trends." Defendants layered false statements, false innuendo and false implication onto dozens of issues relating to St. Jude's device security, just to try to "cash in." Defendants fully intended, anticipated and relied upon the hundreds of re-publications of their defamatory statements that have occurred in the media and throughout cyberspace.

62. Defendants' conduct is a complete departure from the basic premise and rationales for responsible security investigation and, if necessary, disclosure. The well-accepted basis for coordinated disclosure is that investigating potential vulnerabilities takes time and expertise, including the special expertise that manufacturers have regarding their products with knowledge of the actual design and implementation of cybersecurity controls, and how they operate in the real world and not in controlled laboratory conditions. It is counterproductive at best and dangerous to consumers and patients at worst to disclose potential or claimed vulnerabilities in the absence of coordination with manufacturers and/or regulators because such claimed vulnerabilities may be invalid for one or more reasons—as is the case here—creating wholly unnecessary confusion and potential harm. Where legitimately raised potential vulnerabilities are properly investigated, analyzed and confirmed through proper methods and risk assessment as warranting remediation, then disclosures without coordination and without development of a planned "fix" exposes consumers and patients to potential malicious attacks while an update or "fix" is being developed.

63. From a public-health perspective, the FDA's head of medical device cybersecurity stated that Defendants' "type of disclosure we would not consider to be favorable to improving or strengthening the medical device ecosystem."

64. Scientifically speaking, as the third-party researchers at Virta Laboratories, a private cybersecurity firm specializing in hospital cybersecurity ("Virta Labs"), co-founded by a

highly respected researcher at the University of Michigan, concluded of the Muddy Waters Report and Defendants' ensuing statements, "Does the report or follow-up material meet an appropriate evidentiary standard? *No*."

The False, Misleading, and Defamatory Statements of Defendants

65. Defendants' defamatory statements as to St. Jude devices are far reaching but strike chiefly at three areas. They defame the batteries and telemetry circuitry in St. Jude's CRM Devices as vulnerable to a "drain" attack. They defame the St. Jude CRM Devices as susceptible to a "crash attack" rendering them useless. And they defame the security St. Jude places all around its CRM Devices and systems by claiming St. Jude has done nothing to address cybersecurity and defames the St. Jude brand in attacking wholesale all CRM Devices, the Merlin@home system and Merlin.net.

66. Defendants' statements in these areas are false outright and/or create a false implication that St. Jude's CRM Devices are unsafe and that St. Jude has done nothing to address cybersecurity issues in CRM Devices and the related remote monitoring systems.

67. St. Jude fully expects Defendants to continue their scheme by making further false and misleading statements in hopes of adversely affecting St. Jude's stock price for their gain in disregard for the patients who depend on CRM Devices. Defendants' feigned patient concerns are nothing but a way to divert attention from their scheme to profit.

The False Battery Depletion Scare

68. Defendants repeatedly assert that they could remotely deplete a CRM Device's battery life from a distance of up to 50 feet away, by sending a continuous barrage of RF signals, in a matter of hours or a few days.

69. Those statements concerning the tests performed by MedSec are false and misleading because Defendants omit, among other things, that the tests were not representative of real world conditions and did not account for the significant differences in tests performed on devices on a lab bench versus conditions simulating an implanted CRM Device; that safety features are present to protect patients implanted with certain devices against such an attack; and that the attack that MedSec purported to have conducted could not occur in real world conditions with an implanted CRM Device. In short, Defendants' purported battery depletion scare is reckless and irresponsible.

70. Defendants thereby intentionally omitted statements concerning issues about battery security in order to create a false and misleading picture about the vulnerability of St. Jude's CRM Devices to purported battery depletion attacks.

The False Device "Crash"

71. Defendants have repeatedly claimed that they could remotely crash or install malicious software into devices, resulting in a loss of wireless connectivity and the CRM Devices being "bricked"—*in other words, no longer providing therapy to heart patients*.

72. Those statements are false and misleading because the so-called crash scenarios presented by Defendants was not a "crash" at all. The so-called security flaw was, in fact, a design feature. Defendants claimed to have set off red warning lights and rendered a CRM device useless when in fact it was working as designed and providing continued therapy: a "lockout" feature had simply stopped Defendants in their tracks.

