IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA
Roanoke Division

THE NATIONAL BANK OF BLACKSBURG, Plaintiff, v. EVEREST NATIONAL INSURANCE COMPANY, Defendant.	)	Civil Action No. 7:18CV310

Plaintiff, The National Bank of Blacksburg ("Plaintiff" or "National Bank"), hereby files this complaint for Declaratory Judgment, Breach of Contract, and Bad Faith denial of coverage under a financial institution bond against Everest National Insurance Company ("Defendant" or "Everest") and states as follows:

NATURE OF COMPLAINT

1. This Complaint requests that the Court issue judgment pursuant to 28 U.S.C. § 2201, declaring that the financial institution Bond No. 8100003956-141 (the "Bond") issued by Everest requires it to indemnify National Bank under the Bond's Computer & Electronic Crime Rider ("C&E Crime Rider") for the losses it suffered as a direct result of unauthorized hacking and intrusions into National Bank's computer systems.

2. The hacking allowed unidentified criminal actors, through coordinated unauthorized intrusions into National Bank's computer systems and network, to change customer account balances, monitor network communications, remove critical security measures such as anti-theft and anti-fraud protections, conduct keystroke tracking, and otherwise enter or change electronic data and computer programs on National Bank's computer

systems, which allowed them to illegally withdraw funds from the accounts of National Bank customers, post fake deposits, and remove illegal transactions from customer accounts. But for this unlawful hacking and the intrusions into its computer systems, National Bank would not have suffered any losses.

3. Critical to this Court's analysis of National Bank's claims, none of the losses arise from a National Bank customer's debit card being stolen, or from their debit card information being stolen directly from a National Bank customer's possession without their knowledge or permission (e.g. use of a "skimmer" or of a counterfeit or fraudulently obtained debit card).

4. Despite the foregoing facts, Everest has denied coverage for the losses set out in National Bank's proof of loss claims under the Bond's C&E Crime Rider; claiming instead that National Bank's losses fall under the Bond's Debit Card Rider ("Debit Card Rider") and its much lower coverage limit.

5. National Bank will request leave from this Court to file the complete proof-of-loss claim forms filed with Everest under seal, for *in camera* review, in order to protect the confidential information contained therein and not impede any ongoing criminal investigation into this matter. Review of the proof-of-loss claims will demonstrate that the losses under the Bond were the result of sophisticated computer system intrusions and hackings.

6. Declaratory judgment is requested to determine an actual controversy between the parties regarding insurance coverage under the Bond for National Bank's losses.

7. This Complaint further requests that the Court enter judgment awarding damages in favor of National Bank and against Everest for breach of contract and bad faith denial of coverage under the Bond.

THE PARTIES

8. National Bank is a bank organized and existing under the laws of the United States of America with its principal place of business located at 100 South Main Street, Blacksburg, Virginia 24060.

9. Upon information and belief, Everest is a corporation organized and existing under the laws of the State of Delaware with its principal place of business located at 477 Martinsville Road, Liberty Corner, New Jersey 07938-0830.

JURISDICTION AND VENUE

10. This Court has jurisdiction over the subject matter of this case pursuant to 28 U.S.C. § 1332(a) because it involves a controversy between citizens of different states and the amount in controversy exceeds $75,000.

11. This Court has personal jurisdiction over Everest because it transacts business in the Western District of Virginia, entered into the contract at issue in this action in the Western District of Virginia, and has minimum contacts with the Western District of Virginia.

12. Venue is proper in this district pursuant to 28 U.S.C. § 1391.

FACTUAL BACKGROUND

Facts Common to Both Computer System Intrusions

13. National Bank and Everest are parties to the Bond, a true and correct copy of which is attached hereto as **Exhibit A**. The Bond provided insurance coverage to National Bank against certain financial losses for the period of November 1, 2014 through November 1, 2017 (the "Bond Period"). The Bond was in full force and effect during the entire Bond Period.

