IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF PUERTO RICO

TLS MANAGEMENT AND MARKETING SERVICES LLC,
Plaintiff,

v.

RICKY RODRÍGUEZ-TOLEDO, *et al.*,
Defendants.

Civil No. 15–2121 (BJM)

OPINION IN A NON-JURY TRIAL

TLS Management and Marketing Services LLC ("TLS") brought this action under the court's federal question and supplemental jurisdiction against Ricky Rodríguez-Toledo ("Rodríguez"), Lorraine Ramos ("Ramos"), Miguel Santo Domingo-Ortiz ("Santo Domingo"), ASG Accounting Solutions Group, Inc. ("ASG"), and Global Outsourcing Services LLC ("GOS"), alleging violations of Titles I and II of the Electronic Communications Privacy Act ("ECPA"); violations of the Puerto Rico Commercial and Industrial Trade Secret Protection Act, (the "Trade Secret Act"), 10 L.P.R.A. §§ 4131–4141; breach of contract, under Articles 1044, 1054, 1077 and 1206 of the Puerto Rico Civil Code, 31 L.P.R.A. §§ 2994, 3018, 3052, 3371; conversion, under Article 1802 of the Puerto Rico Civil Code, 31 L.P.R.A. § 5141; and tortious interference with various contracts, under Article 1802 of the Puerto Rico Civil Code. 31 L.P.R.A. § 5141. Dkt. 74.

I dismissed TLS's claims under Title II of ECPA, the Stored Communications Act. Dkt. 173 at 12. I denied summary judgment on TLS's claims under Title I of ECPA (the "Wiretap Act") and the Trade Secret Act. I also denied summary judgment on TLS's breach of contract claims against Rodríguez, ASG, and GOS for use and disclosure of the buy-sell agreement and the loan program. I granted TLS's motions for summary judgment on its breach of contract claims against Rodríguez, ASG, and GOS for disclosure of the loan agreement and operating agreement, and against Rodríguez and ASG for disclosure of the U.S. Possession Strategy and retention of TLS's Confidential Information. I also granted GOS's motion for summary judgment on TLS's breach of contract claims against it for disclosure of the U.S. Possession Strategy and retention of TLS's

Confidential Information. I granted Defendants' motion for summary judgment on TLS's conversion claim and tortious interference claims. I dismissed TLS's causes of action against Ramos except for those under the Wiretap Act. Dkt. 383 at 27. And I dismissed TLS's causes of action again Santo Domingo. Dkt. 507.

The case proceeded to a five-day, non-jury trial on the surviving claims. The parties submitted post-trial briefs. Dkts. 524, 525. The case is before me on consent of the parties. Dkt. 93. Remaining are TLS's claims under the Wiretap Act against Ramos, Rodríguez, ASG, and GOS; under the Trade Secret Act against Rodríguez, ASG, and GOS; and for breach of contract against Rodríguez, ASG, and GOS for the use of buy-sell agreements and loan programs. The court also considers what, if any, remedies are appropriate.

FINDINGS OF FACT

The following findings of fact were stipulated by the parties in their proposed pretrial order or proven by a preponderance of the evidence at trial. *See* Dkt. 419.

1. Tax Law Solutions, LLC, was formed in Puerto Rico on June 28, 2010. In 2012, it changed its name to TLS Management and Marketing Services, LLC ("TLS").
2. TLS is a Puerto Rico-based tax planning and consulting firm divided into the Consulting Division and the Puerto Rico Division.
3. TLS's principals are David A. Runge and Richard M. Colombik.
4. Colombik testified that, in his opinion, the Consulting Division is valued at about $4.8 million and the Puerto Rico Division is valued at about $30 million.
5. The Consulting Division creates a personalized Capital Preservation Report ("CPR") for its clients to advise them on how to reduce tax liability. The CPR is the Consulting Division's main product and has been revised about sixty times.
6. TLS's Puerto Rico Division offers a U.S. Possession Strategy ("the Strategy").

7. The Strategy reduces the tax liability of its clientele through strategic use of Puerto Rico's Act 20 and Act 73 tax exemption decrees. The Strategy is implemented through documents, including loan applications, buy-sell agreements, and operating agreements.
8. TLS claims as trade secrets the methods underlying the Strategy, as well as the current and potential client lists, contractor roster, implementation documents and forms, and pricing model.
9. Accounting Solutions Group ("ASG") is a corporation duly organized under the laws of the Commonwealth of Puerto Rico on August 2, 2007. ASG's only stockholder is Ricky Rodríguez.
10. ASG is a boutique firm that offers services in corporate structures, tax planning and preparation, consulting, auditing, and forensic accounting, among others.
11. As part of its services for TLS, ASG handled clients under Puerto Rico tax incentive Act 20 and Act 73.
12. Lorraine Ramos is the wife of Ricky Rodríguez. She is an accountant but does not have a CPA license.
13. Ramos has worked at ASG as a subcontractor. Her work consists of bookkeeping tasks and occupies about one to three hours every month.
14. Ramos is a self-professed technophobe.
15. On March 13, 2012, ASG signed a Subcontractor Agreement ("SCA") with TLS.
16. The SCA included a confidentiality clause and a non-compete clause. The confidentiality clause states: "Except as authorized in writing by TLS, neither Subcontractor nor any entity controlling, controlled by or under common control with Subcontractor (collectively, 'Subcontractor Affiliates') will at any time, directly or indirectly, disclose or utilize in any manner including for Subcontractor's own pecuniary gain, Confidential Information of TLS. Subcontractor may only use Confidential Information of TLS for a purpose that is necessary in carrying out the provisions or this Agreement." Joint Ex. II ¶ 5.1.

17. The court struck the the non-compete clause because it is invalid under Puerto Rican law. Dkt. 383 at 16; *see Arthur Young & Co. v. Vega III*, No. RE-91-508, 1994 WL 909262 (P.R. May 24, 1994) (noncompetition agreements without geographic, temporal, or client limits are invalid).

18. The SCA defines confidential information as "business methods and procedures, clients or prospective clients ('TLS Clients'), agent lists, marketing channels and relationships, marketing methods, costs, prices, products, formulae, compositions, methods, systems, procedures, prospective and executed contracts and other business arrangements, proposals and project plans, and TLS Affiliates." Joint Ex. II at ¶ 5.2.1.

19. The SCA includes as confidential "TLS reports and any information contained therein, related work products including implementation documents, and any other information provided to Client by TLS or TLS Affiliates by or in connection with proposing or delivering TLS Services." Joint Ex. II at ¶ 5.2.2.

20. The SCA includes as confidential the "identities of agents, contractors, consultants, sales representatives, sales associates, subsidiaries, strategic partners, licensors, licensees, TLS Clients, suppliers, or other TLS service providers or sources of supply." Joint Ex. II at ¶ 5.2.3.

21. The SCA states: "TLS Confidential Information shall not include (a) information disclosed with the prior written consent of TLS, (b) information that has been previously disclosed by TLS to the general public, (c) information that is required to be disclosed pursuant to a valid judicial court order, but only to the extent of and for the purpose of such order, and only if after receiving such an order Subcontractor provides timely notice of such order to TLS and cooperates reasonably with TLS's efforts to contest or limit the scope of such order, or (d) any strategy or methodology contained in the TLS Plan that is currently being utilized by Subcontractor or any of Subcontractor's other clients as a result of Subcontractor's prior recommendations (the 'Excluded Strategies')." Joint Ex. II ¶ 5.3.

22. TLS considers any works made for hire under the SCA to be TLS confidential information. Joint Ex. II at ¶ 7.1.

23. The SCA required subcontractors to "return to TLS any Intellectual Property of TLS in Subcontractor's possession" upon termination of the agreement. Joint Ex. II ¶ 8.4.2.

24. By its own terms, the confidentiality clause survives any termination of the SCA. Joint Ex. II ¶ 8.4.3.

25. The SCA provides for equitable remedies in case of breach. "The Parties recognize and acknowledge that irreparable damage without an adequate remedy at law may result from a breach of the Confidentiality and Non-Competition sections of this Agreement." Joint Ex. II at ¶ 9.2.1.

26. By signing the SCA, the subcontractor agrees that TLS may apply for an injunction and, if granted and upheld by a court, the subcontractor will "pay all legal fees and costs of TLS." Joint Ex. II at ¶ 9.2.1.

27. The SCA also provides that, where a court finds a breach of the confidentiality agreement, "TLS shall, in addition to all remedies at equity and law, be entitled to receive from Subcontractor 150% of all fees collected by Subcontractor for such unauthorized use of TLS Confidential Information and any fees to which TLS would have otherwise been entitled to receive from any third party if such unauthorized use of TLS Confidential Information also involved services that would have otherwise resulted in compensation to TLS from any third party, in contravention of this Agreement." Joint Ex. II at ¶ 9.2.2.

28. As a TLS subcontractor, ASG handled clients under Puerto Rico tax incentive Act 20 and Act 73. Rodríguez managed the termination and resignation process for employees and consultants, performed internal financial and accounting duties, and generally impressed Runge and Colombik.

29. Runge and Colombik offered Rodríguez the position of Managing Director at TLS. He accepted.

30. On September 1, 2012, Rodríguez became a TLS employee.

31. On September 1, 2012, Rodríguez signed a Confidentiality and Non-Disclosure Agreement with TLS ("NDA") that included a confidentiality clause. Joint Ex. V.

32. The NDA states: "Whereas ('TLS') willingness to share Confidential Information is contingent on the ('Parties) agreement to keep such information confidential and to use such information only in accordance with the terms and conditions of this Agreement." Joint Ex. V at 1.

33. The NDA includes a confidentiality clause. "Except as authorized in writing, neither Party nor any entity controlling, controlled by or under common control with such Party (collectively, 'Affiliates') will at any time, directly or indirectly, disclose Confidential Information of the other Party." Joint Ex. V at ¶ 1.1.

