SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF NEW YORK

TILLAGE COMMODITIES FUND, L.P., Plaintiff,	Index No. 654765/2016
- against -	**COMPLAINT**
SS&C TECHNOLOGIES, INC., Defendant.	

Plaintiff Tillage Commodities Fund, L.P. ("Tillage" or "the Fund"), by and through its attorneys, Arkin Solbakken LLP, as and for its Complaint against Defendant SS&C Technologies, Inc. ("SS&C"), alleges as follows:

NATURE OF THE ACTION

1. This action arises out of a fraudulent email scheme to which SS&C was a party, revealing its egregious lack of diligence and care, bad-faith breaches of contract, gross negligence and willful misconduct in the performance of its contractual obligations, and entirely false and misleading representations of fact to its customers, the investing public, and regulators.

2. The fraud described in this complaint resulted in the cessation of the Tillage Commodities Fund, dramatic losses for its investors, and the elimination of a heretofore successful business with meaningful growth potential.

3. SS&C is a publicly listed fund administration company with global clients and transfer authority and control over billions in client funds.

4. The primary function of fund administration – an industry which has seen rapid

growth and widespread adoption in response to the large and financially destabilizing actions of fraudulent fund managers like Bernard Madoff – is to protect investors and the monies which the fund administrator is entrusted to process and oversee.

5. Of course, SS&C recognizes that the security of client funds is absolutely paramount to its business and the services it sells.

6. Accordingly, SS&C makes numerous public representations – via its website, white papers, financial reports, Securities Act filings, shareholder materials, and other publications; in communications with customers; and in the media – about its (purportedly) unrivaled and state-of-the-art cybersecurity practices, its supposed compliance with government guidelines and mandates, and its allegedly rigorous internal controls.

7. As shown below, however, SS&C is anything but the model "safe" administrator of investor accounts. Its myriad claims to the contrary are entirely false and illusory.

8. In fact, SS&C fails to exercise even a modicum of care and responsibility in connection with known and obvious cybersecurity threats.

9. Its personnel further fail to follow even the most basic of SS&C's own protocols and procedures, much less conform to SS&C's prescribed contractual authority.

10. As a result of its reckless indifference and purposeful bad faith, SS&C actually facilitated an amateurish fraudulent wire request scheme and disbursed almost $6 million in cash from Tillage's account – a theft that fell squarely with the purview of those SS&C claims to prevent.

11. SS&C wholly failed to live up to financial services industry standards and was grossly negligent in performing its services.

12. SS&C further acted in rank bad faith by misleading the authorities seeking to

recover Tillage's funds and by refusing to provide Tillage with material to which it is contractually entitled.

13. Tillage brings this action to hold SS&C liable for this misconduct, its gross negligence, willful misconduct, and bad faith in the performance of its contractual obligations to Tillage, and to further hold SS&C accountable for its plainly false and misleading statements to the marketplace.

PARTIES/NON-PARTIES

14. Plaintiff Tillage Commodities Fund, LP is a Delaware limited liability partnership incorporated in Delaware. Thomas Funk – a New York resident – is the founder and Managing Member of the Investment Manager of Tillage.

15. Defendant SS&C Technologies, Inc. is a Delaware corporation, with offices at 675 Third Avenue, New York, New York.

JURISDICTION AND VENUE

16. This Court has jurisdiction over the Defendant pursuant to, *inter alia*, New York CPLR §§ 301 & 302.

17. Venue in the county of New York is proper pursuant to, *inter alia*, the parties' contract and New York CPLR § 503.

FACTS RELEVANT TO ALL ALLEGATIONS

I. TILLAGE COMMODITIES FUND LP

18. Tillage is an investment fund started in March of 2012 that uses a systematic, model-based strategy to invest in a diversified portfolio of exchange-listed commodities futures contracts. The Fund, in the entirety of its four-year existence, has had only one active investment account at its prime broker (J.P. Morgan and then ADM Investor Services, both based in New York). Tillage's sole investing activity has been to trade commodity futures

within that account.

19. Prior to the events giving rise to this Complaint, Tillage held approximately $9.26 million in assets under management. Tillage had produced investor returns of 14% in 2014 and 7% in 2015 and, due to these results, had been experiencing increased investor interest, including several prominent institutional investors.

20. Like the vast majority of other funds operating in the wake of the financial crisis of 2008 and the subsequently exposed Madoff fraud, Tillage sought to retain an independent third-party administrator to protect the interests of its investors.

21. To this end, it contracted with SS&C, an entity that states in its corporate summary: "We have created the most comprehensive powerhouse of software technology in the financial services industry – technology that complements our unrivaled expertise and professionalism in fund administration, insurance and pension funds, and asset and wealth management accounting and operations."

