Robin L. Cohen, Esq. (rcohen@mckoolsmith.com)
Radu A. Lelutiu, Esq. (rlelutiu@mckoolsmith.com)
MCKOOL SMITH P.C.
One Manhattan West, 50th Floor
New York, New York 10001
212-402-9400

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

VIRTU FINANCIAL, INC., AND VIRTU AMERICAS, LLC, Plaintiffs, v. AXIS INSURANCE COMPANY, Defendant.	Civil Action No. _____

COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiffs Virtu Financial, Inc. and Virtu Americas, LLC. (collectively, "Virtu") respectfully file this complaint against AXIS Insurance Company ("AXIS"). In support hereof, based on personal knowledge with respect to its own actions and information and belief with respect to the remaining allegations, Virtu states as follows:

INTRODUCTION

1. This is an action for breach of contract, anticipatory breach of contract, and breach of the implied covenant of good faith and fair dealing, arising out of AXIS's unjustified refusal to provide coverage under an insurance policy it sold to Virtu for substantial premiums.

2. Cyberattacks and hacking incidents have become a common occurrence in the life of financial institutions. As the *New York Times* reported last year, "Large financial companies have to thwart hundreds of thousands of cyberattacks every single day. . . . A single weak spot is all savvy hackers need. And they often find them. Already this year, there have been 3,494 successful cyberattacks against financial institutions, according to reports filed with the Treasury Department's Financial Crimes Enforcement Network. . . . Every big organization faces so many threats from so many sources that it can be hard to decide what is important. Mastercard, for example, combats some 460,000 intrusion attempts in a typical day, up 70 percent from a year ago."[1]

3. In 2019, recognizing the significant risk hacking and cyberattacks pose to its business, Virtu—one of the world's leading providers of financial and market-making services—purchased an insurance policy from AXIS that provides broad coverage for, among other things, "computer systems fraud."

4. In mid-May 2020, Virtu's computer systems were successfully hacked, and, as a result, the hackers obtained unauthorized access to the email account of a Virtu executive (the "Executive").

5. A day later, the hackers logged into the Executive's mailbox via Outlook Web Access and were able to view and read messages in the mailbox to and from the Executive.

6. Approximately 13 days later, the hackers created inbox rules that automatically hid certain messages sent from or received in the Executive's inbox. Later, beginning on the same day, pretending to be the Executive, the hackers sent a series of emails from the Executive's email account requesting that Virtu's accounting department issue two wire transfers to overseas banks—one in the amount of approx. $3.6 million, the other in the amount of approx.

[1] *See https://www.nytimes.com/2019/07/30/business/bank-hacks-capital-one.html.*

$7.2 million—for purported capital calls. Believing the requests to pertain to legitimate, ordinary-course business transactions, Virtu's accounting department complied with the requests.

7. A few days after the wire transfers were completed, during a routine reconciliation process, Virtu flagged the two wire transfers as potentially fraudulent and commenced an investigation. After a forensic review, Virtu concluded that the two wire transfers resulted from the hackers' unauthorized access into the Executive's email account and fraudulent use of Virtu's computer systems and networks.

8. Virtu promptly filed police reports and commenced various legal proceedings in an attempt to recoup the funds.

9. Within days of uncovering the hackers' wrongdoing, Virtu also gave notice to AXIS that it had suffered a loss from a computer systems fraud—the very type of fraud against which Virtu had purchased insurance.

10. After requesting significant volumes of information from Virtu, AXIS questioned the coverage requested by Virtu, asserting that "the unauthorized access into Virtu's computer system was not the direct cause of the loss," but rather, the loss was caused by "separate and intervening acts by employees of Virtu who issued the wire transfers because they believed the 'spoofed' email asking for the funds to be transferred to be true."

11. Virtu quickly pointed out the flaws in AXIS's reasoning and even provided a citation to a decision where, faced with a very similar factual scenario in the context of an *identical* coverage grant, this Court and the Second Circuit rejected the very argument AXIS appeared to be making.

12. In response, AXIS still refused to acknowledge coverage. Instead, AXIS lawyered up and, through outside litigation counsel, demanded additional, voluminous information. Virtu promptly complied with AXIS's information demands, but requested that AXIS confirm coverage by Monday August 3.

13. The August 3 deadline came and went and, to date, AXIS has refused to acknowledge coverage.

14. After months of attempting to persuade AXIS to acknowledge coverage and commit to covering Virtu's loss, Virtu has no choice but to file this lawsuit to enforce its contractual obligations.