34. The NDA defines confidential information as "[a]ll information, whether written or otherwise and whether or not it is marked 'confidential', 'proprietary', or 'copyright' at the time of disclosure, regarding ('TLS') business methods and procedures, clients or prospective clients, agent lists, marketing channels and relationships, marketing methods, costs, prices, products, formulas, compositions, methods, systems, procedures, prospective and executed contracts and other business arrangements, proposals and project plans, and ('TLS') Affiliates." Joint Ex. V at ¶ 1.2.1.

35. The NDA includes as confidential TLS "reports and any information contained therein, related work products including implementation documents, client and/or prospective client personal and/or financial information, and any other information provided to ('Recipient') by ('TLS') or ('TLS') Affiliates by or in connection with proposing or delivering ('TLS Services') (individually or collectively, TLS Plans)." Joint Ex. V at ¶ 1.2.2.

36. The NDA includes as confidential "[t]he identities of agents, contractors, consultants, sales representatives, sales associates, subsidiaries, strategic partners, licensors, licensees, customers, prospective customers, suppliers, or other service providers or sources of supply including firms in which a ('TLS') Principal may have an ownership interest (collectively, 'TLS' Affiliates')." Joint Ex. V at ¶ 1.2.3.

37. Like the SCA, the NDA includes an equitable remedies section in which the parties agree that "irreparable damage without an adequate remedy at law may result from a breach of this

Agreement . . . . Each Party agrees to pay all legal fees and costs of the other Party if a preliminary or permanent injunction is ordered due to the actions or inactions of the other Party." Joint Ex. V ¶ 2.1.

38. Runge testified that TLS goes to "great lengths" to protect its confidential information.

39. To protect its confidential information, TLS requires employees, contractors and affiliates, potential and current clients, and outside consultants to sign nondisclosure and non-competition agreements. When TLS hosts conferences, all attendees must also sign confidentiality agreements. U.S. Possession Strategy details are made clear only to people who have signed NDAs.

40. TLS stores hard copies of original, signed documents in a secure filing cabinet at its office.

41. When Rodríguez began working at TLS, client information was scattered among different consultants and contractors' computers. Rodríguez suggested purchasing a TLS Dropbox license to keep all files in the same, central location.

42. Dropbox is a cloud-based storage system for digital files. A Dropbox user can access his account on any device connected to the Internet at www.dropbox.com or through a desktop application on a personal computer. These methods are not exclusive—both may be used to access the same account. The user simply logs in with the username and password associated with that account. This cloud-based storage system permits a user to upload files to his Dropbox account and then, later, access or download those files; the user may use the same or a different device to do this. In essence, Dropbox stores files and the Internet performs the transmission function that enables a user to sync his desktop application with the folders stored in the cloud. The cloud serves as the storage hub for a Dropbox account, and connecting to that hub permits access to the files stored, whether by download or by synchronization.

43. Dropbox users may set the Dropbox account on their personal devices to sync automatically with the folders on the server or cloud. Dropbox users may also choose to manually sync the Dropbox account on their personal devices.

44. When a user is logged in to Dropbox and has an account set to sync automatically, it can take up to ten or fifteen seconds for a file to upload or download based on the file size and Internet speed. If a user does not sync automatically, a manual sync can take a similar amount of time, which also depends on the file size and Internet speed.

45. If a Dropbox user does not sync his account on his device with the folders in the Dropbox cloud, then the folders and files will remain in storage in the cloud until they are synced. The user who manually syncs his account essentially directs Dropbox to send the changes made to folders and files to his device from the cloud. Without this instruction, those folders and files would remain in the cloud.

46. TLS purchased a Dropbox business license to store its electronic information.

47. Rodríguez served as the Dropbox administrator.

48. At the time of the events giving rise to this case only key employees had TLS-issued laptops. Contractors and others used personal laptops to access their TLS Dropbox accounts.

49. People with TLS laptops were supposed to use only TLS laptops to access TLS confidential information, although this policy was never made explicit.

50. Runge and Colombik trusted employees to use their professional judgment when it came to handling confidential information, and they believe that the NDA provided some guidance. TLS did not provide written policies or official guidelines beyond the NDAs.

51. TLS had no specific written policies regarding Dropbox access, password-sharing, or document-sharing.

52. Employees, consultants, and other TLS affiliates needed permission to access certain documents and files; it appears that such permission was merely a password and access to the TLS Dropbox account.

53. TLS has no policy on handling confidential information; on photocopying, printing, or sharing files; on protecting TLS-issued laptops from hacking or viruses; on protecting personal laptops used for TLS business from hacking or viruses; or on using firewalls, encryption, or other measures to secure data.

54. The CPR is never distributed electronically. The CPR is only distributed in hard copy format, printed on paper that cannot be photocopied. When the CPR is photocopied, the resulting copy appears as if all of the printed material were blacked out.

55. Rodríguez's copy of the TLS Dropbox account contents indicate that about fifty-five documents included the words "confidential" or "confidentiality" in the name. Of those, the vast majority were confidentiality agreements. Only a handful were marked "confidential" as if to indicate that the contents of the file were confidential in a privileged sense. *See* Ex. 67.

56. The copy of the TLS Dropbox account does not contain documents or folders labeled "secret," "proprietary," or "copyright," although three files refer to literal copyrights in the file name. *See* Ex. 67.

57. Runge and Colombik did not instruct Rodríguez on the Dropbox settings for file-sharing or access. Rodríguez did not adjust the default Dropbox settings.

58. Dropbox offers additional settings that enable a user to impose additional access restrictions on certain shared folders, for example.

59. Rodríguez created Dropbox accounts for TLS employees.

60. Employees who exited TLS had to return their equipment and key to the office. There was not a termination policy with regard to Dropbox account access.

61. In his TLS Dropbox account, Rodríguez had a folder named "RRT- Confidential File TLS".

62. When he sought to add non-TLS employee accounts to the Dropbox in June 2014, Rodríguez asked for and received permission from Runge. Rodríguez created an account for ASG within the TLS Dropbox, using Ramos's name and her ASG email. Ex. 61.

63. ASG's new TLS Dropbox account was intended not for Ramos but for Rodríguez. Rodríguez wanted to be able to access his ASG files from his TLS Dropbox account because he still worked with clients at ASG while working at TLS. He used Ramos's name to differentiate his TLS account from the ASG account.

64. Dropbox records all file activity in a log. This Dropbox log identifies which accounts logged in, uploaded files to the server, accessed particular folders and files, downloaded files from the server, and were removed from the Dropbox account.

65. A Dropbox log reflecting the devices linked to the TLS Dropbox, creation and sharing of folders, logins, downloaded links and other activity for February 2014 through January 2015 indicates that the account under Ramos's name accessed the Dropbox a handful of times. Ex. 61.

66. In June 2014, Rodríguez created TLS Dropbox accounts for the Producer's Guild and Management Services International. These were also non-TLS employee accounts that Runge approved.

67. As managing director, Rodríguez worked mainly with the Puerto Rico Division. He was not involved in the Consulting Division and did not handle CPRs.

68. The Consulting Division often referred clients to the Puerto Rico Division to join the U.S. Possession Strategy it offered.

69. Rodríguez managed finances for TLS and, on occasion, personal tax filings for Runge and Colombik.

70. Rodríguez was closely involved with the U.S. Possession Strategy. He knew how it worked, managed its implementation for clients, and often explained to clients the structure and governing documents that facilitated the Strategy.

71. Prior to working at TLS, Rodríguez had not performed work pertaining to tax exemption decrees or the Strategy. Neither ASG nor GOS had performed work pertaining to tax exemption decrees or the Strategy prior to Rodríguez working at TLS.

72. TLS has used at relevant times a loan program.

73. As part of the documents utilized for the Strategy, TLS used at relevant times a loan application, a buy-sell agreement, and an operating agreement.

74. Rodríguez created the loan application that TLS used. He downloaded a template from the Internet, and TLS customized it according to its needs.

75. Entire sections of TLS's operating agreement can be found on the Internet on other templates for operating agreements.

76. Loan programs, loan applications, operating agreements, and buy-sell agreements are all standard categories of document used in the tax-planning field and in corporate structuring.

77. Santo Domingo is an entrepreneur and Rodríguez's childhood friend. He holds a law degree and is a notary public.

78. Santo Domingo began working for TLS in September 2012, although he did not sign a confidentiality agreement until the following February.

79. Santo Domingo performed mainly non-business activities for TLS: finding an office, hiring a tour service for a client, arranging music for a conference, and helping a TLS client design a website.

80. During the period Santo Domingo worked for TLS but before he signed a confidentiality agreement, Rodríguez asked him to review the venue clause of some template contracts and notarize a few documents. The contracts included marketing services contracts and a corporate rights assignment.

81. On February 11, 2013, Santo Domingo signed a "Confidentiality and Non-Competition Agreement" with TLS to provide services as a subcontractor.

82. At the end of 2013, Santo Domingo stopped providing services for TLS.

83. In July 2014, Santo Domingo incorporated Global Outsourcing Services ("GOS"). Santo Domingo planned to attract business people to bring their assets to Puerto Rico in order to enjoy the benefits of its tax exemption laws.

84. Around or prior to October 2014, Rodríguez provided Santo Domingo a list of bullet points on the business milestones to be completed for GOS. Rodríguez also directed him to the proper office to apply for an Act 20 exemption decree.

85. Like TLS, GOS had a loan program, used a loan application, and had a buy-sell agreement.

86. Santo Domingo created the buy-sell agreement for GOS.

87. At the beginning of 2014, Rodríguez sent Runge a number of emails complaining about his compensation. Rodríguez felt that his salary should grow in proportion with his increasing responsibilities at TLS.