22. SS&C further represents: "We will always own and maintain the best technology in the industry." *See* SS&C Website, *available at* http://www.ssctech.com/AboutUs.aspx.

23. Indeed, during all time periods relevant to this Complaint, SS&C represented, in substance, that "[a]t SS&C, we . . . ensure and maintain the right security for your business." *See* https://ssctechblog.wordpress.com/2015/06/10/cybersecurity-series-take-note-on-reinvesting/.

II. <u>THE PARTIES' CONTRACT</u>

24. In October 2011, SS&C presented to Tillage a Fund Services Proposal stating that, by its services, "SS&C assumes the operations, staffing, and systems risk from the fund."

25. Not long thereafter, the parties entered into a contract for SS&C's services.

26. Pursuant to the parties' agreement, SS&C has authority to disburse Tillage funds

to: (1) process and disburse investor redemptions (or withdrawals); (2) pay authorized fund expenses; and (3) accept or move subscription funds to a prime broker.

27. To ensure that SS&C could adequately perform these and other functions, it requested and received Tillage's partnership and offering documents so that it was familiar with both Tillage's business model and investment strategy.

28. SS&C further wrote to Tillage that it would devise particular operational and procedural mandates "to ensure that all fund activities are subject to appropriate authorization and oversight, and are in compliance with [SS&C's] internal and regulatory guidelines."

III. SS&C'S SECURITY PROTOCOLS

29. Among SS&C's internal guidelines are those directed at preventing the transfer of funds sought by fraudulent wire transfer requests. In fact, SS&C has long acknowledged that: "According to the FBI, cyber-enabled wire transfer is one of the most common internet scams." SS&C eBrief, *available at* http://www.ssctech.com/eBriefings/eBriefingArticle/tabid/597/Default.aspx?V=6&A=4521.

30. In response to this type of risk, SS&C assures consumers that it "**always use[s] the most up-to-date best practices when transferring and moving funds**, working with third party suppliers, and fighting the ever-evolving threat of cybercrime." *Id.* (emphasis added).

31. This includes, among other things, using a filtering tool on all incoming email communications. *See, e.g.*, SS&C eBrief, *available at* http://www.ssctech.com/ebriefing.aspx?E=3602. As SS&C states, "[i]t is vital that users have a well-disciplined URL filtering tool" for incoming email.

32. SS&C further purportedly uses information protection programs that assure "[a]ccess is restricted and is controlled by identification, authentication, and authorization control processes that are based on least privilege, need-to-do, need-to-know purposes." SS&C

eBrief, *available at*

http://www.ssctech.com/eBriefings/eBriefingArticle/tabid/597/Default.aspx?V=7&A=4333.

33. SS&C purports to be aware of how unauthorized communications may present, advising that fraudulent incoming emails "may appear to come from someone in your address book" and "may include graphics that make them look legitimate." *See* SS&C eBreifing article, *available at*

http://www.ssctech.com/eBriefings/eBriefingArticle/tabid/597/Default.aspx?V=5&A=4571.

34. To foreclose fraud of this nature, SS&C notes: "You need to match the paperwork to the individual, and that takes independent verification and investigation." *See* SS&C eBreifing article, *available at*

http://www.ssctech.com/eBriefings/eBriefingArticle/tabid/597/Default.aspx?V=10&A=252.

35. For these reasons, SS&C employees are directed to consider the behavior of its clients and to check all mail recipients in every field of a wire transfer request in order to detect irregularities.

36. For example, SS&C's internal training material mandates that employees: "[c]arefully check all mail recipients marked in To, Cc, and Bcc Fields."

37. SS&C employees are further directed to respond to wire transfer requests by and through the use of a "Send Secure button," which will delineate the appropriate email address for its client (thereby foreclosing communications with spoofed domains or email addresses).

38. SS&C also required that Tillage verify disbursements by either (i) appending an invoice to support the expense; or (ii) in the case of a redemption, providing redemption letters and instructions from fund investors.

39. For example, SS&C wrote to Tillage on April 18, 2012 and directed that every

payment request from Tillage append such back up documentation. According to SS&C, this would allow it to "**review the payment requests to insure we know/understand what the payment is for** and account for it correctly." (Emphasis added.)

40. Finally, SS&C's purportedly follows a detailed formal wire request approval procedure, which details the role for an SS&C associate, an accounting contact, a Department Manager, and a Department Director (with final release authority), with each fulfilling his or her role as part and parcel to a sequential approval process.