THE PARTIES

15. Virtu Financial, Inc. is a Delaware corporation with its principal place of business in New York. Virtu Financial, Inc. is one of the largest providers of financial services, trading products and market making services.

16. Virtu Americas LLC is a single member limited liability company organized in the state of Delaware. Virtu Americas LLC is an indirect subsidiary of Virtu Financial, Inc.

17. AXIS is an Illinois corporation with its principal place of business in Alpharetta, Georgia. Upon information and belief, AXIS is authorized to sell or write insurance in New York and, at all material times, has conducted and continues to conduct substantial insurance business in the State of New York, including engaging in the business of selling insurance, investigating claims, and/or issuing policies that cover policyholders or activities located in New York.

JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332 based on complete diversity of the parties and an amount in controversy exceeding $75,000, exclusive of interest and costs.

19. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2).

THE POLICY

20. In 2019, Virtu purchased a Financial Institution Bond insurance policy, Bond No. MNN631443/01/2019 ("the Policy"). The term of the Policy is July 20, 2019 to July 20, 2020. The Policy is attached hereto as Exhibit A.

21. Of relevance here, the Policy provides (i) $10 million in coverage, subject to a $500,000 deductible, for losses resulting from computer systems fraud; and (ii) $500,000 in coverage, subject to a $250,000 deductible, for social engineering fraud.

Computer Systems Fraud Coverage

22. In Rider 6, the Policy provides that AXIS will cover:

> Loss resulting directly from a fraudulent
>
> (1) entry of **Electronic Data** or C**omputer Program** into, or
>
> (2) change of **Electronic Data** or **Computer Program**
>
> within any **Computer System** operated by the Insured, whether owned or leased; or any **Computer System** identified in the application for this bond; or a **Computer System** first used by the Insured during the Bond Period, as provided by General Agreement B of this bond;
>
> provided that the entry or change causes
>
> (i) **Property** to be transferred, paid or delivered,
>
> (ii) an account of the Insured, or of its customer to be added, deleted, debited or credited, or

> (iii) an unauthorized account or a fictitious account to be debited or credited.

23. All of the definitions that are relevant to the Computer Systems Fraud Coverage grant are broad. In particular:

> **Computer Program** is defined as "a set of related electronic instructions which direct the operations and functions of a computer or devices connected to it which enable the computer or devices to receive, process, store or send Electronic Data."
>
> **Computer System** is defined as "(1) computers with related peripheral components, including storage components wherever located, (2) systems and applications software, (3) terminal devices, and (4) related communications networks by which Electronic Data are electronically collected, transmitted, processed, stored and retrieved."
>
> **Electronic Data** is defined as "facts or information converted to a form usable in a Computer System by Computer Programs, and which is stored on magnetic tapes or disks, or optical storage disks or other bulk media.
>
> **Property** is defined to include money.

* * *

Social Engineering Fraud Coverage

24. In Rider 10, the Policy provides that AXIS will cover

> Loss resulting directly from an Employee having, in good faith, transferred, paid, or delivered Money or Securities from the Insured's account to a person or account outside of the Insured's control, in reliance upon a **Social Engineering Fraud Instruction** directing such transfer, payment, or delivery of Money or Securities.

25. **Social Engineering Fraud Instruction** is defined as "a telephonic, written, or electronic instruction communicated to an Employee by a natural person purporting to be an Authorized Transfer Agent, or by an individual acting in collusion with such person, for the purpose of intentionally misleading an Employee to transfer, pay, or deliver the Insured's Money or Securities, but which instruction was not actually made by an Authorized Transfer Agent; provided, however, that Social Engineering Fraud Instruction shall not include any such

instruction communicated by an employee of a Vendor who was acting in collusion with any third-party in communicating such instruction."

26. **Authorized Transfer Agent** is defined, in relevant part as "(1) a director, officer, partner, member, or sole proprietor of the Insured; or (2) an Employee who is authorized by the Insured to instruct other Employees to transfer, pay, or deliver the Insured's Money or Securities."

THE HACKING INCIDENT AND THE RESULTING LOSS

27. On or around May 13, 2020, one or more hackers gained unauthorized access to the email account of the Executive.

28. About one day later, the hackers logged into the Executive's mailbox via Outlook Web Access from an IP address that traces back to Amazon Web Services. The hackers continued to log in from this IP address routinely over the following two weeks and were able to read and review inbound and outbound emails.