88. Runge asked Rodríguez to submit a formal request for a raise in March 2014. In response, Rodríguez submitted an industry analysis of CEO salaries.

89. Runge and Rodríguez's accounts differ over the intention behind the analysis Rodríguez submitted, but both agreed at trial that the benchmark number ($750,000) was much larger than TLS could afford. *See* Ex. 37.

90. Rodríguez did not receive a raise, and the discussions strained his business relationship with TLS.

91. Rodríguez began to feel disenchanted with TLS.

92. In April 2014, Runge invited Rodríguez and Santo Domingo to his apartment to discuss a new line of business in the insurance industry. Colombik did not attend the meeting, which struck Rodríguez as odd; he requested Colombik attend future meetings. Santo Domingo and Rodríguez now disagree as to whether it was a U.S. Possession Strategy project or whether it an entirely new entrepreneurial scheme.

93. Santo Domingo and Rodríguez began researching the insurance idea's potential. After a month or two, Rodríguez informed Santo Domingo that the idea would not come to fruition based on information from Runge.

94. A few other, work-related events in 2014 made Rodríguez feel uncomfortable in his role at TLS. Rodríguez thought that the climate had changed, and Runge and Colombik no longer respected his business acumen.

95. On September 3, 2014, Rodríguez copied the following documents from his TLS Dropbox account and placed them in a GOS subfolder of his linked ASG folder: 1) a template of an Operating agreement which Colombik had given to him; 2) a certificate template; 3) a loan program application; 4) a promissory note; 5) a security agreement; and 6) a certificate ledger.

96. Later in September 2014, Rodríguez brought a Western Digital, external hard drive to work and copied the complete contents of the TLS Dropbox account onto an external hard drive. The copied information included templates for TLS forms, client loan applications and buy-sell agreements, lists of current and potential TLS clients, TLS contractors, valuation reports, a new insurance strategy, two CPRs, and other information TLS considers confidential. The drive contained about twenty-six gigabytes of information in total. *See* Ex. 67.

97. The templates and forms copied are standard types of forms in the industry, but TLS, like many companies, personalized them and puts them to particular uses within their own business model.

98. Rodríguez concedes that he did not have authority to copy the contents of the TLS Dropbox account.

99. On January 16, 2015, Rodríguez resigned from TLS.

100. On January 16, 2015, Rodríguez returned his office key, instructed Human Resources to remove him from the payroll, and left the building. Rodríguez notified Runge via email, effective immediately. Ex. 1.

101. Later on, in another communication to Runge, Rodríguez cited poor compensation and general dissatisfaction as factors motivating his resignation.

102. On January 16, 2015, Rodríguez did not remove TLS confidential information from his ASG laptop or disable its TLS Dropbox access. Rodríguez states that he did not access the TLS Dropbox account after his resignation.

103. Rodríguez did not delete the files he copied on September 3, 2014. Rodríguez did not return the external hard drive or wipe the copied TLS Dropbox data from it.

104. After his resignation, Rodríguez asked the principals at then-current TLS client Marlin Environmental ("Marlin") to post references for Rodríguez on his LinkedIn page.

105. In late January or February 2015, Rodríguez took a 70% ownership stake in GOS and began working there.

106. By early 2017, Santo Domingo left GOS, and Rodríguez became the sole owner.

107. In order to provide tax exemption services in Puerto Rico, GOS obtained a tax exemption decree under Act 20.

108. Rodríguez used two of the TLS documents he copied; he modified a loan application for a GOS client, and he used the TLS operating agreement to structure GOS.

109. The GOS website advertised a new insurance solution in language evoking the idea contemplated in Runge, Santo Domingo, and Rodríguez's discussions in April 2014. Ex. 66. GOS never provided the insurance solution to a client.

110. Rodríguez also sought referrals for GOS and contracted with some TLS clients and a former TLS advisor to act as referral sources for GOS. The referral sources did not provide referrals.

111. Rodríguez personally contacted two other TLS clients on GOS's behalf. Ultimately, he met with only one to discuss tax alternatives in Puerto Rico.

112. GOS attracted only one client. That client was not connected to TLS.

113. Harris Hospice ("Harris"), a TLS client, decided to leave TLS in February 2015. Its principal obtained Rodríguez's contact information and asked him to help exit the Strategy.

114. On May 25, 2015, Marlin engaged the services of ASG for "consulting services to assist… ('Client') in the tax compliance review of several transactions they are executing that compromises the tax jurisdictions of the U.S. and the Commonwealth of Puerto Rico."

115. On June 8, 2015, Harris engaged ASG "for consulting services."

116. On June 11, 2015, Marlin signed a new engagement letter with ASG for tax compliance review and the setup of a limited liability corporation ("LLC"). Marlin's attorney provided all forms needed for Marlin's LLC.

117. On June 18, 2015, Harris engaged ASG to create and structure an LLC to facilitate their exit from the Strategy. Exs. XI, XI-a.

118. Marlin paid ASG $2,162.50 for services rendered. Ex. 44.

119. Harris paid ASG $8,690.00 for services rendered. Exs. 38, 40, 48.

120. ASG used the TLS operating agreement template that Colombik had provided to Rodríguez in his capacity as managing director in order to set up Harris's new corporation.

121. Harris and Marlin each sent Rodríguez all of their documentation relating to the U.S. Possession Strategy, which Rodríguez used to prepare memoranda on the most tax efficient way to exit TLS.

122. Rodríguez sent emails to the principals of Harris and of Marlin commenting on TLS information that they forwarded and offering his analysis and advice on Runge's emails. Rodríguez commented on elements of the Strategy, including pricing, implementation and exit, and other business procedures. *See, e.g.*, Exs. 39, 41, 42, 45.

123. Rodríguez concedes that he referred to TLS pricing formulae and other information that belonged to TLS in these emails and did not have express written authority to do so.

124. Runge testified that TLS had difficulty settling on an appropriate pricing structure for the Strategy. TLS tried several different pricing schemes before settling on the version that it currently uses.

125. For both Harris and Marlin, TLS rejected the proposed exit strategies, and the proposed LLCs were not formed.

126. TLS commenced this lawsuit in August 2015. Dkt. 1.

127. In September 2015, TLS sent Defendants litigation hold notices requesting the preservation of "all documents, data, and electronic information from all sources related to the subject matter of this litigation."

128. In February 2015, Rodríguez transferred all the data on his ASG-issued laptop, which still had limited access to the TLS Dropbox account, to a new laptop. He gave the ASG laptop to his children and discarded it a few months later when it stopped working.

129. Rodríguez and Ramos both used this laptop for ASG work. At trial, they both claimed that only he used it to access Dropbox despite Ramos's interrogatory responses to the contrary. The testimony was credible, however, and it is probable that the handful of logins from the Ramos account reflect Rodríguez's activity. Ex. 61.

130. The ASG laptop and the data it contained are the object of an adverse inference instruction. Dkt. 212.

131. In 2016, Rodríguez passed all the TLS Dropbox account information from the Western Digital hard drive to three flash drives, one of which he gave to his counsel in the instant case. *See* Ex. 67.

132. Rodríguez disclosed the other two flash drives containing the TLS Dropbox account information to the Internal Revenue Service ("IRS").

133. At trial, Rodríguez identified three companies that provided services resembling the Strategy: Capstone Capital, Trident RMC, and Caribbean Consulting Partners.

134. Capstone Capital was founded in April 2013 after TLS presented the Strategy to its managing director. It offers insurance-linked securities and life-policy aggregation, which are not services TLS provides.

135. Trident RMC is a management and consultant company that offers outsourcing to Puerto Rico and reduced tax liability for its clients. Trident was founded in 2015 by Michael Sciotti, a former TLS employee, who Rodríguez had hired. As part of his employment, he signed TLS's confidentiality and nondisclosure agreement. Sciotti was terminated from TLS on May 16, 2014. *See* Ex. 67.

136. Caribbean Consulting Partners was founded by the same lawyer who helped structure TLS.

DISCUSSION

I. The Wiretap Act

TLS claims that after Rodríguez resigned in January 2015, Defendants violated the Wiretap Act by intercepting TLS confidential information contained in the TLS Dropbox account by accessing it through Rodríguez's ASG laptop computer.

The Federal Wiretap Act, 18 U.S.C. §§ 2510–2522, "provides a private right of action against one who 'intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication.'" *In re Pharmatrak, Inc.*, 329 F.3d 9, 18 (1st Cir. 2003) (quoting 18 U.S.C. § 2511(1)(a), and citing 18 U.S.C. § 2520 (statutory provision authorizing a private right of action)). To establish a Wiretap Act claim, a plaintiff must show "that a defendant (1) intentionally (2) intercepted, endeavored to intercept or procured another person

to intercept or endeavor to intercept (3) the contents of (4) an electronic communication (5) using a device." *See Pharmatrak*, 329 F.3d at 18.

An "electronic communication" is "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12). A device is "any device or apparatus which can be used to intercept a wire, oral, or electronic communication." *Id*. at § 2510(5). "Intercept" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). Interception is otherwise understood broadly and consists of "captur[ing] or redirecting in any way" the contents of an electronic communication. *United States* v. *Rodriguez*, 968 F.2d 130, 136 (2d Cir. 1992); *accord Noel v. Hall*, 568 F.3d 743, 749 (9th Cir. 2009). The First Circuit has joined the other circuits who have considered the issue and "determined that ECPA . . . require[s] that communications be intercepted contemporaneously." *Boudreau v. Lussier*, No. 16-1049, 2018 U.S. App. Lexis 23283, at *29 (1st Cir. Aug 21, 2018).