41. This procedure requires that wire transfer requests be processed only when submitted by authorized individuals, and only after SS&C had *validated and authenticated* the request:

> Each wire transfer request must be submitted via fax or email by **individuals duly authorized to instruct the movement of money on behalf of the Fund**. . . . The SS&C Associate **validates the instruction for completeness, authenticates the authorization**, confirms the availability of funds, obtains acknowledgement of the request from the SS&C Accounting contact and **informs the Fund Manager that the request has been received**.

See SS&C Investor Relations – Policies and Procedures Manual, at 13 (emphasis added).

IV. SS&C ACTIVELY FACILITATES A MULTI-MILLION DOLLAR FRAUD, NOTWITHSTANDING ITS PURPORTED SECURITY PROTOCOLS AND CONTRARY TO ITS CONTRACTUAL OBLIGATIONS

42. Notwithstanding these and other purported security protocols – and contrary to its contractual obligations – beginning on March 3, 2016, SS&C repeatedly facilitated a fraudulent wire transfer scheme targeting Tillage's bank account at First Republic Bank (over which, per its agreement with Tillage and First Republic Bank, SS&C had sole signing and transfer control).

43. This scheme involved a series of amateurish and fraudulent emails from a third party, using "spoof" domains that were plainly misspelled variants of Tillage's email domain

name, each of which sought wire transfers in increasingly large amounts, to be directed to the Hong Kong bank account of a vaguely identified technology company.

44. SS&C took virtually no steps to "validate" these wire transfer requests or "authenticate" the sender's authorization. Further – and despite its purported use of "cutting edge" technology – SS&C failed to employ any basic email filtering tools that would have blocked, segregated, or marked these emails.

45. To the contrary, SS&C (by and through its employees, including Investor Services Associate Tom Martocci, who served as the main point of contact with Tillage, as well as many others in SS&C's approval chain) repeatedly ignored *facially obvious signs of inauthenticity* in each wire request.

46. *First*, and even leaving aside the fact that ordinary filtering software (as SS&C claims to employ) should have deflected this correspondence, even a cursory examination of the "From" field manifest by the emails at issue would have revealed the fraudulent nature of the request.

47. Specifically, the domain name used by Tillage over the course of its four year services agreement with SS&C is "@tillagecapital.com," while the fraudulent emails used a domain name with one additional "*l*" (*i.e*., "@tilllagecapital.com"). The careful checking of email domain name as detailed in SS&C's internal training manual is a clear requirement of its employees – a requirement with which they did not comply.

48. *Second*, the fraudulent requests included awkward syntax and grammatical errors – which were wholly inconsistent with prior Tillage communications – and which were entirely unclear in substance.

49. For example, the first of this series of emails directed to Mr. Martocci – who was

long familiar with the Tillage Fund and its business – stated as follows:

> **Can you please process the attached International Business Establishment. We are funding HAORAN TECHNOLOGY LIMITED.**
>
> **Please leave me a mail to confirm this and that the wire will go out today.**

50. The instruction to "process [an] International Business Establishment" – is both incomprehensible on its face and *bears no relationship whatsoever* to Tillage's futures-trading business model or investment strategy.

51. Three of the six fraudulent requests make reference to wiring money to generic "investors" which imply a fund redemption is being requested. Yet processing these requests is incomprehensible given that: (1) the stated recipients of the funds were not investors in the Fund; and (2) no redemption letters were provided even though they are expressly required by SS&C.

52. Still other emails fail to make any reference whatsoever to even a potentially legitimate business objective. For example, the email requesting the largest wire transfer during the lifetime of this scheme ($3 million) states nothing more to Mr. Martocci than: "How was your weekend? Let's round business up today."

53. Again, Mr. Martocci and others on the Tillage account team are acutely aware of Tillage's business practices. Had they actually been doing anything to validate and authenticate the wire request at issue, they would have immediately recognized that the communications at issue were not prepared by their client.

54. Indeed, the fact that the fraudster was aware of the fact that a withdrawal of $3 million would "round business up" (by almost entirely looting the monies then existing in Tillage's account) suggests Mr. Martocci worked with the fraudster to "round up" a "business"

directed at leaving Tillage with nothing.

55. This is further evidenced by the fact that Martocci soon thereafter approved the fraudster's next and last request – for $700,000 that still remained in Tillage's account. Had this Martocci-approved wire for $700,000 gone through, Tillage's bank account would have been almost entirely drained.

56. *Third*, the body and substance of the fraudulent wire requests differed from those historically issued by Tillage.