14. The Bond contains a C&E Crime Rider which provides coverage for losses which result directly from an intrusion into National Bank's computer system. Specifically, the C&E Crime Rider insures National Bank against:

> Loss resulting directly from an unauthorized party (other than an Employee) acting alone or in collusion with others, entering or changing Electronic Data or Computer Programs within any Computer System[1] . . . operated by the Insured . . . [p]rovided that the entry or change causes: (1) property [e.g. money] to be transferred, paid or delivered, (2) an account of the Insured [National Bank], or of its customer, to be added, deleted, debited or credited, or (3) an unauthorized account or a fictitious account to be debited or credited.

15. The C&E Crime Rider has a Single Loss Limit of Liability of $8,000,000.00 with a $125,000.00 deductible.

16. The Bond also contains a Debit Card Rider which provides coverage for losses which result directly from the use of lost, stolen or altered debit cards or counterfeit debit cards. Specifically, under the relevant portions of the Debit Card Rider, the Bond covers: "Loss resulting directly from Debit Transactions, or automated mechanical device transactions, due to the fraudulent use of a lost, stolen or altered Debit Card or Counterfeit Debit Card used to access a cardholder's deposit account through an electronic payment device or automated mechanical device." The Debit Card Rider also contains certain limitations and exclusions to coverage not applicable here.

17. The Debit Card Rider has a Single Loss Limit of Liability of $50,000.00 with a $25,000.00 deductible. The Debit Card Rider also has an Aggregate Limit of $250,000.00.

18. The Bond also contains certain exclusions. Relevant here are Exclusions K and L, relied upon by Defendant in denying coverage to National Bank under the C&E Crime Rider.

[1] Unless otherwise defined in this Complaint, all capitalized terms shall have the same meaning as set forth in the Bond.

19. Exclusion K to the Bond excludes coverage for: "loss resulting directly or indirectly from the use or purported use, of credit, debit, charge, access, convenience, or other cards . . . (1) in obtaining credit or funds, or (2) in gaining access to automated mechanical devices which, on behalf of the Insured, disburse Money, accept deposits, cash checks, drafts or similar Written instruments or make credit card loans . . .."

20. Further, Exclusion L to the Bond excludes coverage for: "loss involving automated mechanical devices which, on behalf of the Insured, disburse Money, accept deposits, cash checks, drafts or similar Written instruments or make credit card loans . . .."

21. National Bank uses STAR Processing, Inc. (hereinafter "FirstData") to provide bank card processing services for National Bank customers. FirstData was the exclusive provider of bank card processing services to National Bank during the Bond Period.

22. FirstData provides bank card processing services to National Bank through the STAR Network ("STAR Network"). The STAR Network is a debit payment network that allows National Bank customers to use their bank cards at automatic teller machines (ATMs) and retailers.

23. National Bank employees access the STAR Network through a web portal, which is only accessible through certain computer workstations, which themselves are only accessible by certain National Bank employees.

24. The STAR Network web portal allows National Bank employees substantial control over the parameters of National Bank customers' use of their bank cards, including use at ATMs and retailers. These parameters include the ability to remove or alter anti-theft and anti-fraud protections such as 4-digit personal identification numbers (PINs), daily withdrawal limits, daily debit card usage limits, and fraud score protections.

25. The STAR Network web portal also allows National Bank employees to block or activate customer accounts.

The 2016 Intrusion

26. In late May 2016, an unauthorized party or parties (the "Intruders") unlawfully gained entry into and hacked National Bank's Computer Systems (the "2016 Intrusion").

27. All losses related to the 2016 Intrusion were the result of and would not have been possible but for the hacking of National Bank's Computer Systems which resulted in the entering or changing of Electronic Data and Computer Programs within its Computer Systems.

28. Upon information and belief, the unlawful hacking and entering or changing of Electronic Data and Computer Programs within National Bank's Computer System originated in Russia.

29. Within days of being informed of the 2016 Intrusion, National Bank hired Foregenix, a digital forensics and security firm, to investigate the 2016 Intrusion.