Boudreau requires plaintiffs to engage in detailed, technical analysis of the mechanics of interception in order to meet their burden. *Id*. In *Boudreau*, the First Circuit affirmed a district court's grant of summary judgment on Wiretap Act claims against a defendant after he could not present sufficient evidence that his employer's capture of screenshots from his computer constituted "contemporaneous interception." *Id.* at 21. The opinion distinguishes a lay definition of "contemporaneous interception" from its technical meaning. The defendant argued that screenshots of email timestamps alongside a desktop computer clock with the same time of day qualified as proof of contemporaneity, but the First Circuit stated that stamps showing the same time do not "necessarily evince contemporaneous interception." *Id.* at 29. Determining contemporaneity "would require an understanding of, for example, among other things, what SSP actually does (and on what sort of time-scale it does it) when it captures a screenshot, what a web browser's progress bar actually indicates, and how exactly Yahoo! Mail auto-saves emails as a user

drafts them." *Id.* A court must be able to consider the "precise mechanism" by which interception occurs. *Id.* at 30; *cf. United States v. Councilman*, 418 F.3d at 67, 69 (1st Cir. 2005) (only after lengthy testimony as to how exactly email programs transmit data did the court hold that messages in "transient electronic storage" remained electronic communications in transit). Other circuit courts likewise emphasize the importance of expert testimony in order to analyze whether technology permits contemporaneous interception under ECPA. *Boudreau*, 2018 U.S. App. Lexis 23283, at *30 (citing *Luis v. Zang*, 833 F.3d 619, 631–32 (6th Cir. 2016); *United States v. Szymuskiewicz*, 622 F.3d 701, 703–04 (7th Cir. 2010)).

Dropbox differs from classic methods of electronic communication because users do not normally communicate with each other, as in email, but rather communicate with the Dropbox cloud by uploading, downloading, and syncing files. An interception in the Dropbox context takes the form not of duplicating or redirecting communications but rather syncing a Dropbox account in order to capture changes made to files on the Dropbox server. Synchronization arguably may fall into the broadly defined "intercept" because it represents the capture or redirection of a transmission, depending on the mechanics of how the interception occurs. *See Noel*, 568 F.3d at 749.

Importantly, however, Dropbox users have the option to either sync their own folders automatically with the folders on the server or to sync those folders manually. Defendants' expert testified that even when a user's Dropbox account is set to sync automatically and reflect changes made to a folder by other users or on other devices, it can take ten to fifteen seconds for a file to upload or download. On the other hand, if a user is not already logged into his account when the changes are made or does not elect to sync files automatically, then the communications are stored in the cloud. The user must then initiate the synchronization himself, causing the transmission of files from cloud to computer. This is more akin to direction than redirection. Without the user's action, the files would remain in the cloud. In the case of manual synchronization, there might be no existing transmission to intercept through redirection; rather, the user directs the transmission from beginning to end. This scenario is analogous to accessing files in permanent storage, which

exceeds the scope of the Wiretap Act. Nevertheless, electronic communication in "transient electronic storage that is intrinsic to the communication process" may still be intercepted within the meaning of the Wiretap Act in theory, provided the user's laptop was logged in and set to sync automatically. *See Boudreau*, 2018 U.S. App. Lexis 23283, at *30. Here, however, the record is silent as to whether Rodríguez's ASG laptop was set to sync automatically or whether it was ever logged in to the TLS Dropbox account so as to conceivably intercept any transmissions after Rodríguez left TLS.

TLS attributes the deficiency in proving contemporaneous interception to the discarded ASG laptop, and asks the court to invoke the adverse inference for spoliation. *See* Dkt. 212. TLS's expert claimed that the only way he could prove contemporaneity or interception was to analyze the laptop through which it allegedly occurred. Defendants' expert, however, noted that Dropbox retains a log of all file activity. This Dropbox log identifies which accounts uploaded files to the server, accessed particular folders and files, and downloaded files from the server. Defendants introduced into evidence a log indicating the devices linked to Dropbox, creation and sharing of folders, logins, and other activity for February through October 2014. *See* Ex. 61. This log supports the testimony that a similar record exists for the period between Rodríguez's resignation and when he discarded the ASG laptop. Strangely, neither party produced such a record, yet TLS never challenged Defendants' assertions that such a record exists and what it could potentially prove.

Rodríguez admitted that the ASG laptop retained access to the TLS Dropbox account after his resignation but denied TLS's claim that he accessed the TLS account. This log, it seems, would prove clearly whether or not Rodríguez automatically synced files from the Dropbox, thus redirecting TLS's transmissions. Because it would show both a login and any automatic or manual download, it would also clarify whether or not Rodríguez had the intent the Wiretap Act requires. TLS, as the plaintiff, has the burden here. Most troubling, TLS did not contradict the existence of this log. In light of this failure, the court accords very little weight to the adverse inference that arose due to Rodríguez's disposal of his laptop. With an adverse inference sanction, the "trier of fact may (*but need not*) infer from a party's obliteration of a document relevant to a litigated issue

that the contents of the document were unfavorable to that party." *Booker v. Mass. Dep't of Pub. Health*, 612 F.3d 34, 45 (1st Cir. 2010) (quoting *Testa v. Wal–Mart Stores, Inc.*, 144 F.3d 173, 177 (1st Cir. 1998)) (emphasis added); *see also Nation-Wide Check Corp. v. Forest Hills Distribs., Inc.*, 692 F.2d 214, 217 (1st Cir. 1982) ("When the contents of a document are relevant to an issue in a case, the trier of fact generally may receive the fact of the document's nonproduction or destruction as evidence that the party which has prevented production did so . . . [because] the contents would harm him.") (emphasis added). With additional doubt over whether there was a contemporaneous interception as opposed to access to stored documents, the weight of the evidence favors the Defendants. As a result, the court need not delve deeper into whether an automatic Dropbox synchronization, had it been proven, in fact qualifies as a contemporaneous interception under the Wiretap Act.

In the end, TLS has failed to prove by a preponderance of the evidence that Defendants intercepted any information from TLS's Dropbox account after Rodríguez left TLS in January 2015. Accordingly, I find that TLS has not proven by a preponderance of the evidence that Defendants violated the Wiretap Act.

II. The Trade Secret Act[1]

TLS claims as trade secrets the Capital Preservation Report ("CPR"), the U.S. Possession Strategy, and the confidential information that comprises the Strategy, as defined in the SCA and NDA. Mere subjective belief that something is a trade secret is not dispositive, however. *Trade Secrets* § 4.04 (Law Journal Press 2018) (citing *Fail-Safe, LLC v. A.O. Smith Corp.*, 674 F.3d 889, 894 (7th Cir. 2012)). To prevail, TLS must first show that its claimed trade secrets are (1)

[1] Puerto Rico adopted the Uniform Trade Secrets Act ("UTSA") in 2011. Nearly every state has adopted the UTSA. 1 MILGRIM ON TRADE SECRETS § 1.01(c)(i) (Matthew Bender 2018). Puerto Rico state court proceedings are conducted in Spanish and few, if any, trade secret cases have been translated into English, which is required for this court to consider them. *See* D.P.R. Civ. R. 5(g). In their briefs, the parties have relied exclusively on the statutory language, the facts of the case, and persuasive authority; they have neither translated nor stipulated to translations of case law. *See* Dkts. 524, 525. As such, this court will "begin with settled principles of state law and then consider persuasive authority from other jurisdictions and the teachings of learned treatises." *Wheeling & Lake Erie Ry. Co. v. Keach*, 799 F.3d 1, 10 (1st Cir. 2015).

information that (2) has financial value or provides a business advantage (3) because they are not common knowledge or readily accessible, and (4) TLS employs reasonable security measures to maintain secrecy. *See* 10 L.P.R.A. §§ 4132(a)–(b).

Then, TLS must prove that Defendants misappropriated those trade secrets. "Misappropriation" is defined as:

> (a) The acquisition of a trade secret belonging to another by a person who knew or should have known that he/she acquired such secret directly or indirectly through improper means, or
>
> (b) the disclosure or use of a trade secret belonging to another without his/her express or implicit consent, by a person who:
>
> > (1) used improper means to gain knowledge of the trade secret, or
> >
> > (2) at the time of disclosure or use, such person knew or should have known that such trade secret was:
> >
> > > (A) Obtained through a person who acquired such information through the use of improper means;
> > >
> > > (B) obtained under circumstances from which a duty to maintain confidentiality or to limit use ensues;
> > >
> > > (C) obtained through a person who had the duty-bound to the trade secret's owner to maintain confidentiality or limit use, or
> > >
> > > (D) known by accident or by mistake.

Id. at § 4134.

As a preliminary matter, Defendants argue that the CPR should not be included as a trade secret because TLS did not expressly claim it as a trade secret until trial began. Defendants cite Federal Rules of Civil Procedure 26 and 37 in support of excluding the CPR. Rule 26 also requires parties to timely supplement disclosures and responses "if the party learns that in some material respect the disclosure or response is incomplete" and has not otherwise been disclosed. Fed. R. Civ. Pro. 26(e)(1)(A). Failure to disclose information may result in exclusion of that information at trial unless "the failure was substantially justified or is harmless." Fed. R. Civ. Pro. 37(c)(1).

"Rule 26 promotes fairness both in the discovery process and at trial." *Thibeault v. Square D. Company*, 960 F.2d 239, 244 (1st Cir. 1992).

Defendants are correct that the CPR was not specifically listed in the pretrial order, Dkt. 419, and dispositive motions focused on the Strategy. Nor is the CPR listed explicitly in either the NDA or SCA as Confidential Information, though it falls under a "related work products . . . in connection with proposing or delivering" TLS services. Joint Ex. V ¶ 1.2.2.