57. Tillage has made a total of over 210 requests to SS&C for wire transfers covering expenses over its four year life. The average of these wires had been for $3,567 and the largest had been for $12,410. The only other wire transfers that occurred outside of investor subscriptions and redemptions was for the heavily documented transfers of the Fund's bank account from J.P. Morgan to First Republic and the switch the Fund made from its prime broker being J.P. Morgan to ADM Investor Services.

58. Here, however, the fraudulent wire requests sought substantial six and seven figure amounts (with one totaling $3 million, or 3/4 of the total account at that point in time) without reference to an actual Tillage shareholder (were it being viewed as an investor redemption) and in the absence of any supporting documentation whatsoever (were it being deemed an expense).

59. Additionally, Tillage's standard practice was to provide documentary support for any disbursements sought, uniformly concluding each wire request with a sentence providing that: "Should [SS&C] require anything further, please call [Tillage] at XXX-XXX-XXXX."

60. But, both of these hallmarks were absent from the fraudulent wire requests, which concluded only with the statement: "Should you require anything further, please do not

hesitate to send me *a mail*" (emphasis added).

61. Further, unlike other Tillage communications, the fraudulent wire requests did not comply with SS&C's written instruction to Tillage that such requests must copy the so-called "OMR-Tillage" group – a collection of SS&C employees in continual contact with the Fund and charged with reviewing and managing Tillage's account and wire requests.

62. *Fourth*, the fraudulent wire requests sought to transfer funds to two technology companies with bank accounts in Hong Kong – foreign entities with which Tillage had no relationship whatsoever, and about which SS&C had received no further explanatory documentation. SS&C knew or should have known such a request was suspect, given that Tillage's sole investing activity since inception has been trading futures through its sole prime broker. It has not once made any other investment; nor has it ever wired funds outside of the United States.

63. *Fifth,* throughout the twenty-one day course of the fraudulent scheme, SS&C indisputably failed to deploy the internal controls it otherwise represents it employs.

64. For example, SS&C's formal wire approval process as described above requires four employees to sign off before the release of the wire. Yet, records indicate that the fraudulent wire request for $1.5 million processed by SS&C on March 16, 2016, was released at 1:18 EST – a time ***before*** the time stamp showing the approval of the last two of the requisite four SS&C employees.

65. In all events, as discussed above, SS&C can disburse funds to: (1) process and disburse investor redemptions (or withdrawals); (2) pay authorized fund expenses; and (3) accept or move subscription funds to a prime broker.

66. SS&C's disbursement of funds in response to fraudulent wire requests seeking

these monies for other purposes (such as to "process [an] International Business Establishment") exceeded the scope of its contractual authority.

67. In fact, Mr. Martocci, who had worked on the Tillage account since August 2014, was very aware of Tillage's business practices, and had received approximately sixty authentic wire requests from Tillage in the past.

68. It defies belief that Mr. Martocci could have read these amateurish and fraudulent emails – which sought, in rapid succession, wires in ascending amounts, to be directed to Hong Kong banks, which bore no resemblance in form or substance to any prior Tillage communications and which made no sense in light of its known business model of solely trading futures – and believed they were prepared by his client.

69. Even more disturbing is that email evidence provided to Tillage shows that SS&C employees were not just following clearly fraudulent instructions but that they were actually **responding** and engaging in a two way dialogue with the criminal all the while never communicating with their true client as the account was drained.

70. Either SS&C processed this series of fraudulent wire transfer requests without *any review whatsoever*, in total abdication of its obligations – or SS&C knowingly facilitated the fraud.

71. In the end, SS&C processed a total of six fraudulent wire requests received over a twenty-one day period, resulting in a total loss of $5.9 million – each without Tillage's knowledge, consent, or approval.

72. Only after Mr. Martocci's approval of a seventh wire request (which would have wiped Tillage out entirely) did SS&C contact Tillage's Thomas Funk by phone in an effort to discuss the subject activity.

73. In processing these fraudulent wire transactions and facilitating the theft of Tillage's funds, SS&C not only failed to detect the foregoing obvious signs of fraud – it also failed to comply with its own internal controls for a wire transfer.

74. SS&C did not examine the To/From/CC fields in the requests of any of these seven emails, which would have revealed both the plainly false domain names and the fact that the proper parties were not copied on them.

75. Nor did SS&C acknowledge receipt of the wires by use of a "Send Secure button" (as required by its Internal Training Manuals), which would have immediately routed SS&Cs response to Tillage's proper email domain – thus alerting Tillage of the fraud. Instead, SS&C simply "replied to" the fraudulent requestor.

76. SS&C did not require any supporting documentation to support the disbursements, and SS&C most certainly did not adhere to the internal review and approval standards it claims are required.

