KELLY M. DIEPHUIS, OSB No. 081704
kelly@angelilaw.com
EDWARD A. PIPER, OSB No. 141609
ed@angelilaw.com
ANGELI LAW GROUP LLC
121 S.W. Morrison Street, Suite 400
Portland, Oregon 97204
Telephone: (503) 954-2232
Facsimile: (503) 227-0880

Attorneys for Plaintiff Columbia Sportswear Company

UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

PORTLAND DIVISION

COLUMBIA SPORTSWEAR COMPANY, an Oregon corporation, Plaintiff, v. 3MD INC. dba DENALI ADVANCED INTEGRATION, a Washington corporation, and MICHAEL LEEPER, an individual, Defendants.	CASE NO.: _____ **COMPLAINT** (violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; violations of the Wiretap Act, 18 U.S.C. § 2510 *et seq.*; conversion; breach of the duty of loyalty) DEMAND FOR JURY TRIAL

Plaintiff Columbia Sportswear Company ("Columbia") brings this action against Defendants 3MD Inc. dba Denali Advanced Integration ("Denali") and Michael Leeper ("Leeper") (together, "Defendants"). Columbia alleges as follows:

INTRODUCTION

1. This case concerns a flagrant invasion of Columbia's and its employees' privacy by a technology consulting firm that secretly and repeatedly hacked into Columbia's private

computer network, including several employees' private company email accounts. That firm, Denali, is a Washington-based "IT provider" and former vendor to Columbia. Leeper, who works as Denali's Chief Technology Officer ("CTO"), is the Denali employee who committed the hacking.

2. Before joining Denali, Leeper held a high-level position in Columbia's Information Technology ("IT") Department. By virtue of his position, Leeper had nearly unlimited access to Columbia's private computer network, including the thousands of secure "@columbia.com" email accounts used by Columbia employees around the world. However, in mid-February 2014, Leeper accepted an executive position with Denali and notified Columbia that he would resign. As with all departing employees, Columbia terminated Leeper's regular network account when his employment ended. However, on March 2, 2014—*one day* before his last day of employment—Leeper created a separate, unauthorized network account under a false name, "Jeff Manning," called "jmanning." Using the jmanning account, Leeper could continue to access Columbia's private computer network after his resignation.

3. Over approximately the next two and a half years, and without Columbia's knowledge or consent, Leeper secretly hacked into the private company email accounts of numerous Columbia employees, and, on information and belief, into other parts of Columbia's private computer network. He did so hundreds of times. During the intrusions, Leeper illegally accessed a wide variety of confidential business information belonging to Columbia. That information included emails concerning business transactions in which Denali had a financial interest; emails concerning transactions between Columbia and Denali's competitors; and confidential budget documents related to the IT Department's long-range planning. Leeper

illegally accessed that information in furtherance of Denali's desire to profit from its business relationship with Columbia, and in his capacity as Denali's CTO.

4. Columbia has implemented numerous safeguards to ensure the integrity and security of its IT systems. It uses similar safeguards to protect its confidential business information from unauthorized disclosure or use. In each instance, Columbia has no choice but to trust the IT staff that implements those safeguards to maintain and abide by them. A breach of that trust—particularly where, as here, committed to obtain an unfair commercial advantage on behalf of a third party—is an act of serious misconduct. Columbia brings this lawsuit to recover damages associated with Defendants' unlawful intrusions into its private computer network, to secure the return of whatever unlawfully accessed Columbia information they may still possess, and to recover the reasonable attorneys' fees and costs it incurs in bringing this action.

THE PARTIES

5. Columbia is a publicly traded Oregon corporation with its headquarters in Washington County, Oregon. Columbia is a well-known manufacturer and distributor of outerwear, sportswear, and a variety of other clothing, equipment, and accessories. It conducts business worldwide.

6. Denali is a privately held Washington corporation with its headquarters in King County, Washington. Denali is a consulting firm and reseller of computer hardware and software with offices in Washington, Oregon, Texas, the United Kingdom, and Ireland. Denali does business in Oregon, and from 2012 to the present it has been registered with the State of Oregon as a foreign business corporation authorized to transact business within the state.

7. Leeper is an individual who, on information and belief, resides in Oregon. From 2014 to the present, Leeper has been employed by Denali as its CTO.

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction over Columbia's federal claims pursuant to 28 U.S.C. § 1331.