TLS argues that it was unaware that Rodríguez's sweep of the Dropbox account included at least two CPRs until well after discovery ended. Defendants rightly respond that TLS knows precisely what is on its Dropbox account, has had continuous access to that account, and had three full months before trial during which it had a copy of the documents Rodríguez copied to examine the contents. By the same token, however, Defendants had the copied data for nearly four years before trial. Rodríguez admitted to copying the entire TLS Dropbox account, and he cannot now disavow responsibility for having copied documents with which he was unfamiliar. This is an entirely foreseeable consequence of his actions. Both parties were faced with an overwhelming quantity of data, but each party had access to that data, in some form or another, for the same period of time. Excluding the two CPRs on the drive would allow Defendants to pick and choose which claims TLS may bring against them in contravention of Rule 26's underlying intent that litigation be fair. Failure to explicitly disclose two documents on a hard drive with twenty-six gigabytes of information is substantially justified, especially when the information was already available to Defendants.

Moving on, the Trade Secret Act broadly defines "information." A trade secret could be any "[k]knowledge that broadens or clarifies knowledge already garnered. It includes, but is not limited to, any formula, compilation, method, technique, process, recipe, design, treatment, model or pattern." *Id.* § 4131(a). For trade secret purposes, "information" casts a wide net. Regardless of the broad scope, not all knowledge qualifies as trade secret-eligible information. TLS proposes that the CPR, the Strategy, and the documents and information underlying the Strategy all qualify as information protectable as trade secrets.

The CPR is a report that TLS customizes for each Consulting Division client. Colombik testified that the CPR embodies the Consulting Division. Each client receives a personalized CPR, and its underlying model evolves as laws and techniques change. The CPR has been revised about sixty times. It is distributed to clients, but disclosure through sale or other commercialization does not necessarily defeat a marketed product's trade secret status. *See Milgrim* § 1.05(2).

Methods, techniques, and what might be classified as "know-how" require a greater degree of precision and specificity when outlining what qualifies as a trade secret and what does not. *Milgrim* § 1.09(3). When skill, knowledge, and experience can be compiled to create a secret use that provides competitive advantage, that compilation may qualify as a trade secret. *Id.* (citing *SI Handling Sys., Inc. v. Heisley*, 753 F.2d 1244, 1261–1262 (3d Cir. 1985) (recognizing that certain methods and techniques merited trade secret protection but information that consisted only of employees' skill, knowledge and experience was not a trade secret). In this case, individual client information and public information contained in the CPR are not trade secrets. The method by which TLS compiles that information and the skill, knowledge, and experience used to compile it are the core of what can be protected as a trade secret. The CPR itself qualifies as a trade secret not because it covers knowledge or skill but because the compilation of that knowledge and skill, applied to client information, provides TLS with a competitive advantage. Here, TLS's claim of trade secret status for the CPR itself is appropriately specific and narrow. *See Milgrim*, § 1.09(3) ("If protection is sought for a very broad accumulation of knowledge and experience, a court might reject such claim as an attempt to simply cover knowledge and skill . . . a reasonable degree of precision and specificity is appropriate.")

The U.S. Possession Strategy is a tax-planning method dependent on Puerto Rico tax law and embodied in the documents TLS and its clients use to implement the Strategy. TLS argues that the Strategy and the different forms and templates used to implement the Strategy are trade secrets. These documents, in many cases, are standard templates for the creation and consummation of business relationships. However, "sometimes highly valuable trade secrets may have material in the same 'package' that is not a trade secret; the presence of such material should not in any way

negate the trade secret value of that which in fact is secret." *See* 1 Milgrim on Trade Secrets § 1.08(4) (Matthew Bender 2018).

The Strategy is analogous to the CPR; it is a process and method building on the knowledge and experience of employees that is used to give TLS a business advantage. *See Milgrim* § 1.09(3) (citing *SI Handling*, 753 F.2d at 1261–62). Including work product, such as the CPR or Strategy, interprets "information" sensibly. The same, however, cannot be said of the documents and data that underlie the Strategy.

The inclusion of these underlying documents in the NDA and SCA does not elevate them to trade secret status. *See Milgrim* § 4.02(1)(b) (citing *ITT Telecom Prods. Corp. v. Dooley*, 262 Cal. Rptr. 773 (Cal. Ct. App. 1989)). The SCA includes as confidential:

> business methods and procedures, clients or prospective clients ("TLS Clients"), agent lists, marketing channels and relationships, marketing methods, costs, prices, products, formulae, compositions, methods, systems, procedures, prospective and executed contracts and other business arrangements, proposals and project plans, and TLS Affiliates.

Joint Ex. II at ¶ 5.2.1. The SCA also includes as confidential "TLS reports and any information contained therein, related work products including implementation documents, and any other information provided to Client by TLS or TLS Affiliates by or in connection with proposing or delivering TLS Services." Joint Ex. II at ¶ 5.2.2.Finally, the SCA also considers confidential "identities of agents, contractors, consultants, sales representatives, sales associates, subsidiaries, strategic partners, licensors, licensees, TLS Clients, suppliers, or other TLS service providers or sources of supply." Joint Ex. II at ¶ 5.2.3. The NDA confidentiality clauses are equally sweeping. *See supra* Findings of Fact, ¶¶ 32–36.

"The mere presence of a confidentiality agreement does not elevate nontrade secret matter to trade secret status . . . [or] bestow even confidential status on information that is not in fact confidential." *Milgrim* § 4.02(1)(b). The documents and templates underlying the Strategy are all commonly used in the tax-planning industry. Granting trade secret protection for standard forms available online perverts the purpose of trade secret law. Trade secrets cannot be publicly available

information, and downloadable Internet forms and templates qualify as public information as much as tax exemption decrees and IRS guidelines. Accordingly, I find that the documents and forms that TLS uses to implement the Strategy are not by themselves protectable as trade secrets.

Courts are divided over whether customer lists and pricing methods may be accorded trade secret status. "The customer list cases stand on the periphery of that area of the law which can best be described as 'the trade secret quagmire.' The confusion created by decisions concerning the use of customer lists and customer contracts by ex-employees is due to the fact that the decisions seemingly turn on arbitrary distinctions unrelated to trade practices." *Crouch v. Swing Mach. Co.*, 468 S.W.2d 604, 606 (Tex. Civ. App. 1971). On the other hand, a trade secret may relate to those more peripheral aspects of business relations, such as pricing, marketing, and customer identity. Restatement (Third) of Unfair Competition § 39 cmt. d (Am. Law. Inst. 1995). "A customer list is not protectable as a trade secret under the rule stated in § 39 unless it is sufficiently valuable and secret to afford an economic advantage to a person who has access to the list." *Id.* at § 42 cmt. f. State courts are divided on the question of customer lists. *See Milgrim* § 1.09(7). Often, the question of whether a customer list is granted trade secret protection depends on whether it is readily ascertainable from another source or lacks value. This implicitly acknowledges that such a list is eligible for trade secret status. Pricing has been treated similarly, with state courts both granting and denying trade secret status to cost and pricing information. *Id.* at § 1.09(8)(b). This suggests that the determination depends on the facts presented at trial, so pricing also qualifies as "information" for the purposes of § 4131(a).

A claimed trade secret must also have "independent financial value or that provides a business advantage, insofar as such information is not common knowledge or readily accessible." 10 L.P.R.A. § 4132(a). The CPR is a closely guarded secret, shared only with clients and consisting of some public and some private information. Though an outsider might guess at its contents, structure, and method of analysis, there is no method by which it can be accessed absent a disclosure.

The Strategy's value, in contrast, depends on highly public information: Act 20 and Act 73 tax incentives, federal tax laws, and industry-standard forms. In fact, tax legislation is its keystone. Milgrim analogizes: "it may be said that painting constitutes only a novel combination of the three primary colors and (normally) two-dimensional forms. Yet the combinations are infinite. A trade secret is equally recognized when a familiar principle is given a new application." *Milgrim* § 1.07(5). Similarly, the laws and forms cannot achieve trade secret status due to their wide publication and ready accessibility. The Strategy, however, remains largely either unknown or inaccessible despite the commonly known information underlying it. Runge testified that, to his knowledge, no other company offered the same U.S. Possession Strategy that TLS markets, and Rodríguez identified only two companies that offer similar services, both involving a former TLS affiliate or consultant. Trade secret holders do not have to ensure absolute secrecy; they may make limited disclosures to further economic interest without losing trade secret status. *Metallurgical Indus. v. Fourtek, Inc.*, 790 F.2d 1195, 1200 (5th Cir. 1986) (citing Restatement of Torts, § 757 cmt. b (1939)). Disclosures to employees are a necessary part of growing a business, though subsequent use of the secret by said employee may indicate an issue with TLS's security measures. *See id.*

A Minnesota court ruled that trade secret status was not defeated merely because more than one company in an industry knew the information; as long as the information was not generally known, it could still enjoy trade secret status. *Electro-Craft Corp. v. Controlled Motion, Inc.*, 332 N.W.2d 890, 900 (Minn. 1983); *accord Fishkin v. Susquehanna Partners, G.P.*, 563 F. Supp. 2d 547, 582–586 (E.D. Pa. 2008) (noting that multiple companies may hold a trade secret, though the information at issue was too widely known and ascertainable to constitute a trade secret); *but see Wal-Mart Stores v. P.O. Mkt.*, 66 S.W.3d 620, 632–635 (Ark. 2002) (reversing a multimillion dollar award because the trade secret's individual elements were generally known and their combination was obvious to someone investigating the subject). Here, the knowledge of the Strategy originated with TLS and does not appear to be readily ascertainable by companies unaffiliated with TLS, so it meets the statutory requirement under § 4132(a).