29. On May 26, 2020, to retain control of the mailbox and set the stage for the fraudulent transactions that would later unfold, the hackers created inbox rules that allowed them to hide certain messages in the mailbox from the Executive. Later on the same date, the hackers—posing as the Executive—sent an email to certain of Virtu's accounting personnel requesting the transfer of approx. $3.6 million to a bank located in China. The hackers—posing as the Executive—asserted that the funds were needed for an ordinary-course transaction.

30. Believing that the hackers' email was in fact sent by the Executive, Virtu's accounting personnel executed the wire transaction.

31. On or around May 27, 2020, the hackers—posing as the Executive—sent an email to certain of Virtu's accounting personnel requesting the transfer of approx. $7.2 million to

another bank located in China. The hackers—posing as the Executive—again asserted that the funds were needed for an ordinary-course capital call.

32. Believing that the hackers' email was in fact sent by the Executive, Virtu's accounting personnel executed the wire transaction.

33. All of the hackers' emails were transmitted via Virtu's computer systems and from the Executive's actual email account and, in all respects, appeared to be legitimate.

34. To set up the rules that prevented the Executive from seeing the email traffic between the hackers and Virtu's accounting personnel and thereafter send the emails on behalf of the Executive, the hackers entered Electronic Data or Computer Programs into and/or changed Electronic Data or Computer Programs associated with Virtu's computer systems.

35. On or around May 29, 2020, during a routine reconciliation of Virtu's accounts, Virtu flagged the two wire transfers as potentially fraudulent.

36. Virtu began a prompt investigation that included, among other things, a forensic review of server logs and of the Executive's various devices. The investigation, which was later corroborated by a third-party forensic consultant, revealed the information detailed above.

37. Virtu promptly reported the matter to the law enforcement authorities and commenced various efforts to recoup the money.

38. After extensive efforts, Virtu's legal team was able to obtain an injunction freezing (i) approx. $3.6 million; and (ii) approx. $287,474 in two accounts held within the Bank of China.

39. However, Virtu believes it unlikely that the remaining funds (approx. $6.915 million) will be recovered. In addition, Virtu has incurred significant forensic and legal costs to investigate the hacking incident and seek to recoup the funds.

VIRTU'S REQUEST FOR COVERAGE

40. On June 1, 2020, through its insurance broker, Virtu gave notice to AXIS and requested that AXIS confirm coverage for the hacking incident and the resulting loss (the "Hacking Claim").

41. In response, AXIS requested that Virtu fill out a detailed proof of loss, which Virtu promptly did. The proof of loss and a sword affidavit Virtu provided with the proof of loss are attached hereto as Exhibit B.

42. On June 26, 2020, a representative of AXIS, Fred Zauderer, wrote to Virtu advising that, based on an "initial review and subject to further investigation, it appears that Virtu has sustained a single Social Engineering Fraud ('SEF') loss." A copy of Mr. Zauderer's June 26, 2020 email is included in Exhibit C attached hereto.

43. Virtu's general counsel promptly wrote back to Mr. Zauderer, explaining that Virtu believed that it was also entitled to Computer Systems Fraud Coverage. In response, Mr. Zauderer wrote: "I do not believe that this incident is covered under Rider 6 of the AXIS policy. The unauthorized access into Virtu's computer system was not the direct cause of the loss. It appears that there were separate and intervening acts by employees of Virtu who issued the wire transfers because they believed the 'spoofed' email asking for the funds to be transferred to be true." *See* Exhibit C.

44. The next business day, through the undersigned counsel, Virtu responded to Mr. Zauderer, explaining that AXIS's causation arguments were incorrect, and that "[t]he proximate cause of the Loss was the series of fraudulent emails sent by the hackers, using Virtu's computer systems/networks, and not the actions of Virtu's accounting department." A copy of this correspondence is attached hereto as Exhibit D.

45. Counsel for Virtu also explained that, in *Medidata Solutions Inc. v. Federal Insurance Co.*, 729 F. App'x 117, 119 (2d Cir. 2018), the Second Circuit had "addressed a scenario virtually identical to the one at issue here—in the context of an *identical* coverage grant—and unambiguously rejected the very argument AXIS made in the June 26, 2020 correspondence."

46. Counsel for Virtu requested that AXIS confirm coverage under Rider 6 by July 3, 2020.

47. AXIS thereafter hired its own coverage counsel. But instead of recognizing that AXIS's causation arguments were meritless, counsel for AXIS sent Virtu yet another laundry list of documents and information requests.

48. Even though Virtu believed that much of the information requested by AXIS was contained in a sworn affidavit Virtu provided to AXIS in mid-June, Virtu promptly complied with all of AXIS's requests.