73. Although Defendants claimed that after purportedly "crashing" the CRM Devices, it was "impossible to tell whether, and how" the CRM Devices "are functioning," as St. Jude has emphasized and demonstrated, that claim is false, too.

74. "In fact," as confirmed by Virta Labs, "it is possible to test whether the sensing and pacing functions—which we would argue are the most essential clinical functions—are working." Virta Labs cited a publicly available website that shows how, and any credible researcher would have been able to test the clinical functions under the so-called crash attack Defendants attempted. Defendants, however, knowingly promoted the false view that the device had become disabled.

75. Thus, Defendants intentionally omitted statements and established testing protocols in order to create a false and misleading picture about the vulnerability of St. Jude's CRM Devices to so-called crash attacks.

The False Picture of St. Jude's Device and System Security

76. Defendants paint their false picture of St. Jude's devices with strident accusations about the severity of risks, with common reference to, for example, a "large-scale attack."

77. These claims are false and misleading. Defendants' false implication, however, is clear: St. Jude's devices are broadly at significant risk of imminent cyber attack. St. Jude has demonstrated that this is patently false, and, as Virta Labs further observed, "[t]he Muddy Waters report does not provide enough evidence to support the claim that an attacker could simultaneously control many implants, although it speculates with respect to 'large-scale' attacks." "In our opinion," Virta Labs concluded, the Muddy Waters Report "regrettably engages in fearmongering when it claims that 'large-scale' attacks are a plausible outcome of the vulnerabilities they report." Indeed, St. Jude has never received a report of a purported security compromise of St. Jude's CRM Devices or related remote monitoring as to a patient in any of the ways Defendants claim.

78. Defendants intentionally constructed their false implication about St. Jude's devices using nonspecific claims unsupported by any evidence, even though, pursuant to industry standards, Defendants' researchers could have gained St. Jude's cooperation—directly and/or

through governmental or other channels—to investigate their theories. Hiding behind the claim that testing a wide-scale attack would be illegal, they omitted the key information that would have allowed an ethical security researcher to investigate such a claim. Defendants knew, however, that they lacked any material evidentiary basis or proof for stating the devices were subject to a large-scale remote attack.

79. While Defendants claim St. Jude's devices made from off-the-shelf hardware are insecure for this reason, Defendants' outdated position endorses the thoroughly discredited notion of "security through obscurity." What Defendants described as a flaw, they knew to be common and accepted practice.

80. Indeed, non-proprietary hardware is common in medical devices industry-wide.

81. Defendants' various false and misleading statements have, as they intended, been repeated and chronicled in hundreds of media reports. In furtherance of their scheme, Defendants coordinated a campaign of misleading and false statements, as illustrated below.

82. It began August 25, 2016. Block appeared on Bloomberg TV, claiming St. Jude's devices' "communication protocol has been compromised" and were effectively "low hanging fruit for attackers to exploit." Block made many other similar statements just as false and defamatory in media interviews and elsewhere.

83. Block's statements are defamatory and false. As discussed above, St. Jude and independent analysts determined that St. Jude's device technology was not compromised and that Block's statements were demonstrably incorrect.

84. Defendants' statements or implications purportedly identifying vulnerabilities applicable to all Merlin@home units are false and misleading. St. Jude made multiple

improvements since 2013 that prevent the types of attacks described by Defendants. St. Jude has an ongoing program to replace older units to further enhance security.

85. Also on August 25, 2016, Muddy Waters stated in the Muddy Waters Report that St. Jude's devices pose "unnecessary health risks"; should be "recalled"; were facing "cyber attacks" that would "crash" them, "battery drain" them and cause "pacing at a potentially dangerous rate"; that these and "numerous other types of attacks" purportedly "can be executed on a very large scale"; that St. Jude "literally distributed" by "the hundreds of thousands" of invitations to hackers in the form of "keys to the castle"; and that the "keys to the castle" are "readily available on Ebay" to hackers who need "no background in cybersecurity" to attack St. Jude devices that are "in fact compromised."