Courts generally find that information has the required independent financial value if a competitor would find it useful and duplication would require cost, time, and effort. *Milgrim* § 1.07A. "In a similar vein, independent economic value is not 'assessed using hindsight,' i.e., the fact that a trade secret later turns out to not have been as valuable as originally thought does not mean that it did not have the requisite independent economic value at the time of misappropriation." *Id.* For example, were someone to misappropriate a trade secret but be unable to profit from it because a law or other necessary circumstance had changed, the trade secret's value would not be diminished.

Trade secrets that combine public and nonpublic information are often treated as independently valuable "as long as a competitor would have to incur considerable expense to recreate the combination." *Milgrim* § 1.01(2)(c)(iii)(C). The CPR has undergone sixty different revisions over the course of its lifespan. That it would require cost, time, and effort to duplicate the methods it contains seems clear. The Strategy, likewise, is updated and adjusted according to individual client's needs and changes in the applicable law. The two companies that Rodríguez noted which offer services similar to the U.S. Possession Strategy compete with TLS, and their impact on TLS's market share is unclear. Be that as it may, TLS litigates vigorously in defense of its intellectual property, indicating a baseline economic value that is often accepted as sufficient for this inquiry.

Next, TLS must prove that it took reasonable security measures to protect its claimed trade secrets. In large part, whether or not information qualifies as a trade secret is determined by its secret keepers. *See* 10 L.P.R.A. § 4133. Reasonable measures must be taken to maintain the confidentiality of a trade secret, or it loses its protected status. *Id.* A measure's reasonableness depends on the foreseeability of potential access, the risks associated with that access, and the cost-benefit ratio between the measure and the secret itself. *Id.* "Measures that can be deemed to be reasonable to maintain the confidentiality of the trade secret include," *inter alia*, "requiring company employees authorized to access such information to sign confidentiality agreements," "establishing control measures for the use of or access to such information by company

employees," or "implementing any technologically available measures when publishing or transmitting such information over the Internet, including the use of email, web pages, message boards, and any other equivalent medium." *Id.* §§ 4133(c), (g), (h).

Runge testified that TLS goes to "great lengths" to protect its confidential information. U.S. Possession Strategy details are made clear only to people who have signed NDAs, even when it comes to attracting prospective clients. TLS never issued the CPR in electronic format but rather distributed it to clients on paper that could not be photocopied. In the TLS Dropbox account, only two CPRs appeared, indicating that few electronic versions exist where general employees might access them. Likewise, a step-by-step description of the Strategy does not seem to appear in any single document or file on the Dropbox. Rather, implementation of the Strategy depends on the knowledge and experience of TLS's employees, who, as mentioned, are bound by NDAs. I find that these measures were reasonably sufficient to protect and maintain the confidentiality of the CPR and the Strategy.

The measures meant to protect the documents and information underlying the Strategy are a different matter. Beyond the broad SCA and NDA language, Runge and Colombik acknowledged that employees and others were trusted to use their professional judgment and discretion when handling confidential information. Employees, consultants, and affiliates needed password-protected accounts to access the TLS Dropbox account. Beyond a simple password, however, TLS has no policy on handling confidential information; on photocopying, printing, or sharing files; on protecting TLS-issued laptops from hacking or viruses; on protecting personal laptops used for TLS business from hacking or viruses; or on using firewalls, encryption, or other measures to secure data. Dropbox boasts additional security features besides a password, but neither Runge nor Colombik asked Rodríguez, who administered the TLS Dropbox, to instruct employees on its use, to restrict sharing capacities, or to limit access to certain folders or files. As a result, he did not do so. The contents of the Dropbox account that Rodríguez copied indicate that some documents were labeled "confidential" but not many and certainly not as many as TLS claims are trade secrets. *See*

Ex. 67. These unlabeled documents include client information and spreadsheets as well as pricing generally and for specific clients.

Reasonableness depends on "foreseeable conduct whereby the trade secret could be accessed and the nature of the risk ensuing from such conduct." 10 L.P.R.A. § 4133. When information is stored in the cloud for hundreds of employees, consultants, clients, advisors, and affiliates to access, it is clear that someone else might also attempt to get their hands on it. The fact that one former employee formed a competing company demonstrates that the claimed secrets were in demand and the confidentiality agreements might not be sufficient protection. The risk posed by unauthorized access, a company competing with TLS for market share and clients, is great. Runge identified the clients as the "revenue model" of their business; losing clients would impact revenue directly. Clearly, violations of the NDA were foreseeable and presented a danger to the Puerto Rico Division's survival. The documents and client identities left exposed in the Dropbox account simply were not protected to a reasonable degree.

A short cost-benefit analysis between potential security measures to mitigate those foreseeable risks and the trade secret indicates that TLS should have taken additional security measures had they wanted to properly protect the information underlying the Strategy. There were a number of ways TLS could have limited access to its confidential information at no or at minimal cost to themselves. TLS used only the basic default settings on Dropbox, but the Dropbox enables further protections that went unused. For example, sharing links and files could have been restricted. TLS also could have asked employees to label files and folders "confidential," "proprietary," or "secret." Some files on the account are labeled "confidential," but the number pales in comparison to the number claimed as trade secrets. *See* Ex. 67. A policy on password-sharing, on handling confidential information, and on file-sharing could have been inserted into the NDA that TLS required employees, consultants, and affiliates to sign.

These are all simply implemented, minimally expensive security measures with disproportionately large benefits. In comparison, TLS never issued the CPR in electronic format but rather distributed it to clients on paper that could not be photocopied. When TLS values its

Puerto Rico Division at more than six times its Consulting Division, it is reasonable to expect greater security measures in proportion to the greater value. The measures protecting the documents underlying the Strategy appear to have been haphazard and utterly dependent on confidentiality agreements and employee discretion. Especially in the digital age, where electronic information is always vulnerable, lacking clear policies on confidential information, technology, and digital security is unreasonable. TLS has shown by a preponderance of the evidence that the CPR and the Strategy qualify as trade secrets. TLS has not shown that the documents and information underlying the Strategy were the object of reasonable security measures, so those materials are denied trade secret status. This delineation between the documents and information composing the Strategy and the Strategy itself fits squarely within the trade secret canon. Trade secret law treats a whole as greater than the sum of its common, accessible, known parts. *Milgrim* § 1.08(4). When a trade secret consists of well-known components, there is extensive public literature, and the defendant is experienced and knowledgeable in the domain, there may still be trade secret protection. *Id.* at § 1.08(5). In those cases, "the scope of trade secret rights will be narrowly drawn to the plaintiff's precise utilization of the components." *Id.* Nor does this delineation affect the SCA and NDA's definitions of the underlying documents and information as "confidential." Contracts may provide confidentiality of information even in the absence of trade secret status. *See, e.g.*, *Dooley*, 262 Cal. Rptr at 781–82.

The next question is whether TLS has proven that Defendants misappropriated its trade secrets—namely the CPR and the Strategy. Misappropriation is "[t]he acquisition of a trade secret belonging to another by a person who knew or should have known that he/she acquired such secret directly or indirectly through improper means, or the disclosure or use of a trade secret belonging to another without his/her express or implicit consent." § 4134(a)–(b).

Here, although Rodríguez had legitimate access to the TLS Dropbox in general, he conceded that he acted without authority when he copied its entire contents in September 2014. That copy captured two CPRs. Accordingly, Rodríguez's unauthorized acquisition of the CPR violates § 4134(a).

In addition, Rodríguez meets the elements in § 4134(b)(2). That subsection identifies misappropriation as disclosure or use of another's trade secret without consent by a person who, "at the time of disclosure or use, such person knew or should have known that such trade secret was . . . obtained under circumstances from which a duty to maintain confidentiality or to limit use ensues . . . or known by accident or by mistake." § 4134(b)(2)(B), (2)(D). The language of § 4134(b) notably encompasses disclosure *or* use. Unauthorized disclosure of the CPR or the Strategy alone may support liability for misappropriation. 4 *Milgrim on Trade Secrets* § 15.01; *see, e.g.*, *StorageCraft Tech. Corp. v. Kirby*, 744 F.3d 1183, 1185 (10th Cir. 2014) (accepting an argument that, in the absence of any evidence of use, defendant's mere disclosure of a trade secret to a competitor gave plaintiff grounds for a reasonable royalty as relief).

Rodríguez both disclosed and used his knowledge of the Strategy in emails with TLS clients who sought to leave TLS. Harris, a TLS client, decided to exit the Strategy in February 2015, after Rodríguez left TLS. Harris formally engaged ASG for consulting services on June 8 and for arranging his exit from TLS via an LLC on June 18. During that time, Harris emailed Rodríguez all of its documentation relating to the Strategy. Rodríguez commented on it, gave Harris advice, and used it to prepare an exit strategy memorandum for Harris. Rodríguez opined on TLS's loan program, implementing the final Strategy stages, and TLS's pricing estimates. Ex. 39, 45. Harris paid ASG $8,690.00 for services rendered. Exs. 38, 40, 48.

Marlin, another TLS client, also decided to exit the Strategy and also engaged ASG to assist. On May 25, 2015, Marlin engaged ASG for consulting and tax compliance services; on June 11, Marlin engaged ASG to structure its exit from TLS. During that time, Marlin emailed Rodríguez all of its documentation relating to the Strategy. Rodríguez commented on it, gave Marlin advice, and used it to prepare an exit strategy memorandum. Exs. 41, 42. Marlin paid ASG $2,162.50 for services rendered. Ex. 44.