49. On July 27, 2020, counsel for Virtu advised AXIS that it needed confirmation by "Monday, August 3, that the Loss is covered under Rider 6," and that, "[a]bsent such confirmation, we have been instructed to seek prompt judicial assistance to compel AXIS to comply with its contractual obligations to Virtu." A copy of counsel's correspondence is attached hereto as Exhibit E.

50. On Friday, July 31, 2020, counsel for AXIS responded to Virtu's July 27 correspondence, advising that AXIS would not provide its coverage position by the deadline requested by Virtu.

51. Based on AXIS's course of conduct and Mr. Zauderer's statement that no coverage is available under Rider 6, Virtu believes that AXIS intends to deny coverage.

COUNT ONE

(BREACH OF CONTRACT)

52. Virtu repeats and realleges the allegations contained in the foregoing as if fully set forth herein.

53. The Policy is a valid and enforceable contract.

54. Virtu Financial, Inc. and Virtu Americas LLC are insureds under Policy.

55. The Hacking Claim constitutes a covered Claim under the Policy.

56. Virtu has given AXIS timely notice under the Policy of the Hacking Claim.

57. Virtu has fully complied with all terms, conditions and prerequisites to coverage set forth in the Policy, or has been excused from compliance with such terms, conditions or prerequisites in connection with the Hacking Claim.

58. AXIS's June 26, 2020 rejection of coverage under Rider 6 for the Hacking Claim and/or refusal to take a timely coverage position constitutes a breach of contract.

59. As a result of that breach, Virtu has been and will continue to be damaged in an amount to be determined at trial.

COUNT TWO

(ANTICIPATORY BREACH OF CONTRACT)

60. Virtu repeats and realleges the allegations contained in the foregoing as if fully set forth herein.

61. The Policy is a valid and enforceable contract.

62. Virtu Financial, Inc. and Virtu Americas LLC are insureds under Policy.

63. The Hacking Claim constitutes a covered Claim under the Policy.

64. Virtu has given AXIS timely notice under the Policy of the Hacking Claim.

65. Virtu has fully complied with all terms, conditions and prerequisites to coverage set forth in the Policy, or has been excused from compliance with such terms, conditions or prerequisites in connection with the Hacking Claim.

66. AXIS's June 26, 2020 rejection of coverage under Rider 6 for the Hacking Claim and/or refusal to take a timely coverage position indicate that AXIS intends to breach its contractual obligation to Virtu.

67. As a result of AXIS's actions, Virtu has been and will continue to be damaged in an amount to be determined at trial.

COUNT THREE

(BREACH OF THE COVENANT OF GOOD FAITH AND FAIR DEALING)

68. Virtu repeats and realleges the allegations contained in the foregoing as if fully set forth herein.

69. The Policy contains an implied covenant of good faith and fair dealing.

70. Pursuant to that covenant, AXIS is required to (i) deal with claims expeditiously and fairly; (ii) refrain from taking meritless coverage positions that fail even the most basic tenants of contractual interpretation and New York insurance coverage precedent; and (iii) refrain from unnecessarily inflicting costs—including legal costs—on Virtu by taking unprincipled coverage positions, let alone tactically demanding significant volumes of information in an attempt to delay.

71. Through the repeated actions and tactics described herein, AXIS has breached the covenant of good faith and fair dealing set forth in New York Insurance Law § 2601(a).

72. As a result of AXIS's breach, Virtu has suffered and will continue to suffer damages in an amount to be determined in this action, including pre- and post-judgment interest.

73. AXIS's bad faith conduct towards Virtu is egregious, willful, and malicious, entitling Virtu to punitive damages in an amount to be determined at trial.

WHEREFORE, Plaintiffs request that the Court enter an order and judgment herein:

(i) On Counts One and Two, judgment declaring that AXIS must pay the Hacking Claim;

(ii) On Count Three, judgment declaring that AXIS has breached the covenant of good faith and fair dealing through its bad faith conduct;

(iii) On all Counts, awarding all costs incurred as a consequence of having to prosecute this lawsuit, including attorneys' fees; and

(iv) On all causes of action, awarding Plaintiffs such other and further relief as in law and justice it may be entitled to receive.

Dated: August 10, 2020

Respectfully submitted,

Robin L. Cohen, Esq.
rcohen@mckoolsmith.com
Radu A. Lelutiu, Esq.
rlelutiu@mckoolsmith.com
MCKOOL SMITH P.C.
One Manhattan West, 50th Floor
New York, New York 10001
212-402-9400
Attorneys for Plaintiffs