9. This Court has supplemental jurisdiction over Columbia's related state-law claims pursuant to 28 U.S.C. § 1367(a), *i.e.*, because those claims derive from the same nucleus of operative facts and form part of the same case or controversy. Each of Columbia's state-law claims is—like its federal claims—based on Defendants' intrusions into Columbia's private computer network.

10. Venue is proper within this District pursuant to 28 U.S.C. § 1391(b)(2) because all or a substantial part of the events giving rise to Columbia's claims occurred in the State of Oregon, and a substantial part of the property that is the subject of this action is situated in the State of Oregon.

FACTS

A. Leeper Worked in a Position of Trust and Confidence in Columbia's IT Department, Where He Developed an Intimate Knowledge of—and Had Nearly Unlimited Access to—the Company's Private Computer Network.

11. In or around May of 2000, Columbia hired Leeper into its IT Department. Leeper's first position in the company was as a manager of the "desktop services" team. Over the next decade and a half, Leeper progressed upward through Columbia's IT Department. At the time of his departure in March 2014, he held the position of Senior Director of Technology Infrastructure. In that position, Leeper was responsible for maintaining Columbia's global IT systems, among other things. He also dealt frequently with Denali and Columbia's other technology vendors.

12. During his employment with Columbia, Leeper developed an intimate knowledge of Columbia's email systems and broader private computer network. As a practical matter, his

duties required him to have nearly unlimited access to the company's network. His duties thus put him in a unique position among his coworkers: while the vast majority of Columbia employees were (and are) permitted to access only their own email accounts and limited other parts of the company's private computer network, Leeper could access nearly *all* of that network, including thousands of other employees' company email accounts. Additionally, unlike the vast majority of other Columbia employees, Leeper could create new network accounts and give existing accounts "permissions" enabling them to access otherwise forbidden parts of Columbia's network.

13. Leeper's unique responsibilities also gave him access to much of Columbia's most sensitive confidential business information. His duties, for example, at times required him to assist executives and other high-level employees with their email accounts, which frequently contained such information. Leeper also was responsible for maintaining the computer servers on which Columbia stores virtually all of its electronic data, including confidential information concerning the company's finances, strategic planning, and numerous other business topics.

14. Having been entrusted with access to Columbia's most sensitive confidential business information, Leeper was employed by Columbia in a position of extreme trust and confidence.

15. Leeper knew that Columbia prohibited unauthorized access, whether by an employee or a third party, to an employee's email account or any other part of its private computer network.

B. In March 2014, Leeper Resigned to Become CTO of Denali, a Technology Consultant and Reseller with Which He Previously Did Business on Behalf of Columbia.

16. Between approximately 2012 and 2016, Columbia purchased various computer hardware, software, and consulting services from Denali. Leeper initiated Columbia's business

relationship with Denali, which functions as a middleman between hardware and software manufacturers, like IBM and EMC Corporation, and end-users, like Columbia. Denali negotiates a price and other terms with a manufacturer, sells the hardware or software to the end-user at a markup, and then offers the end-user various consulting and support services related to the hardware or software.

17. Columbia also uses multiple other vendors—*i.e.*, Denali's competitors—to procure computer hardware, software, and related consulting services. For those and other reasons, and as Leeper knew well, Denali could have derived commercial benefit during its business relationship with Columbia from predicting what particular computer hardware or software Columbia needed, what Columbia was willing to pay for that hardware or software, and what Columbia's growth and strategic plans entailed for its future IT needs.

18. During his employment with Columbia, Leeper was responsible for procuring computer hardware, software, and consulting services from Denali on behalf of Columbia. He interacted with Denali frequently.

19. In early 2014, Denali President Majdi Daher recruited Leeper to become Denali's CTO. Leeper gave notice of his resignation in mid-February 2014. Leeper's last day at Columbia was March 3, 2014.

20. In his new role as Denali's CTO, Leeper played an important role in managing Denali's business relationship with Columbia and in promoting the sale of Denali's products and services to Columbia. Leeper worked in concert with Denali's sales team, regularly contacting employees in Columbia's IT Department to discuss ways in which Denali might expand its business with Columbia.

C. On the Eve of His Departure from Columbia, Leeper Secretly Created an Unauthorized Network Account That Allowed Him to Hack into Columbia's Private Computer Network Following His Resignation.