Rodríguez conceded that he did not have authority to refer to TLS information in these emails. That information encompassed non-trade secret documents and pricing but also Strategy implementation and the procedure by which clients could exit. As the former managing director of

TLS, a party to ASG's SCA, and a party to the NDA, Rodríguez had sufficient notice that he had a duty to "maintain confidentiality." He obtained the information in the course of his employment at TLS, a condition of which included signing an NDA. ASG was bound by the confidentiality clause in the SCA as well as in the NDA Rodríguez signed because it is an "entity . . . controlled by" Rodríguez. Joint Ex. V 1.1. Defendants argue that ASG never disclosed the Strategy because the clients provided the documents and everyone involved in the conversation was subject to nondisclosure and confidentiality agreements. This misapprehends the law. Even where a trade secret has been acquired properly, use or disclosure without authorization constitute misappropriation. *Milgrim* §1.01(2)(c)(ii). Although the clients may have largely understood the process by which they could exit TLS or the cost estimates of exiting the Strategy, it is unlikely that they were familiar with the mechanics of why they had to undergo such specific exit procedures or why TLS provided certain cost estimates. Furthermore, "use of a trade secret to injure the trade secret owner or for any purpose other than serving the interest of the trade secret owner will be seen as 'use' for misappropriation purposes." *Id.* Each customer retained ASG for the purpose of leaving TLS, and Rodríguez applied his knowledge of the Strategy to smooth the way for these clients.

With regard to the CPR, there is no evidence that Rodríguez used the two reports that he copied, nor is there evidence that he disclosed the CPR to clients or potential clients of ASG or GOS. TLS is not seeking liability under the Trade Secret Act for any disclosure to a regulatory agency. *See generally* Dkt. 419 at 54–55. As a result, the court does not need to reach Defendants' whistleblower defense. The court does, however, note that Puerto Rico provides whistleblower protections only for government employees, 1 L.P.R.A. § 601, and the Trade Secret Act, 10 L.P.R.A. §§ 4131 *et seq.*, makes no provision for non-governmental employees.

Accordingly, I find that TLS has proven by a preponderance of the evidence that Rodríguez and ASG violated the Trade Secret Act by misappropriating the CPR through wrongful acquisition and the Strategy through unauthorized disclosure and use.

III. Breach of Contract

"Under Puerto Rico law, a cause of action for breach of contract consists of three elements: (1) a valid contract, (2) a breach by one of the parties to the contract; and (3) resulting damages." *Ocasio v. Perfect Sweet Inc.*, No. 16-2012, 2018 U.S. Dist. LEXIS 124598, at *7 (D.P.R. July 23, 2018) (quoting *Mega Media Holdings, Inc. v. Aerco Broad. Corp.*, 852 F. Supp. 2d 189, 199 (D.P.R. 2012)). A party seeking damages must show a causal link between the breach and the damages sought. *See Nazario v. Vélez & Asoc.*, 98 T.S.P.R. 54 (P.R. 1998) ("As is known, when the breach of a contractual obligation causes harm to any of the contracting parties, an action for damages for breach of contract lies."); *see also Colon v. Blades*, 717 F. Supp. 2d 175, 185 (D.P.R. 2010) ("An action for damages for breach of contract . . . only lies when the damage suffered exclusively arises as a consequence of the breach of an obligation specifically agreed upon, which damage would not occur without the existence of a contract."). TLS alleges that Rodríguez, ASG, and GOS are all liable for breach of contract.

A number of TLS's breach of contract allegations were granted for the issue of liability at the summary judgment stage. Dkt. 383. The court held that ASG, GOS, and Rodríguez breached the confidentiality clauses in the contracts by taking and using TLS's loan agreement and operating agreement. *Id*. at 18. The court further held that Rodríguez and ASG violated the confidentiality clauses of the SCA and NDA by both using the Strategy and, through using it, disclosing it to the clients for whom they were working. *Id*. at 19. For the same claim the court granted summary judgment in favor of GOS. *Id*. at 20. The court also granted summary judgment for TLS's claim that ASG and Rodríguez breached the NDA and SCA by keeping files after their employment with TLS ended. Dkt. 383 at 20–21. GOS was granted summary judgment on the same claim. *Id*. TLS's remaining breach of contract issue at trial, apart from damages, was a claim against Rodríguez, ASG, and GOS for using similar buy-sell agreements and loan programs. Dkt. 419 at 42.

As a preliminary matter, there must be a valid contract for there to be a subsequent breach. A valid contract exists where there is "(1) the consent of the contracting parties, (2) a definite object which may be the subject of the contract, and (3) the cause for the obligation which may be

established." 31 L.P.R.A. § 3391. Contracting parties indicate their consent by mutual "offer and acceptance of the thing and the cause which are to constitute the contract." 31 L.P.R.A. § 3401. A contract exists from the moment one or more persons consent to bind himself or themselves, with regard to another or others, to give something or to render some service." 31 L.P.R.A. § 3371. The parties agree that the SCA and the NDA are valid, binding contracts.

The NDA affects Rodríguez, ASG, and GOS's relationship with TLS because Rodríguez controls both entities as the sole shareholder. *See* Joint Ex. V ¶ 1.1 (the NDA encompasses the parties and "any entity controlling, controlled by or under common control" of the parties). Likewise, the SCA affects Rodríguez and GOS because he is the "entity controlling" ASG, and GOS is "under common control with [ASG]." Joint Ex. II ¶ 51.

The confidentiality clause in the SCA states:

> 5. Confidentiality
>
> 5.1. Except as authorized in writing by TLS, neither Subcontractor nor any entity controlling, controlled by or under common control with Subcontractor (collectively, "Subcontractor Affiliates") will at any time directly or indirectly, disclose or utilize in any manner including for Subcontractor's own pecuniary gain, Confidential Information of TLS. Subcontractor may only use Confidential Information of TLS for a purpose that is necessary in carrying out the provisions of this Agreement.
>
> 5.2. "TLS Confidential Information" shall include, without limitation, all of the following, which shall be treated as Confidential Information of TLS by Subcontractor:
>
> 5.2.1. All information, whether written or otherwise and whether or not it is marked "confidential", "proprietary", or "copyright" at the time of disclosure, regarding TLS' business methods and procedures, clients or prospective clients ("TLS Clients"), agent lists, marketing channels and relationships, marketing methods, costs, prices, products, formulae, compositions, methods, systems, procedures, prospective and executed contracts and other business arrangements, proposals and project plans, and TLS Affiliates;
>
> 5.2.2. TLS reports and any information contained therein, related work products including implementation documents, and any other information provided to Client by TLS or TLS Affiliates by or in connection with proposing or delivering TLS Services (individually or collectively, "TLS Plans");

> 5.2.3. The identities of agents, contractors, consultants, sales representatives, sales associates, subsidiaries, strategic partners, licensors, licensees, TLS Clients, suppliers, or other TLS service providers or sources of supply (collectively, "TLS Affiliates");
>
> 5.3. TLS Confidential Information shall not include (a) information disclosed with the prior written consent of TLS, (b) information that has been previously disclosed by TLS to the general public, (c) information that is required to be disclosed pursuant to a valid judicial court order, but only to the extent of and for the purpose of such order, and only if after receiving such an order Subcontractor provides timely notice of such order to TLS and cooperates reasonably with TLS' efforts to contest or limit the scope of such order, or (d) any strategy or methodology contained in the TLS Plan that is currently being utilized by Subcontractor or any of Subcontractor's other clients as a result of Subcontractor's prior recommendations (the "Excluded Strategies").

Joint Ex. II ¶¶ 5.1–5.3.

The confidentiality clause clearly prohibits the use of TLS's methods and procedures, but it does not outlaw the use of every method or procedure resembling TLS's. Defendants argue that claiming a breach for similar buy-sell agreements and loan programs is an "outlandish interpretation." Dkt. 525 at 83. The clause is indeed broad, but, as the court has said, breadth does not automatically invalidate a confidentiality clause. Dkt. 383 at 16. Expansive definitions in contracts have been upheld. *Puerto Rico Tourism Co. v. Priceline.com, Inc.*, No. CV 14–01318 (JAF), 2015 WL 5098488, at *5 (D.P.R. Aug. 31, 2015) (court found a statute was unambiguous even though the definitions included lists of terms "without limitation"); *Cellu-Beep, Inc. v. Telecorp, Inc.*, 322 F. Supp. 2d 122, 124 (D.P.R. 2004) (arbitration clause including description of terms that were "without limitation" was "pretty explicit and its language plainly obvious").

To prove a breach of contract with regard to the buy-sell agreement and the loan program, TLS must prove that its own distinct buy-sell agreement and loan program were used in violation of the confidentiality clause. At trial, more evidence was devoted to the confidential information in general and items for which liability had been established, such as the loan agreement and operating agreement, than to the buy-sell agreement or to the loan program. Each of these are common business methods and procedures utilizing them unfold in many different contexts at many different companies.

ASG and GOS each used buy-sell agreements, which TLS employed in the event a client chose to exit TLS. The GOS buy-sell agreement template used, however, was not TLS's. Santo Domingo prepared the form on his own and customized it to GOS's needs. TLS did not show any relation between the TLS buy-sell agreement and the GOS or the ASG versions. The confidentiality agreement cannot be interpreted so broadly as to inhibit former employees and contractors from ever using methods or procedures that bear a resemblance to those TLS practiced.

This reasoning applies with even more force the loan program, which regulates the relationship between company and client. Had TLS been able to prove at trial that ASG or GOS borrowed the same underlying formulae or an identical structure, then extending the confidentiality clause to include this specific business method would be sensible. Without that specificity, protecting the common concept of a loan program which shares only features that, by definition, make it a loan program and none of the features that characterize it as a TLS-specific program, exceeds the reach of the confidentiality clause.

Accordingly, I find that TLS has not proven by a preponderance of the evidence that Defendants breached their agreements with respect to the buy-sell agreements and loan program.

IV. Remedies

TLS brought claims alleging Wiretap Act violations, Trade Secret Act violations, and breach of contract against Rodríguez, Ramos, ASG, and GOS. TLS did not carry its burden with regard to the Wiretap Act. TLS proved that Rodríguez and ASG violated Trade Secret Act. Prior to trial, the court found liability on the part of Rodríguez and ASG for breaching the confidentiality clauses by using TLS's loan agreement and operating agreement, for using and disclosing the Strategy to clients, and for keeping files after employment with TLS ended.