77. Instead, on seven separate occasions, Mr. Martocci directed the release of Tillage's funds oftentimes merely minutes after receiving the fraudulent wire requests.

78. Had SS&C at any point complied with its own internal mandates directed at authenticating and verifying disbursement efforts, no theft would have been possible.

V. <u>SS&C FACILITATES THE FRAUD FURTHER</u>

79. As if these failures were not enough, SS&C actively and inexplicably assisted the perpetrator of this fraudulent scheme, by helping the perpetrator correct and clarify his or her initially flawed wire instructions.

80. In particular, the first fraudulent email of March 3, 2016 had directed that funds be wired directly to a company called "Haoran Technologies" and its account at Hangseng Bank in Hong Kong. Tom Martocci worked with other SS&C employees to amend and help correct

the transaction, adding HSBC Hong Kong as the correspondent bank, and moving Hangseng Bank to be named the beneficiary bank.

81. When these amendments to the first wire request still did not resolve the matter and the wire was rejected, SS&C employees communicated this to the fraudster giving the fraudster the opportunity to again modify future instructions and name a different recipient company for the wires, the aptly named Away Technologies, which had an account directly at HSBC Bank.

82. This was the process employed for the next five subsequent, successful wires, until $5.9 million had been stolen from Tillage.

83. This two-way communication between the spoofer and SS&C continued throughout the course of the month as additional requests were made.

84. SS&C did not inform Tillage of any of these events. Nor did the initial bank rejection give SS&C any pause as to the authenticity of the subject communications.

85. This is despite the fact that at no point during the parties' four-year relationship had Tillage ever once requested that SS&C direct investment funds to any entities other than its one active prime broker.

86. SS&C also neglected to tell the Hong Kong police about its cooperative actions with the fraudster and how the wire recipients were changed through this communication.

87. But for SS&C's "help," the fraudster's effort to steal from SS&C's client would have been thwarted.

VI. TO CONCEAL ITS OWN WRONGDOING, SS&C OBSTRUCTS THE INVESTIGATION AND RECOVERY OF TILLAGE'S FUNDS

88. Tillage has also learned, through the limited set of emails provided to it by SS&C, that SS&C first began to investigate the fraud at issue no later than March 22, 2016.

89. This was just one day after SS&C had disbursed another $3 million to the fraudster – and still within the 24-hour period when the FBI informed Tillage that they are able to recover stolen funds.

90. Inexplicably, however, SS&C waited an additional two days – until March 24, 2016 – to communicate with Tillage about these six transactions totaling $5.9MM.

91. Upon receipt of this notification, Tillage immediately directed its efforts to recovering the stolen funds – all the while being falsely assured by SS&C that SS&C would assist in these recovery efforts.

92. SS&C purported to take the fraud on Tillage seriously, advising Tillage that SS&C was addressing the matter with its Chief Executive Officer, William C. Stone.

93. In fact, however, SS&C proceeded to make numerous false and misleading statements to multiple governmental authorities, intentionally providing misleading and incomplete information – all in an effort to deflect from its own culpability.

94. For example, on March 24, 2016, SS&C submitted a report to the Hong Kong Police Force that falsely stated, among other things, that:

> On each of March 3, 8, 9, 14, 16, 21 and 24 SS&C Technologies, Inc. received emails from known contacts at [Tillage Commodities Funds (LP (the "Client")] to wire monies from the Client's bank account. Signed letters of authorization were provided with valid signatures on our standard form.

95. Yet, at the time this report was made SS&C indisputably knew the wire transfer requests at issue were not, in fact, "from known contacts at" Tillage.

96. Instead, as SS&C was well aware, these emails were directed to it from a "spoof" domain used by individuals who falsely claimed to be Tillage principals.

97. Nor did any one of the subject wire requests reflect "valid signatures" that were presented via SS&C's "standard form."

98. Instead, the signatures used by the fraudster were copies that were, on information and belief, obtained from SS&C's own unsecure system, and were submitted on "forms" not used by Tillage or SS&C at any point during the course of the parties' four year relationship.

99. Additionally, in the report sent to Hong Kong police, SS&C neglected to disclose that it assisted the spoofer in the change of instructions from one bank to the other and instead wrote that "The proceeds of the March 3rd wire were returned to us for unrelated reasons." This was entirely misleading and done for the purpose of withholding the extent of SS&C's aid and assistance with the fraud.

100. Similarly, when Tillage's regulator, the National Futures Association, contacted SS&C in connection with the events at issue, SS&C suggested to the regulator that a former employee of Tillage may be at fault for the fraud.

101. But SS&C knew at this time that there was no legitimate basis for this claim – in fact, Tillage had provided SS&C with evidence that this accusation was false.