86. Defendants' statements are false and misleading:

a. There were no "unnecessary health risks." The rigorous FDA approval process, the FDA advice for device users and the conclusions of independent researchers and St. Jude debunked this accusation.

b. Claiming CRM Devices should be "recalled" creates the false implication that the devices are so unsafe that patients should discontinue use of remote monitoring or are better off having them removed via surgery. The FDA, independent researchers and St. Jude demonstrated its falsity.

c. There was no "crash" of a St. Jude CRM Device. This claim was fiction and despite the purported rigor of MedSec's analysis and Muddy Waters's staff-attempted video demonstration, was debunked in a matter of hours by the University of Michigan. St. Jude also examined the video separately

and confirmed the false and misleading demonstration in Defendants' video.

d. The red warning lights that MedSec claimed proved that it had induced a "crash" of the CRM Devices only indicated that the electrical leads of the device were not connected to human heart tissue—or to anything else—as they are when implanted in a patient. Defendants simply misrepresented a basic feature of the device, not a security flaw, and intentionally omitted an explanation of *proper* testing, which employs connected leads (or recognizes the effect of their absence). Startlingly, despite a presumed deep familiarity with academic and clinical standards, including peer-reviewing protocol, Dr. Nayak deliberately *ignored all of it* in order to help prop up Defendants' false findings. Dr. Nayak's letter also furthered Defendants' scheme to put St. Jude at a competitive disadvantage by urging prospective CRM Device recipients to consider the purported flaws in St. Jude's devices when discussing with their own doctors whether to get a CRM Device.

e. MedSec's claim (presented in a screenshot) that it had caused a CRM Device to operate at an excessively fast rate was flatly contradicted by the 40 beats per minute reading on the screen. Defendants misrepresented the performance of the device. Dr. Nayak, in particular, as a board certified electrophysiologist who purportedly vetted Defendants' experiments, had to have known from what is obvious that the leads were not connected and that the pacing was not excessive.

f. In contrast, Dr. Thomas Crawford, a University of Michigan professor of internal medicine, a cardiologist and a clinical electrophysiologist, stated publicly that, "[g]iven the significant benefits from remote monitoring, patients should continue to use their prescribed cardiac devices while independent researchers investigate the claims made by MedSec and their financial partner Muddy Waters Capital LLC."

g. Dr. Crawford's statement contradicted Dr. Nayak's recommendation. The FDA has, as noted above, also agreed that patients should not discontinue using their remote monitoring devices.

h. MedSec claimed that it had caused a pacemaker to stop operating because MedSec was unable to detect activity in the pacemaker using a St. Jude programming device. However, MedSec's transmission of radio waves during its purported hack attack had caused the pacemaker they appear to have used to lock out their transmissions—a feature of the design that effectively blocked MedSec's efforts while allowing the pacemaker to continue to function. In their purported test, Defendants misrepresented a pacemaker design feature which protects battery life and enhances battery longevity—another security feature—as if it were evidence of a fatal flaw.

i. Other safeguards in CRM Devices can cause them to revert to a "Safe Mode," under certain circumstances, including when battery life drops below certain levels. The "Safe Mode" causes the CRM Devices to revert to default hardware settings as a further protection against, among other things, low battery life.

j. Defendants also either recklessly or intentionally failed to disclose in describing their testing that it would take hundreds of hours of continuous hacking of the device to discharge a new battery to a threshold level. In addition, Defendants failed to test in conditions representative of those when a device is actually implanted (and not just being tested outside the body) and misrepresented their results as if they applied to all devices in real-world settings. In any event, the CRM Devices at issue are designed to trigger a vibratory or auditory alert for the patient indicating a low battery and doctors can also monitor battery life through remote monitoring and in person office visits. The patient alert is typically triggered when there are still months of use before the battery can no longer operate the CRM Device. Accordingly, there is no credible threat that the device will stop operating and harm the patient due to battery depletion as Defendants misrepresented.

k. MedSec offers no factual basis for plausible or realistic risk of "large scale attacks." MedSec attempted to hack only one CRM Device at a time and provided no evidence, much less sufficient evidence, that a large number of CRM Devices could be hacked through the Internet or any other means. St. Jude has also provided updates and other submissions to the FDA and other regulatory authorities about the security of its CRM Devices and related remote monitoring devices. Defendants had no factual basis for their statements and misrepresented the supposed risk of large scale attack.

87. On August 26, 2016, Bone appeared on CNBC and took the scheme still further, claiming that there was a "complete absence of any security protections whatsoever in St. Jude Medical equipment."