21. At approximately 12:11 p.m. on March 2, 2014—one day before his last day of work at Columbia—Leeper surreptitiously created for himself a "backdoor" through which he could continue to access Columbia's private computer network following the termination of his employment. He created a network account under a false name, "Jeff Manning," called "jmanning" that would allow him to log on remotely to Columbia's network. Leeper did so without Columbia's knowledge, much less its permission.

22. The jmanning account enabled Leeper to access Columbia's private computer network in several ways. First, it gave him credentials with which he could access Columbia's Virtual Private Network ("VPN"). Columbia's VPN gives users secure access to the company's private, internal computer network via an external internet connection. A laptop user in a coffee shop or on a wifi-enabled airplane, for example, can use Columbia's VPN to access the same documents, folders, and other information stored on Columbia's private computer network (including, but not limited to, company email) to which she would have access if she were sitting at her desk at Columbia's headquarters.

23. Leeper's jmanning credentials also enabled him to access Columbia's Virtual Desktop Infrastructure ("VDI"). Columbia's VDI recreates a user's computer desktop on an external server, and then permits the user to access the recreated desktop remotely. Columbia employees' computer desktops typically are connected to the company's private computer network. For that reason, Columbia's VDI typically enables a user to access the network and any resources (*e.g.*, files, folders, or mailboxes) stored on or connected to the network. When a user finishes using a VDI, the virtual desktop itself (including, for example, any files a user may have saved to the virtual desktop) is erased.

24. Finally, together with an older "service" network account named "svcmom," the jmanning account allowed Leeper to hack into Columbia employees' private company email accounts. The "svcmom" account originally was created in 2002 for the purpose of monitoring key events on Columbia's network, sending alerts, and performing other administrative functions, all of which it did automatically. The svcmom account functioned largely in the same manner as other Columbia network accounts, but, because it was designed solely for administrative use, it did not permit users to access Columbia's VPN.

25. In approximately 2007, Columbia ceased using the svcmom account when it upgraded to a newer monitoring system. After that point, Leeper had no legitimate business reason to use the svcmom account. However, on information and belief, shortly before and after his resignation, Leeper gave the svcmom account several new "permissions" that would allow a user of the account to access other Columbia employees' email accounts. As a result, Leeper would be able to access those accounts in at least two ways following his resignation: (i) he could use the jmanning account to log onto Columbia's VPN or to create a VDI, open Microsoft Outlook, and enter his svcmom credentials, or (ii) he could open an internet browser and enter his svcmom credentials directly into Microsoft's web-based email client. In either case, Leeper would have full—and unauthorized—access to the private email accounts to which he had connected the svcmom account.

D. Over the Next Two and a Half Years—and at Least in Part on Denali's Behalf and for Denali's Benefit—Leeper Hacked into Columbia's Private Computer Network on Hundreds of Separate Occasions.

26. At no point did Columbia authorize Leeper to access any part of Columbia's private computer network using the jmanning or svcmom accounts.

27. However, over the next two and a half years, Leeper knowingly, willfully, and repeatedly hacked into Columbia's private computer network by accessing its VPN and VDI

with the jmanning account. He did so hundreds of times; Columbia's internal IT records, which automatically record the number of times a particular user has logged onto its network, show that jmanning has accessed the network 700 separate times as of today's date.

28. After unlawfully accessing Columbia's network with the jmanning account, Leeper used the svcmom account to hack into several Columbia employees' private email accounts. He then accessed hundreds of emails stored in those accounts. Each time Leeper accessed one of those emails, he obtained the contents of and metadata associated with the message, which were at least temporarily stored on the computer or other electronic device he used to commit the hacking.

29. Leeper committed the hacking at least in part on Denali's behalf and for its benefit. Columbia's computer forensic evidence generally is limited to the period after it detected the hacking; the full extent of Defendants' misconduct—*i.e.*, the extent of the hacking that occurred between Leeper's resignation and the time Columbia detected the intrusions—currently is unknown. However, the computer forensic evidence that Columbia has obtained to date demonstrates that Leeper hacked into Columbia's private computer network at least in part in an attempt to obtain an unfair commercial advantage for Denali over its competitors for Columbia's business.