30. Upon the completion of its investigation, Foregenix produced a report to National Bank (the "Foregenix Report"). A true and correct copy of the Foregenix Report will be offered for production under seal, for *in camera* review by the Court.

31. The Foregenix Report determined that the 2016 Intrusion likely originated from a phishing email which allowed the installation of malware that permitted unauthorized access to National Bank's Computer Systems through a compromised computer workstation ("Workstation One").

32. Upon information and belief, the phishing email allowed the Intruders to install additional unknown malicious computer script or malware in order to remotely control

Workstation One and network to a separate workstation, ("Workstation Two") utilizing National Bank's Computer Systems and internal network.

33. At the time of the 2016 Intrusion, Workstation Two had access to the STAR Network and the ability to manage National Bank customer accounts and their use of ATMs (Automatic Teller Machines) and bankcards.

34. The Intruder(s) also transferred and installed malware onto National Bank's Computer Systems that allowed the Intruder(s) to identify and steal certain National Bank employees' usernames and passwords. As a result, the Intruder(s) gained unauthorized administrative-level access to the STAR Network.

35. With administrative-level access, the Intruder(s) were able to actively monitor customer accounts and remove or modify numerous security measures on accounts belonging to National Bank customers. But for the removal of these security measures, the Intruder(s) would have been unable to carry out their bank robbery.

36. Beginning on Saturday, May 28, 2018 and continuing through the early morning of Monday, May 30, 2018, the Intruder(s) used hundreds of ATMs across North America to dispense funds from National Bank customer accounts. At this time, the Intruder(s) had unrestricted access to National Bank's Computer Systems, customer accounts, and the STAR Network. The exact mechanics of this criminal enterprise are still not fully known.

37. During the 2016 Intrusion, the Intruder(s) used Workstation Two to actively monitor the customer accounts from which funds were being fraudulently removed. This allowed the Intruder(s) to continue their fraudulent withdrawals by removing blocks and returning customer accounts to active status.

38. The removal or modification of security measures, combined with the Inturder(s) ability to remove blocks and return accounts to active status, had the effect of allowing extensive ATM withdrawals from the compromised customer accounts that could not otherwise have been obtained.

39. The total loss resulting from these fraudulent disbursements, related fees, and other incidental transactions was $569,648.24 (the "2016 Loss").

40. National Bank was alerted to the 2016 Intrusion on the morning of May 30, 2016, when an officer of National Bank was notified of the fraudulent removal of funds by representatives from VISA, Inc.

41. After being notified of the criminal activity, National Bank took immediate steps to prevent any further fraudulent withdrawals from customer accounts. National Bank also made sure that all unauthorized adjustments to or withdrawals from customer accounts were corrected such that all National Bank customers were made whole from any possible losses.

42. By June 1, 2016, National Bank had identified each customer account that had money fraudulently withdrawn from it and had credited the accounts for any fraudulently withdrawn funds from its own general ledger account. As a result, on June 1, 2016, National Bank suffered a loss of $569,648.24.

43. Later in June, after the 2016 Intrusion ended, National Bank, working in coordination with FirstData, implemented additional security protocols, as recommended by FirstData. These protocols are known as "Velocity Rules" and were implemented in order to provide additional layers of security.

44. On or about July 27, 2017, National Bank timely filed its sworn proof of loss claim for the 2016 Intrusion with Everest ("2016 Proof of Loss"). A true and correct copy of the 2016 Proof of Loss will be offered for production under seal, for *in camera* review by the Court.

45. In its 2016 Proof of Loss, National Bank detailed that its losses of $569,648.24 resulting from the 2016 Intrusion were covered under the C&E Crime Rider because the losses resulted directly from and would not have happened but for the entry or changing of Electronic Data, e.g. the removal of critical security measures, and/or Computer Programs, e.g. malware such as key stroke loggers and remote access controls, and were thus fully recoverable, less the applicable deductible.