102. Nonetheless, SS&C continued to repeat these accusations (with full knowledge of their falsity) to Tillage's regulator in an effort to distract from its own misconduct and culpability.

103. Finally, to this day, SS&C refuses to provide Tillage with all of its communications with the fraudster, in yet another blatant breach of its contractual obligations to its client.

104. As a result of its reckless misconduct, gross negligence, and bad faith, SS&C frustrated (if not entirely foreclosed) recovery of any portion of the amounts stolen from Tillage.

VII. SS&C'S FALSE STATEMENTS TO CONSUMERS, THE INVESTING PUBLIC, AND REGULATORS

105. SS&C's intentional misconduct and gross negligence is matter of grave concern not only for Tillage, but for the public at large.

106. By SS&C's own admission, it services "some 10,000 financial services organizations, from the world's largest institutions to local firms, . . . [who] manage an aggregate of over $44 trillion in assets."

107. SS&C's fund customer base is repeatedly assured by SS&C, both through its proposals and public advertising, that it employs the "most up-to-date practices when transferring and moving funds."

108. This is untrue. SS&C fails to employ even the most rudimentary of verification, review, use of filtering software, or other protections and does not even adhere to its own mandated approval process.

109. Similarly, SS&C ignores entirely the authentication or verification procedures that are both (i) recommended by government cybersecurity initiatives and (ii) set forth by its own guidelines.

110. SS&C has represented that:

> To respond to growing worldwide cyber security concerns, we continue to use our full time dedicated security team to review and implement security controls to align with changing U.S. government cyber security initiatives and guidelines, as well as respond to threats that we internally identify. We also continue to engage outside security experts to independently test our technology environment on an ongoing and regular basis.

See 2014 SS&C Annual Report.

111. But again, these representations are untrue. In fact, no security team deployed by SS&C has implemented security controls aligned with U.S. government initiatives and guidelines.

112. Indeed, the FBI and the Department of Justice have repeatedly recognized and warned against *precisely the type of fraudulent email scheme* that SS&C allowed to deplete Tillage's account. *See, e.g.*, *Business Email Compromise,* https://www.fbi.gov/news/stories/business-e-mail-compromise and https://www.ic3.gov/media/2015/150122.aspx.

113. To prevent against this form of fraud, the FBI recommends basic cybersecurity safeguards such as :

- "verifying changes in vendor payment location and confirm requests to transfer funds"
- "**creating detection systems that flag e-mails with extensions that are similar to company e-mail but not exactly the same"**
- "knowing the habits of your customers, including the reason, detail, and amount of payments. Beware of any significant changes."

See https://www.fbi.gov/news/stories/business-e-mail-compromise (emphasis added).

114. The FBI further warns: "Do no use the 'Reply To' option to respond to any business emails. Use the 'Forward' option and either type in address or get it from address book." *See* https://www.ic3.gov/media/2015/150122.aspx.

115. Yet SS&C did not utilize any one of these or other security controls that align with U.S. government cybersecurity initiatives and guidelines.

116. Had these been implemented by SS&C, Tillage would not have become the victim of this amateurish but costly fraud.

117. SS&C's claims to the marketplace are false, and are designed to mislead SS&C clients and potential clients.

118. SS&C also uses these misrepresentations to avoid regulatory scrutiny, which would require resource intense compliance.

119. Indeed, SS&C applied for exemption from regulation by the SEC based on its (false) representations of the highest levels of security from cybercrimes.

120. Among other things, by letter to the U.S. Securities and Exchange Commission dated July 20, 2015, in SS&C's Notice of Filing of Application for exemption from registration as a clearing agency, SS&C claimed that "SS&C has never experienced a breach of security or privacy." *Id.*, https://www.sec.gov/comments/600-34/60034-2.pdf.

121. On information and belief, this statement was knowingly false when made, and is indisputably false today.

CAUSES OF ACTION

FIRST CAUSE OF ACTION
(Breach of Contract)

122. Plaintiff repeats and re-alleges the allegations set forth in the preceding and following paragraphs as if the same were fully set forth herein.

123. Plaintiff and Defendant entered into a contract governing the terms of SS&C's engagement and its obligations as fund administrator. These obligations are set forth in the "Agreement to Provide Administration Services" as supplemented by the Investor Relations – Policies and Procedures, Wire Transfer Request Procedure and other documents and instructions authored by SS&C regarding its services to Plaintiff (the "Agreement").

124. Plaintiff performed all its duties and obligations under the Agreement.

125. Nonetheless, Defendant breached the Agreement with gross negligence, willful misconduct, and in bad faith as set forth herein.