30. For example, on July 25, 2016, between 4:22 p.m. and 4:34 p.m. and again between 8:49 p.m. and 9:00 p.m., Leeper hacked into company email accounts belonging to two employees in Columbia's IT Department. He unlawfully accessed—at a minimum—dozens of their emails on each occasion. He did the same on July 27, 2016 between 3:35 p.m. and 3:48 p.m.; on August 1, 2016 between 3:01 p.m. and 3:13 p.m.; and on August 9, 2016 between 3:06 p.m. and 3:18 p.m. Those two employees are responsible for aspects of Columbia's IT

procurement, *i.e.*, for purchasing the types of computer hardware and software for which Denali acts as a reseller and consultant. Leeper worked with both employees during his employment with Columbia and knew their respective roles well. During the period in which he was unlawfully hacking into their email accounts, Leeper would occasionally contact one of the two employees and discuss ways in which Denali potentially could expand its business with Columbia.

31. Additionally, the hacked emails themselves dealt with subjects in which Denali had a clear commercial interest. For example, among the emails that Leeper unlawfully accessed on July 25, July 27, August 1, and August 9 were messages concerning budgeting for upgrades to IT equipment that Denali resells and services; messages relating to the IT Department's confidential long-range planning, some of which included detailed spreadsheets showing various aspects of Columbia's prior IT spending and projected spending over the coming years; communications between Columbia and Denali's competitors regarding various IT-related transactions; and, in some cases, messages attaching contracts between Columbia and Denali's competitors.

32. In at least one case, Leeper specifically targeted an email concerning a transaction in which Denali had a potential business interest. As of approximately 3:47 p.m. on July 27, 2016, Leeper had logged into the two IT employees' email accounts and was accessing messages in one of the employees' "Sent Items" folder. At 3:47:26, a message with the subject line "Pure Storage Partner Discussion" arrived in the other employee's inbox. Within the same second—*i.e.*, at 3:47:26—Leeper switched into the recipient's email account and accessed the new message. He then returned to and continued accessing the "Sent Items" folder of the first employee. Pure Storage, Inc. is a well-known provider of computer equipment with whom

Columbia was exploring a potential transaction. Though Denali resells equipment of the type that Pure Storage manufactures, Denali was not at that time an approved reseller for Pure Storage. As a result, Denali would not have been eligible to participate as a reseller in that transaction. However, during the summer or early fall of 2016, Columbia learned that Denali had become an "approved" Pure Storage reseller.

33. Defendants' intrusions went well beyond the email accounts belonging to the two Columbia IT employees described above. Rather, during the late summer and early fall of 2016, Leeper hacked into at least *eight* different Columbia employees' email accounts. Among those accounts were accounts belonging to several high-level executives and other employees with whom Leeper had no personal relationship, but whose accounts contained highly confidential business communications of potential commercial value to Denali.

34. On numerous occasions, Leeper used the jmanning account to connect to Columbia's private computer network via VPN but did not access any Columbia email accounts. Instead, on information and belief, on those occasions, he accessed other documents and information stored on Columbia's network.

E. Columbia Discovered Defendants' Misconduct and Immediately Took Steps to Remediate the Breaches.

35. Columbia detected Leeper's intrusions while implementing an upgrade to its email system during the summer of 2016. At the time, however, it could not confirm the identity of the hacker, the particular information that the hacker had unlawfully accessed, or for how long the hacker had been unlawfully invading Columbia's private computer network. Columbia reported the matter to the FBI for investigation and began monitoring the jmanning and svcmom accounts. It did so in an attempt to confirm the hacker's identity, to determine what information

the hacker had accessed or obtained, and to learn other information that would allow Columbia fully to remediate the breach of its network.

36. Columbia engaged outside legal counsel to assist it in the investigation and remediation of the breach. For those services, Columbia has paid its outside legal counsel a total of over $5,000.

37. Additionally, numerous Columbia employees spent dozens of work hours between the months of July and October 2016 working with Columbia's outside counsel, its email providers, and the FBI, and reviewing data associated with the intrusions. They did so in an attempt to confirm the identity of the hacker, to determine which particular information had been compromised, to ensure that all means of illicit access employed by the hacker had been identified and closed, and otherwise to remediate the breach. The value of those employees' time to Columbia, calculated in the amount it paid those employees for their work, likewise exceeds $5,000.

38. Despite Columbia's requests, Defendants have refused to cooperate in Columbia's efforts to remediate their intrusions. Accordingly, to date, Columbia has been unable to determine whether Defendants still possess any of the confidential business information they illegally accessed during their hacking. Columbia has likewise been unable to determine the extent to which Defendants have used or disseminated, or intend in the future to use or disseminate, that information. Defendants' continued possession of any such information, and any past or future use or dissemination of such information, threatens Columbia with irreparable harm for which there exists no adequate remedy at law.

CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF
(Violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq.*)
(Both Defendants)

39. Columbia repeats and incorporates by reference, as if fully set forth herein, the allegations in all preceding paragraphs.

40. The Columbia computer systems that store the emails and other information that Defendants unlawfully accessed are "protected computers" within the meaning of 18 U.S.C. § 1030(e)(2) because they are used in and affect interstate and foreign commerce and communication. Columbia employees around the world use those computer systems to communicate via email and otherwise to conduct business on Columbia's behalf.

41. Defendants intentionally accessed those computer systems without authorization. Neither Leeper nor Denali was authorized to access or view the contents of any Columbia employee's private company email account. Nor were Defendants authorized to log onto the other parts of Columbia's private computer network that, on information and belief, they unlawfully accessed and viewed.

42. Defendants obtained information from the Columbia computer systems they unlawfully accessed. As explained above, during the intrusions, Defendants accessed confidential Columbia business information at least in part for the purpose of securing an unfair commercial advantage for Denali over its competitors for Columbia's business.

43. At all relevant times, Leeper was an employee and high-level executive of Denali. He committed the hacking described above at least in part on Denali's behalf, for its commercial benefit, and within the scope of his role as Denali's CTO. Thus, Denali is vicariously liable for Leeper's hacking.

44. As a result of Defendants' intrusions, Columbia has suffered loss over the preceding one-year period in an aggregate amount of over $5,000. Columbia engaged outside counsel to assist it in investigating and remediating Defendants' breaches of its private computer network. Columbia has paid its outside counsel over $5,000 for those purposes. Additionally, Columbia employees have spent dozens of work hours working with Columbia's outside counsel, its email providers, and the FBI, reviewing data associated with the intrusions, and otherwise taking steps to ensure that the effects of Defendants' intrusions are fully remediated. The value of their time is, in the aggregate, over $5,000.

45. In committing the intrusions described above, Defendants violated 18 U.S.C. § 1030(a)(2)(C). Columbia is entitled to an award of economic damages under 18 U.S.C. § 1030(g) in an amount to be proven at trial.

SECOND CLAIM FOR RELIEF
(Violations of the Wiretap Act, 18 U.S.C. § 2510 *et seq.*)
(Both Defendants)

46. Columbia repeats and incorporates by reference, as if fully set forth herein, the allegations in all preceding paragraphs.

47. The email messages that Defendants unlawfully accessed are electronic communications within the meaning of 18 U.S.C. § 2510(12).

48. While committing the intrusions described above, Defendants intercepted several email messages in violation of 18 U.S.C. § 2511(1)(a). Specifically, while Leeper was unlawfully logged into Columbia employees' private email accounts, new messages addressed to the accounts would arrive in the users' inboxes. Leeper's interception of those messages was contemporaneous with their transmission: the new messages arrived in the recipients' inboxes and in the remote mailboxes through which Leeper accomplished his hacking at the same time.

In receiving those new messages while unlawfully logged into the email accounts to which the messages were addressed, Leeper intercepted the messages in violation of 18 U.S.C. § 2511(1)(a).

49. Additionally, on at least one occasion, Leeper accessed an email message at the same moment it arrived in its intended recipient's inbox. The "Pure Partner Storage Discussion" email arrived in its recipient's inbox at 3:47:26 p.m. on July 27, 2016; Leeper, who was logged into the account at that time, accessed the message at *precisely* the same time, *i.e.*, at 3:47:26 p.m. on July 27, 2016. In doing so, Leeper intercepted that message in violation of 18 U.S.C. § 2511(1)(a). On information and belief, Leeper accessed and intercepted other email messages in the same manner.

50. Additionally, on information and belief, Leeper disclosed to others at Denali and used the intercepted messages in violation of 18 U.S.C. § 2511(1)(c)-(d).

51. At all relevant times, Leeper was an employee and high-level executive of Denali. He committed the interceptions described above at least in part on Denali's behalf, for its commercial benefit, and within the scope of his role as Denali's CTO. Thus, Denali is vicariously liable for those interceptions.

52. Under 18 U.S.C. § 2520(b)-(c), Columbia is entitled to recover (i) the greater of (a) its actual damages and any profits made by Defendants as a result of the violations described above, or (b) statutory damages of $100 per day for each day of violation or $10,000, whichever is greater; (ii) punitive damages in an amount to be proven at trial; and (iii) the reasonable attorneys' fees and costs it incurs in bringing this action.