46. On June 13, 2018, Everest, through its third-party claims administrator, issued a coverage determination ("Coverage Determination") in relation to the 2016 Proof of Loss. A true and correct copy of the Coverage Determination will be offered for production under seal, for *in camera* review by the Court.

47. In its Coverage Determination, Everest denied coverage for the 2016 intrusion under the C&E Crime Rider.

48. In its Coverage Determination, Everest asserted that the losses incurred by National Bank and identified in the 2016 Proof of Loss were, instead, covered exclusively under the Debit Card Rider.

49. Everest further asserted that, absent the Debit Card Rider, the Bond provided no coverage to National Bank for the 2016 Intrusion because of Exclusion K and Exclusion L to the Bond.

50. The Coverage Determination provided to National Bank is inconsistent with the terms of the Bond and improperly denied coverage under the C&E Crime Rider to National Bank.

The 2017 Intrusion

51. In early January 2017, an unauthorized party or parties unlawfully gained entry into and hacked National Bank's Computer Systems (the "2017 Intrusion").

52. Upon information and belief, the same Intruder(s) responsible for the 2016 Intrusion were also responsible for the 2017 Intrusion.[2]

53. All losses related to the 2017 Intrusion were the result of and would not have been possible but for the hacking of National Bank's Computer Systems which resulted in the entering or changing of Electronic Data and Computer Programs within the Computer Systems.

54. Within days of being informed of the 2017 Intrusion, National Bank hired Verizon, which provides digital forensics and security consulting to its commercial customers, to fully investigate the 2017 Intrusion.

55. Upon the completion of its investigation, Verizon produced a report to National Bank (the "Verizon Report"). A true and correct copy of the Verizon Report will be offered for production under seal, for *in camera* review by the Court.

56. The Verizon Report determined that, like the 2016 Intrusion, the 2017 Intrusion most likely originated from a phishing email to a National Bank employee.

57. Unlike the 2016 Intrusion, this phishing email contained a malicious macro Word document which downloaded malware capable of, among other things, stealing username and passwords and controlling National Bank's computer system.

[2] For purposes of clarity, and because National Bank believes the 2017 Intrusion was perpetrated by the same group of unauthorized individuals, these individuals will also be referred to as the "Intruder(s)".

58. According to the Verizon Report, the malware likely originated from an IP address in Russia.

59. During the time period the Intruders had access to National Bank's computer network, the Intruder(s) compromised and installed malware on multiple National Bank employee workstations and accounts. One of the workstations compromised during the 2017 Intrusion was Workstation Two, which at the time had access to the STAR Network.

60. At the time of the 2017 Intrusion, Workstation Two also had access to Navigator, which is software used by National Bank to manage its customer's banking transactions including credits and debits to customer accounts.

61. Upon information and belief, once the Intruder(s) gained access to National Bank's computer system they used malware downloaded onto National Bank's computer system to obtain employee user credentials and passwords for both the STAR Network and Navigator.

62. The Intruder(s) accessed Workstation Two and another workstation multiple times in order to enter and change Electronic Data and Computer Programs in National Bank's Computer System. The Intruder(s) also established a network connection between both workstations and a Russian IP address using the malware they had installed.

63. For a period of time, the Intruder(s) had administrative-level access to National Bank's customer accounts, the Star Network, and Navigator, through Workstation Two. With this administrative-level access, the Intruder(s) used Navigator to fraudulently credit $2,070,000.00 to certain National Bank customer accounts.

64. These fraudulent credits increased the amount of money the Intruder(s) could fraudulently withdraw from the affected customer accounts by hundreds of thousands of dollars.

65. From January 7, 2017 until January 9, 2017, the Intruder(s), using the STAR Network and Workstation Two, removed or modified critical security and anti-theft measures associated with the customer accounts that were fraudulently credited.

66. Beginning on January 7, 2017, and lasting through the morning of January 9, 2017, the Intruder(s) used hundreds of ATMs to access these funds from the same customer accounts in a coordinated criminal enterprise and bank robbery.