The Trade Secret Act provides for equitable and legal relief. In cases where a plaintiff proves that a trade secret has been misappropriated, "the court may issue a permanent injunction once the case has been fully heard." 10 L.P.R.A. § 4136. "The court may, under extraordinary circumstances, order that reasonable royalties be paid if it finds that prohibiting the future use of an industrial or trade secret would be an unreasonable measure." *Id.* TLS has requested permanent

injunctive relief against Rodríguez and ASG, ordering them to return all TLS trade secrets in their possession and enjoining them from using or disclosing those trade secrets in the future.

TLS further demands damages for the material harm sustained. TLS seeks $34,500,000, the market value of the Strategy, or, in the alternative, $4,858,000, the market value of the CPR. Dkt. 524 at 32. TLS argues that these sums measure statutory damages as well as royalties for four years of misappropriation of its trade secrets. The law states:

> Except in cases in which there has been a change in position or situation, before the defendant was aware or should have been aware of the concept of misappropriation concerning the information of the industrial or trade secret, and this renders a monetary settlement non-equitable, the plaintiff may recover any material damages sustained because of such misappropriation. The plaintiff may also claim any additional damages caused by any advantage obtained by the defendant as a result of such misappropriation which have not been included in the computation of losses caused by such damages. If unable to prove, to the satisfaction of the court, material damages or damages caused by improper advantage, the court may order the payment of royalties for a term that shall not be longer than the term for which the use of such information would have been prohibited.
>
> The court, in its discretion, may fix the sum total for damages in an amount that shall not exceed thrice (3) the proven damages when the court finds that the violation was intentional and perpetrated in bad faith.

10 L.P.R.A. § 4137.

TLS failed to present an expert qualified to testify to the valuation of TLS, the CPR, or the Strategy. Though Colombik offered his personal opinion as to the values, he did not provide a breakdown of the damages or analyze any specific harms TLS suffered as a result of the violation. As a result, I do not grant much weight to his testimony on this issue. Even if I did consider Colombik's valuation testimony, I find that the amounts TLS requests—$34,300,00 or $4,858,000—grossly exceed the any reasonable estimate of the material harm TLS sustained due to Defendants' limited use of TLS's trade secrets.

In the absence of that specific proof, the statute empowers the court to order the payment of royalties. *See* § 4137. A non-exhaustive list of the factors that the court should consider are: "[l]oss of profit for the owner of such information; value of the sum that would have been paid to

a consultant to develop such information; depreciation of such information's value as a result of disclosure; developing costs in the process of acquiring such information, or such information's market value." § 4137(a)–(e). The CPR and the Strategy's value have been unaffected due to the limited use and disclosure that Rodríguez's misappropriation entailed. Loss of profit, cost of development, and cost of acquisition through legal means are all difficult to estimate, and little to no proof was presented as to these facts. Here, the only solid figures of the value of what Defendants misappropriated is the $10,852.50 paid to ASG by Harris and Marlin.

"The court, in its discretion, may fix the sum total for damages in an amount that shall not exceed thrice (3) the proven damages when the court finds that the violation was intentional [and/or] perpetrated in bad faith." [2] § 4137. In this case, Rodríguez intentionally put his knowledge of the Strategy to use for clients leaving TLS for his own personal, pecuniary gain. Rodríguez did so despite two different confidentiality agreements prohibiting him and prohibiting ASG from such conduct. In light of the misappropriation of the CPR and the intentional disclosure and use of the Strategy, the court awards damages of $32,557.50 to TLS under the Trade Secret Act.

As relief for breach of contract, TLS again demands a permanent injunction against Rodríguez, ASG, and GOS ordering them to return to TLS all TLS documents in their possession

[2] TLS cites a discrepancy in the translation of § 4137 between the English and Spanish editions of the Laws of Puerto Rico Annotated. The English edition states that the court may treble damages when a "violation was intentional *and* perpetrated in bad faith." 10 L.P.R.A. § 4137 (emphasis added). The Spanish edition does not require both conditions: damages may be tripled when "la violación fue intencional *o* de mala fe." 10 L.P.R.A. § 4137 (emphasis added). It is the district court's duty to ensure that all pleadings in a federal court be conducted in English. *United States v. Rivera-Rosario*, 300 F.3d 1, 6 (1st Cir 2002); *see also Estades-Negroni v. Assocs. Corp. of N. Am.*, 359 F.3d 1, 2 (1st Cir. 2004); *United States v. Millán-Isaac*, 749 F.3d 57, 63 (1st Cir. 2014). District court judges "must not consider any untranslated documents placed before them." *Millán-Isaac*, 749 F.3d at 64. This policy clarifies evidentiary and legal matters for the appellate court, and it facilitates the integration of all district courts within the federal system. Notwithstanding, First Circuit case law on the subject remains primarily focused on opinions and evidence provided in Spanish without a certified translation. It does not address the issue faced by counsel when the official English translation is incorrect. When there is a discrepancy between the English and the Spanish edition of a statute, Puerto Rican law instructs that the statute's language of origin prevails. 31 L.P.R.A. § 13. "If the statute is of Spanish origin, the Spanish text shall be preferred to the English." *Id.*; *accord Farthing v. Coco Beach Resort Mgmt.*, 2017 U.S. Dist. LEXIS 217887, at *8 n.1 ("Insofar as the English translation is incorrect, the Court uses its own translation of the statute.") (Velez-Rive, J.). Because this is a state law claim, the court follows the proper translation of "or" rather than "and."

and permanently enjoining them from using or disclosing TLS confidential information as defined in the SCA and NDA (Joint Exhibits II and V, ¶¶ 5 and 1, respectively). TLS also demands $27,131.25 as damages for ASG and Rodríguez's breach of the SCA. Finally, TLS demands reasonable costs and attorneys' fees under the SCA and NDA.

Like the SCA, the NDA includes an equitable remedies section in which the parties agree that "irreparable damage without an adequate remedy at law may result from a breach of this Agreement . . . . Each Party agrees to pay all legal fees and costs of the other Party if a preliminary or permanent injunction is ordered due to the actions or inactions of the other Party." Joint Ex. V ¶ 2.1.Exs. II and V, ¶¶ 9.2.1 and 2.1. The court found irreparable harm and granted a preliminary injunction to TLS. Dkt. 212. The court now grants a permanent injunction against Rodríguez, ASG, and GOS. Each party must return to TLS all TLS documents in their possession and may not use or disclose TLS confidential information.

The SCA also entitles TLS to "150% of all fees collected by Subcontractor for such unauthorized use of TLS Confidential Information." Joint Ex. V ¶ 9.2.2. Marlin and Harris collectively paid ASG $10,852.50 for consulting services which involved the use and disclosure of confidential information. The court will enforce the contract terms related to obtaining injunctive relief, as allowed under the SCA and NDA, but refrains from awarding TLS 150% of the fees collected as allowed under the SCA because this would be duplicative of the damages awarded under the Trade Secret Act. "A plaintiff is not entitled to duplicative damages; it may recover only the amount of damages it actually suffered." *Garshman Co. v. G.E.*, 176 F.3d 1, 5 (1st Cir. 1999). Legal remedies are intended to make a plaintiff whole but not "more than whole." *Sindi v. El-Moslimany*, 896 F.3d 1, 26 (1st Cir. 2018). TLS seeks relief for essentially the same conduct: use and disclosure of the Strategy and its underlying forms in violation of the SCA and NDA. To award TLS damages for the same conduct under two different statutory schemes would permit TLS to double dip. *See Bogan v. City of Boston*, 489 F.3d 417, 425 (1st Cir. 2007) (internal quotations omitted) ("The law abhors duplicative recoveries; thus double awards for the same injury are impermissible."); *accord Dopp v. HTP Corp.*, 947 F.2d 506, 517 (1st Cir. 1991) (rev'd

in part on other grounds) (remedies may become redundant where the same conduct gives rise to multiple causes of action).

TLS's request for costs and attorneys' fees may be made through a post-judgment motion in accordance with Local Rule 54(a). TLS should be prepared to provide its invoices and evidence that its attorneys' rates are consistent with industry standards.

PERMANENT INJUNCTION ORDER

Ricky Rodríguez-Toledo, ASG Accounting Solutions Group, Inc., Global Outsourcing Services LLC, and their officers, servants, employees, attorneys, successors and assigns, and any person acting in concert or participation with them, are hereby enjoined from using or disclosing any of TLS's "confidential information" or its trade secrets in violation of, and as defined by, the SCA and NDA. Joint Ex. II ¶¶ 5.2–5.2.3; Joint Ex. V ¶¶ 1.2.–1.2.4. "Confidential information" includes TLS's business methods, systems, and procedures; clients; agent lists; marketing channels and relationships; marketing methods; costs; prices; products; formulae; prospective and executed contracts; business arrangements; proposals; project plans; reports; implementation documents; and clients' personal and financial information. "Confidential information" also includes the identities of TLS's agents, contractors, consultants, sales representatives, sales associates, subsidiaries, strategic partners, licensors, and licensees. Trade secrets include the Capital Preservation Report and the U.S. Possession Strategy. Defendants must locate and return to TLS all documents in their possession, if any, that contain TLS's confidential information or trade secrets. Defendants must also ensure that their businesses, including the webpages for those businesses, are not employing TLS's confidential information or trade secrets.

IT IS SO ORDERED.

In San Juan, Puerto Rico, this 28th day of September, 2018.

S/Bruce J. McGiverin
BRUCE J. MCGIVERIN
United States Magistrate Judge