88. This blatant falsehood (repeated in multiple other interviews and media) is part and parcel of the scheme to affect St. Jude's stock price. Among other things, as explained above, MedSec attempted to crash St. Jude's CRM Devices but was unable to do so as a result of various safeguards and inherent design features. Bone intentionally or recklessly misrepresented St. Jude's security steps in its devices and its history regarding cybersecurity which, as detailed throughout this complaint, are numerous and ongoing.

89. Bone also said on CNBC that Defendants chose not to "go to the company [St. Jude]" because, she claimed, St. Jude has a "history of sweeping these issues under the carpet." Defendants made multiple similar if not identical statements.

90. These statements and their implication are demonstrably false.

a. For example, since 2009, St. Jude's technologies have been certified annually by a third party expert.

b. In another illustration, officials at the U.S. Department of Homeland Security ("DHS") approached St. Jude in 2014 on behalf of private security researchers examining St. Jude's products. St. Jude promptly responded and cooperated with the investigation, and DHS took no action.

c. St. Jude's track record is the opposite of what Bone stated in furtherance of the scheme to profit from their misconduct and false statements. As discussed above, St. Jude's cybersecurity efforts are robust, effective and ongoing.

91. On August 29, 2016, Defendants released the Second MW Report, claiming that "the hundreds of thousands of" users of St. Jude's devices are "obviously . . . vulnerable to a large-scale attack."

92. As explained above, this statement (and others) and their implication are demonstrably false and categorically irresponsible. Defendants had no factual basis for their statements.

93. As part of their scheme to drive down the price of St. Jude stock and reap profits from short sales of St. Jude stock, Defendants spoke and printed numerous other such statements which are similar in kind, tone, import, effect and implication, all with a common goal of cashing in. Such statements or factual implications are similarly false and baseless.

COUNT I – DEFAMATION

Defamation By Implication

94. St. Jude re-alleges and incorporates by reference paragraphs 1 through 93 as if fully set forth herein.

95. As set forth above, Defendants have, through their statements about the purported safety problems with St. Jude's medical devices, publicly stated or implied that St. Jude's products are insecure and dangerous, and that St. Jude has routinely ignored these concerns in the past out of greed, laziness, inattention, or incompetence.

96. As set forth in detail above, these implied statements of fact are demonstrably false and misleading.

97. Defendants have made these statements and implications by the selection and juxtaposition of true statements so as to imply a defamatory connection between them, as well as by omitting facts that would have dispelled the defamatory implication and revealed the truth.

98. Defendants intended to make these defamatory implications and to cause the expected and intended repetition of them on a wide scale in order that each of them together and individually would profit from Muddy Waters's admitted short positions in St. Jude's stock, and did so either knowing that they were false, or in reckless disregard of their truth or falsity.

99. These implied statements of fact have harmed and will harm or threaten to harm St. Jude in its business or trade of cardiac medical devices, and so are defamatory *per se*. Because Defendants' false and misleading statements are defamatory per se, damages are presumed.

Defamation

100. As set forth above, Defendants have made numerous demonstrably false statements of fact concerning St. Jude and its medical device technology products concerning purported security shortfalls. Defendants also intended and expected the repetition of them on a wide scale.

101. Defendants made these statements either knowing that they were false, or in reckless disregard of their truth or falsity, in order that each of them could profit from Muddy Waters's admitted short positions in St. Jude's stock.

102. These statements of fact have harmed, will harm or threaten to harm St. Jude in its business or trade of cardiac medical devices, and so are defamatory *per se*. Because Defendants' false and misleading statements are defamatory per se, damages are presumed.

COUNT II – LANHAM ACT – 15 U.S.C. § 1125

103. St. Jude re-alleges and incorporates by reference paragraphs 1 through 93 as if fully set forth herein.

104. As set forth above, Defendants have made, both directly and by implication, numerous false statements concerning St. Jude's medical device technology products and St. Jude's conduct of their cardiac medical device businesses.

105. These statements were made for the purpose of promoting Defendants' business and plan to short St. Jude stock and to advertise Defendants' services and solicit customers for their respective businesses, including MedSec's self-proclaimed one-of-a-kind "vulnerability researchers" with a stated goal of recovering startup costs and Muddy Waters's self-styled "pioneer" approach to "research product."