126. In particular, SS&C repeatedly breached the Agreement by disbursing funds without Plaintiff's instruction or approval, in response to wire transfer requests made by unknown third-parties who were not authorized to request or approve such transfers.

127. Indeed, the Agreement expressly provides that redemptions/withdrawals will be made only "upon approval from [Tillage]," that SS&C is contracted to "Operate bank account as instructed by Management," and that SS&C itself does "not have the ability to authorize transactions."

128. These repeated and unauthorized disbursements also exceeded SS&C's authority under the Agreement, as the wire transfer requests identified purported business purposes that fall outside the scope of services for which SS&C was contracted and which bear no relationship whatsoever to Tillage's investment strategy.

129. In some instances, the fraudulent wire transfer requests ordered the transfer of funds to purported Tillage "investors." By disbursing funds in response to these requests, SS&C violated its contractual obligation to engage in "consultation with [Tillage]" before processing the transaction, and to "confirm that all required documentation has been provided."

130. These improper disbursements were also contrary to the written mandates and directives that SS&C provided to Tillage during the course of their relationship, requiring that wire transfer requests adhere to specific protocols purportedly designed to guard against unauthorized disbursements.

131. Finally, after belatedly notifying Plaintiff of these unauthorized disbursements (made without any request or approval by the Tillage), SS&C further refused to provide Plaintiff access to all of its communications with the defrauding third party. This ongoing refusal violates SS&C's contractual obligation to provide Plaintiff and its employees with access to materials necessary to document the transactions recorded by SS&C purportedly on Tillage's behalf.

132. As a result of Defendant's breach of contract, Plaintiff is entitled to damages in

an amount to be proven at trial, but no less than $10 million.

SECOND CAUSE OF ACTION
(Breach of the Implied Covenant of Good Faith and Fair Dealing)

133. Plaintiff repeats and re-alleges the allegations set forth in the preceding and following paragraphs as if the same were fully set forth herein.

134. Defendant breached the implied covenant of good faith and fair dealing of the Agreement, which – other than certain void limitations of liability – is a valid and enforceable contract against Defendant.

135. The Agreement included implied promises on the part of Defendant not to (among other things) disburse funds at the request of third-parties in connection with unauthorized business activities; delay notifying Plaintiff promptly upon suspicion of fraudulent activity; mislead government authorities or regulators as to the details of the fraud; or otherwise engage in activities obstructing Plaintiff's ability to recover such funds.

136. The Agreement also included implied promises on the part of Defendant to (among other things) follow basic, widely known, and common-sense cybersecurity procedures in processing wire transfer requests; to adhere (as represented) to the cybersecurity recommendations set forth by the U.S. government; to satisfy its own stated policies and practices regarding the authentication of wire transfer requests; to ensure that Plaintiff had notice not just of any significant disbursements but also of any suspected irregularities; and to provide Plaintiff the information necessary to seek to recover any funds lost due to Defendant's misconduct, failures, or contractual violations.

137. Plaintiff would not have entered into the Agreements but for these implied promises.

138. Defendant breached each of these implied promises as set forth herein. Among

other things, Defendant

- facilitated the theft of $5.9 million by disregarding basic cybersecurity protocols and procedures;

- declined to notify Plaintiff of the theft until at least two days after it identified the possible fraud;

- submitted a false report to the Hong Kong Police in an effort to evade responsibility for its failure – claiming, incorrectly, that the fraudulent transfer requests came from within Tillage and included "signed letters of authorization" with "valid signatures on our standard form," and neglecting to disclose that it assisted the spoofer in the change of instructions from one bank to the other – and thus obstructed law enforcement's efforts to investigate the theft;

- falsely and repeatedly suggested (to regulators and others) that Plaintiff's former employee might be responsible for the fraud, with full knowledge of the falsity of this statement;

- refused to provide Plaintiff with all of Defendant's communications with the fraudster; and

- otherwise attempted to insulate itself from liability at the expense of Plaintiff.

139. As a result of Defendant's breach of the implied covenant of good faith and fair dealing, Plaintiff is entitled to damages in an amount to be proven at trial, but no less than $10 million.

THIRD CAUSE OF ACTION
(Violations of GBL § 349)

140. Plaintiff repeats and re-alleges each and every allegation set forth in the preceding and following paragraphs as if the same were fully set forth herein.

141. Plaintiff has been injured and suffered damages by Defendant's violations of New York General Business Law ("GBL") § 349(a), which states: "Deceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful."