67. During the 2017 Intrusion, the Intruder(s) used WorkStation Two and the STAR Network to actively monitor the customer accounts from which funds were being fraudulently withdrawn. This allowed the Intruder(s) to remove blocks, activate accounts and continue to access and remove funds from the affected accounts.

68. The Intruder(s) also used Navigator to delete fraudulent debits from customer accounts.

69. The removal or modification of National Bank's security measures and the removal of account blocks and fraudulent debits had the effect of allowing extensive ATM withdrawals from the compromised customer accounts that could not otherwise have been obtained.

70. The total loss resulting from these fraudulent disbursements, related fees, and other incidental transactions was $1,833,984.58 (the "2017 Loss").

71. National Bank was alerted to the 2017 Intrusion on the morning of January 9, 2017, when an officer of National Bank was alerted to the fraudulent withdrawals.

72. After being notified of the criminal activity, National Bank took immediate steps to prevent any further fraudulent withdrawals from customer accounts.

73. By January 10, 2017, National Bank had identified each customer account that had money fraudulently credited and then withdrawn from it. The Intruder(s) only removed funds that had been fraudulently credited to the accounts using Navigator.

74. National Bank removed the fraudulent credits and withdrawals and placed them on its own general ledger account. As a result, on January 10, 2017, National Bank suffered a loss of $1,833,984.58.

75. On or about July 27, 2017, National Bank timely filed its sworn proof of loss claim for the 2017 Intrusion with Everest ("2017 Proof of Loss"). A true and correct copy of the 2017 Proof of Loss will be offered for production under seal, for *in camera* review by the Court.

76. In its 2017 Proof of Loss, National Bank asserted that the 2017 Loss was covered under the C&E Crime Rider and thus fully recoverable minus the applicable deductible.

77. On June 13, 2018, Everest, through its third-party claims administrator, issued its Coverage Determination in relation to the 2017 Proof of Loss. In its Coverage Determination, Everest denied coverage for the 2017 Intrusion under the C&E Crime Rider. A true and correct copy of the Coverage Determination will be offered for production under seal, for *in camera* review by the Court.

78. In its Coverage Determination, Everest asserted that the losses incurred by National Bank and identified in the 2017 Proof of Loss were covered under the Debit Card Rider.

79. Everest further determined that absent the Debit Card Rider, the Bond provides no coverage to National Bank for the 2017 Intrusion because of Exclusion L and Exclusion K to the Bond.

80. In its Coverage Determination, Everest further determined that the 2016 Intrusion and the 2017 Intrusion were a single event, and thus, pursuant to the Debit Card Rider, National Bank's total coverage under the Bond was $50,000.00 for both intrusions.

81. Everest's Coverage Determination was inconsistent with and contrary to the terms of the Bond.

82. In its Coverage Determination, Everest agreed that National Bank had established that its losses suffered from the 2016 Intrusion and the 2017 Intrusion totaled $2,433,632.82.

COUNT ONE – DECLARATORY JUDGMENT

83. National Bank repeats and alleges the allegations of paragraphs 1 through 82 as if fully set forth herein.

84. Based upon the actions of the Intruder(s), including but not limited to their unauthorized entry into and hacking of National Bank's Computer Systems, the 2016 Loss and the 2017 Loss are covered under the Bond's C&E Crime Rider, which covers losses resulting directly from an unauthorized party entering or changing Electronic Data or Computer Programs on National Bank's Computer Systems.

85. Everest is contractually obligated under the Bond to fully cover National Bank for the 2016 Loss and the 2017 Loss under the C&E Crime Rider.

86. In its Coverage Determination, Everest asserted that the 2016 Loss and the 2017 Loss were not covered under the Bond's C&E Crime Rider but, instead, were covered exclusively under the Bond's Debit Card Rider or were otherwise excluded under one or more of the Bond's exclusions.

87. There exists an actual case and controversy between Everest and National Bank that is justiciable in nature as to whether the 2016 Loss and the 2017 Loss are covered under the Bond's C&E Crime Rider.