106. Defendants' statements were made in an effort to damage St. Jude's standing and business compared to its competitors. These statements were also made in order to further a coordinated campaign to raise their public profile and to promote their investment and cyber-security research and services.

107. These false statements about St. Jude's medical device technology have deceived, have the potential to deceive, were intended to deceive or will deceive, those who hear or read them, including patients, doctors, and investors, into believing that St. Jude's devices are deeply insecure and affirmatively dangerous; and into believing that St. Jude put "profits ahead of patients."

108. This deception was intended to affect St. Jude's stock price and influence patients and doctors' purchasing decisions, all of which may be expected to lead them to avoid St. Jude's products in favor of those made by St. Jude's competitors.

109. St. Jude is or will likely be substantially injured as a result of these false statements including, among other things, loss of goodwill. This harm and risk of future harm is ongoing.

COUNT III - DECEPTIVE TRADE PRACTICES ACT – MINN. STAT. § 325D.44

110. St. Jude re-alleges and incorporates by reference paragraphs 1 through 93 as if fully set forth herein.

111. As set forth above, in the course of conducting their business and advertising their services, Defendants have, both directly and by implication, made false and misleading representations of fact that disparage St. Jude's medical device technology, services, and the conduct of their businesses.

112. Defendants have made these representations knowing them to be false and misleading in order that each of them could profit from Muddy Waters's admitted short positions in St. Jude's stock.

113. As a result of these false and misleading representations, Defendants have been unjustly enriched and St. Jude has been harmed and is likely to be harmed including by, among other things, loss of goodwill.

COUNT IV – CIVIL CONSPIRACY

114. St. Jude re-alleges and incorporates by reference paragraphs 1 through 93 as if fully set forth herein.

115. In concert with taking a short position in St. Jude's stock, Defendants reached an agreement to defame and disparage St. Jude and its products in order to drive down the stock price and capture ill-gotten profits and deprive St. Jude of goodwill and cause additional costs and expenses.

116. Defendants took concerted action in furtherance of these unlawful ends. Defendants have engaged in a coordinated smear campaign across a variety of media in order to impugn the safety and security of St. Jude's medical devices. As discussed above, Defendants' actions and statements amounted to defamation, false advertising, and deceptive and unfair trade practices.

117. Defendants' conspiracy has adversely and improperly affected St. Jude's stock price, unjustly enriched Defendants, and harmed St. Jude through defamation per se, defamation

by implication and violations of federal law for which St. Jude is entitled to damages, equitable relief and disgorgement of profits made by Defendants.

PRAYER FOR RELIEF

WHEREFORE, St. Jude respectfully requests that the Court enter judgment as follows:

1. Judgment in favor of St. Jude and against each of the Defendants.

2. Disgorgement of profits made by Defendants.

3. Award St. Jude appropriate equitable or injunctive relief.

4. Award St. Jude damages to be determined at trial.

5. Award St. Jude treble damages for violations of 15 U.S.C. § 1125.

6. Award St. Jude reasonable attorneys' fees and costs.

7. Any other relief this Court deems equitable and just.

Date: September 7, 2016

By: s/Michael V. Ciresi

Daniel L. Ring*
Robert J. Kriss*
Joseph M. Snapper*
Mayer Brown LLP
71 S. Wacker Drive
Chicago, IL 60606
Phone: (312) 782-0600
dring@mayerbrown.com
rkriss@mayerbrown.com
jsnapper@mayerbrown.com

Rajesh De*
Mayer Brown LLP
1999 K Street, N.W.
Washington, DC 20006
Phone: (202) 263-3000
rde@mayerbrown.com

Of Counsel

Michael V. Ciresi (MN #0016949)
James C. Joslin (MN #0394815) (District Admission Pending)
Heather M. McElroy (MN #034168X)
Ciresi Conlin LLP
225 S. 6th St., Suite 4600
Minneapolis, MN 55402
Phone: 612.361.8202
Email: MVC@CiresiConlin.com
JCJ@CiresiConlin.com
HMM@CiresiConlin.com

Attorneys for Plaintiff St. Jude Medical, Inc.

* = *pro hac vice* to be filed