THIRD CLAIM FOR RELIEF
(Conversion)
(Both Defendants)

53. Columbia repeats and incorporates by reference, as if fully set forth herein, the allegations in all preceding paragraphs.

54. The emails and other confidential business information that Defendants unlawfully accessed, including, among others, email messages and documents related to the IT Department's confidential long-range planning, are Columbia's exclusive property. Columbia takes steps to keep that information confidential, and to ensure that nobody other than specific, authorized Columbia employees accesses it. Columbia also takes steps to control the information's dissemination, and to ensure that it is not transmitted to computers or other electronic devices other than those belonging to Columbia employees authorized to access and view the information.

55. By unlawfully accessing Columbia's emails and other confidential business information, Leeper exercised dominion and control over Columbia's property in a manner inconsistent with Columbia's right to control it. Specifically, by unlawfully accessing the information following the termination of his Columbia employment, Leeper exercised control over it in a manner inconsistent with Columbia's right to keep that information confidential; as described above, neither Defendant was authorized to access or view the private email accounts into which Leeper hacked, or to access or view Columbia's other confidential business information.

56. Additionally, by unlawfully causing Columbia's computer servers to transmit Columbia's confidential business information to the computers or other electronic devices he used to commit the hacking, Leeper exercised control over the information in a manner

inconsistent with Columbia's right to limit its dissemination to computers or other electronic devices belonging to authorized Columbia employees.

57. At all relevant times, Leeper was an employee and high-level executive of Denali. He committed the conversion described above at least in part on Denali's behalf, for its commercial benefit, and within the scope of his role as Denali's CTO. Thus, Denali is vicariously liable for Leeper's conversion.

58. As a result of Defendants' conversion, Columbia has suffered damages, including the costs associated with remediating the intrusions described above. Columbia is entitled to awards of economic damages and punitive damages in amounts to be proven at trial.

FOURTH CLAIM FOR RELIEF
(Breach of the Duty of Loyalty)
(Defendant Leeper)

59. Columbia repeats and incorporates by reference, as if fully set forth herein, the allegations in all preceding paragraphs.

60. At all times during his employment, Leeper owed a duty of undivided loyalty to Columbia.

61. Leeper breached his duty of loyalty to Columbia by secretly creating the jmanning account and, on information and belief, by giving the svcmom account additional "permissions" to access other employees' email accounts, each for the purpose of unlawfully accessing Columbia's private computer network after his resignation and obtaining information with which Denali could secure an unfair commercial advantage; by failing to disclose his misconduct to Columbia; and, on information and belief, in other ways.

62. Leeper accomplished his breaches of his duty of loyalty to Columbia through fraud and deceit. In creating the jmanning account, he used a false name that would seem

innocuous if another user happened upon it. Additionally, as one of the employees responsible for maintaining Columbia's global IT systems, Leeper had a duty to disclose to Columbia any breach or potential breach of those systems. His failure to disclose his creation of the jmanning account or his alterations to the svcmom account was both fraudulent and deceitful.

63. Due to Leeper's concealment, Columbia could not have discovered Leeper's breaches of his duty of loyalty through the exercise of reasonable diligence.

64. As a result of Leeper's breaches of his duty of loyalty to Columbia, Columbia has suffered damages, including the costs associated with remediating the intrusions described above. Columbia is entitled to awards of economic damages and punitive damages in amounts to be proven at trial.

JURY DEMAND

65. Columbia hereby demands a trial by jury as to all issues so triable in this action.

PRAYER

WHEREFORE, Columbia prays for relief as follows:

1. An order preliminarily and permanently enjoining Defendants, and all persons acting in concert with or on behalf of Defendants, from using, disclosing, or possessing any Columbia information accessed, viewed, or otherwise obtained as a result of their unlawful intrusions into Columbia's private computer network, to the extent Defendants possess any such information;

2. An award of damages, including but not limited to economic, statutory, and punitive damages, as permitted by law and in amounts to be proven at trial;

3. The reasonable attorneys' fees and costs that Columbia incurs in bringing this action;

4. Pre- and post-judgment interest as allowed by law; and

5. Such other relief as the Court may deem just and proper.

DATED this 1st day of March, 2017.

ANGELI LAW GROUP LLC

s/*Kelly M. Diephuis*
KELLY M. DIEPHUIS, OSB. No. 081704
EDWARD A. PIPER, OSB No. 141609
Ph: (503) 954-2232

Attorneys for Plaintiff Columbia Sportswear Company