88. Wherefore, Plaintiff, National Bank, asks this Court to enter judgment pursuant to 28 U.S.C. § 2201 against Defendant, Everest, and in favor of National Bank, adjudging and declaring that Everest has a duty to fully indemnify National Bank for both the 2016 Loss and the 2017 Loss under the Bond's C&E Crime Rider.

COUNT TWO – BREACH OF CONTRACT

89. National Bank repeats and alleges the allegations of paragraphs 1 through 88 as if fully set forth herein.

90. The Bond is a valid and enforceable insurance contact.

91. Everest has a duty to indemnify National Bank for the 2016 Loss and the 2017 Loss under the Bond's C&E Crime Rider.

92. Everest breached its duty to National Bank under the Bond by determining that the 2016 Loss and the 2017 Loss were not covered under the Bond's C&E Crime Rider; by its refusal to fully compensate National Bank for the 2016 Loss and the 2017 Loss under the C&E Crime Rider; and by determining that the 2016 Loss and 2017 Loss were covered under the Bond's Debit Card Rider or were otherwise not covered under one or more of the Bond's exclusions.

93. As a direct result of Everest's breaches of the Bond, National Bank has suffered damages of $2,433,632.82, less any applicable deductible.

COUNT THREE – STATUTORY ATTORNEY'S FEES

94. National Bank repeats and alleges the allegations of paragraphs 1 through 93 as if fully set forth herein.

95. The 2016 Loss is covered under the Bond's C&E Crime Rider.

96. The 2017 Loss is covered under the Bond's C&E Crime Rider.

97. On June 13, 2018, Everest provided its Coverage Determination which states that National Bank had established that its total losses suffered from the 2016 Intrusion and the 2017 Intrusion was $2,433,632.82.

98. Everest did not have a good faith basis to deny coverage under the Bond's C&E Crime Rider for National Bank's losses from the 2016 Intrusion or the 2017 Intrusion.

99. Under Va. Code Ann. § 38.2-209, should the Court determine that Everest did not act in good faith in denying coverage to National Bank under the Bond's C&E Crime Rider for its losses from the 2016 and/or 2017 Intrusions, National Bank is entitled to recover from Everest such costs and reasonable attorney's fees as the Court may award.

PRAYER FOR RELIEF

WHEREFORE, the Plaintiff respectfully prays for:

a. Judgment on Count One pursuant to 28 U.S.C. § 2201 against Defendant, Everest, and in favor of Plaintiff, National Bank, adjudging and declaring that Everest has a duty to fully indemnify National Bank for the both the 2016 Loss and the 2017 Loss under the Bond's C&E Crime Rider, pursuant to the terms of the Bond;

b. Judgment on Count Two against Defendant, Everest, and in favor of Plaintiff, National Bank, for all damages arising from Defendant's breach of contract, totaling $2,433,632.82;

c. Judgment on Count Three against Defendant, Everest, and in favor of Plaintiff, National Bank, for attorney's fees, costs, and all other fees and expenses permitted by Va. Code Ann. § 38.2-209; and

d. Judgment against Defendant, Everest, and in favor of Plaintiff, National Bank for any and all further relief as this Court deems just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure Rule 38(b), Plaintiff hereby demands a jury trial on all issues so triable.

Respectfully submitted,

By: **s/ James K. Cowan, Jr.**
Counsel

Douglas W. Densmore (VSB 19994)
James K. Cowan, Jr. (VSB 37163)
Brian S. Wheeler (VSB 74248)
Eric D. Chapman (VSB 86409)
CowanPerry PC
250 South Main Street, Suite 226
Blacksburg, Virginia 24060
Telephone: (540) 443-2850
Facsimile: (888) 755-1450
ddensmore@cowanperry.com
jcowan@cowanperry.com
bwheeler@cowanperry.com
echapman@cowanperry.com

Counsel for Plaintiff, The National Bank of Blacksburg