142. Defendant has in the State of New York engaged in consumer-oriented acts and

practices, insofar as the representations it makes regarding its purported superior and state of the art cybersecurity protocols are directed at the public at large and are designed to and do influence the consumers it targets. SS&C further directs to consumers purported internal mandates and other documentation that would suggest diligence in redressing risks associated with cybersecurity. These materials are likely to mislead a reasonable consumer acting reasonably under the circumstances.

143. Defendant's deceptive acts and practices include false and materially misleading statements about its (purportedly) unrivaled and state-of-the-art cybersecurity practices, its supposed compliance with government guidelines and mandates, and its allegedly rigorous internal controls.

144. Defendant's deceptive acts and practices have a broad impact on the public at large, as they are disseminated to the public via state-wide advertising and promotions, and other public statements aimed at consumers throughout the State of New York.

145. Given the outsized role played by SS&C in handling customer funds and the potential for large dollar losses, this deception is particularly dangerous and worthy of the State's prompt attention.

146. Defendant's violations of GBL § 349 caused damages to Plaintiff.

147. Had SS&C been truthful and not deceptive about its practices prior to the occurrence of the fraud detailed herein, Tillage's loss would not have occurred.

148. Pursuant to GBL § 349(h), Plaintiff is entitled to an injunction enjoining Defendant's wrongful acts and practices that violate GBL § 349, monetary damages in an amount to be proven at trial as a result of Defendant's willful and wrongful violations of GBL § 349, and an award of reasonable attorneys' fees and costs.

FOURTH CAUSE OF ACTION
(Violations of GBL §§ 350 and 350-a)

149. Plaintiff repeats and re-alleges each and every allegation set forth in the preceding and following paragraphs as if the same were fully set forth herein.

150. Plaintiff has been injured and suffered damages by Defendant's violations of GBL § 350, which states: "False advertising in the conduct of any business, trade or commerce or in the furnishing of any service in this state is hereby declared unlawful," and GBL § 350-a, which states: "The term 'false advertising' means advertising, including labeling, of a commodity . . . if such advertising is misleading in a material respect. In determining whether any advertising is misleading, there shall be taken into account (among other things) not only representations made by statement, word, design, device, sound or any combination thereof, but also the extent to which the advertising fails to reveal facts material in the light of such representations with respect to the commodity . . . to which the advertising relates under the conditions prescribed in said advertisement, or under such conditions as are customary or usual."

151. Defendant has engaged in consumer-oriented acts and practices in the State of New York, including false advertising, that are deceptive or misleading in a material way. Such acts and practices are likely to mislead a reasonable consumer acting reasonably under the circumstances.

152. Defendant's deceptive acts and practices and false advertising include false and materially misleading statements about its (purportedly) unrivaled and state-of-the-art cybersecurity practices, its supposed compliance with government guidelines and mandates, and its allegedly rigorous internal controls.

153. Defendant's deceptive acts and practices, including false advertising, have a

broad impact on the public at large, as they are disseminated to the public via state-wide advertising and promotions, and other public statements aimed at consumers throughout the State of New York.

154. Given the outsized role played by SS&C in handling customer funds and the potential for large dollar losses, this deception is particularly dangerous and worthy of the State's prompt attention.

155. Plaintiff justifiably relied on Defendant's false advertising.

156. Defendant's violations of GBL §§ 350 and 350-a caused damages to Plaintiff.

157. Had SS&C been truthful and not deceptive about its false advertising prior to the occurrence of the fraud detailed herein, Tillage's loss would not have occurred.

158. Pursuant to GBL § 350-e, Plaintiff is entitled to an injunction enjoining Defendant's wrongful acts and practices that violate GBL §§ 350 and 350-a, monetary damages in an amount to be proven at trial as a result of Defendant's willful and wrongful violations of GBL §§ 350 and 350-a, and reasonable attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays that judgment be entered in its favor and against Defendant as follows:

(i) Damages on each of its claims in an amount to be determined at trial, but no less than $10 million;

(ii) An injunction enjoining Defendant's wrongful acts and practices that violate GBL §§ 349, 350 and 350-a;

(iii) Punitive and/or exemplary damages in an amount to be determined at trial;

(iv) An award of pre- and post-judgment interest, attorneys' fees, costs, and disbursements in connection with this action; and

(v) Any other relief that the Court deems just and proper under the circumstances.

Dated: September 16, 2016
New York, New York

Respectfully submitted,

ARKIN SOLBAKKEN LLP

By: /s/ *Lisa C. Solbakken, Esq.*
Lisa C. Solbakken, Esq.
Alex Reisen, Esq.
750 Lexington Avenue, 25th Floor
New York, New York 10022
(212) 333-0200 (phone)
(212) 333-2350 (fax)

Attorneys for Plaintiff