STATE OF NORTH CAROLINA

COUNTY OF MECKLENBURG

PARK STERLING BANK,

Plaintiff,

vs.

WALLACE & PITTMAN, PLLC

Defendant.

IN THE GENERAL COURT OF JUSTICE
SUPERIOR COURT DIVISION
12 CVS 12725

ANSWER, AFFIRMATIVE DEFENSES & COUNTERCLAIMS

Wallace & Pittman, PLLC ("Wallace & Pittman"), by and through counsel, answers the Complaint of Plaintiff Park Sterling Bank (the "Bank") as follows:

PARTIES, JURISDICTION, AND VENUE

1. Wallace & Pittman lacks knowledge or information sufficient to form a belief regarding the allegations of Paragraph 1.

2. Wallace & Pittman admits the allegations of Paragraph 2.

3. Wallace & Pittman admits the allegations of Paragraph 3.

4. Admitted.

5. Admitted.

FACTS

6. The allegations of the preceding paragraphs are incorporated herein as if set forth in full.

7. Admitted.

8. Wallace & Pittman admits the existence of the Account Agreement, which is in writing, speaks for itself and is the best evidence of its contents. Except as admitted, Wallace & Pittman denies the allegations of Paragraph 8.

9. Wallace & Pittman admits the existence of the Treasury Management Products Agreement, which is in writing, speaks for itself and is the best evidence of its contents. Except as admitted, Wallace & Pittman denies the allegations of Paragraph9.

10. Wallace & Pittman admits that it received access to the Bank's online banking service that allowed designated employees of Wallace & Pittman to access its account information and to order funds transfers electronically, including wire transfers, from its accounts. Wallace & Pittman denies the allegation that such online banking service was "secure."

11. Admitted.

12. Wallace & Pittman admits the existence of the Treasury Management Products Agreement, which is in writing, speaks for itself and is the best evidence of its contents. Except as admitted, Wallace & Pittman denies the allegations of Paragraph 12.

13. Wallace & Pittman admits the existence of the Treasury Management Products Agreement, which is in writing, speaks for itself and is the best evidence of its contents. Except as admitted, Wallace & Pittman denies the allegations of Paragraph 13.

14. Wallace & Pittman admits that it believed that the authenticity of payment orders issued by Defendant to PSB would be verified pursuant to security procedures that included, among other things, verification of Defendant's user name, password, pin number and use of challenge questions. Except as admitted, Wallace & Pittman denies the allegation of Paragraph 14.

15. Denied.

16. Denied.

17. Wallace & Pittman denies that the Bank received a wire transfer order at 2:58 PM EDT [sic] on May 9, 2012 from Wallace & Pittman. Defendant lacks knowledge or information regarding the remaining allegations of Paragraph 17.

18. Wallace & Pittman admits that the wire transfer directed payment to JP Morgan Chase, in New York for the benefit of a "Konstantin Pomogalove" for credit to an account in Moscow, Russia. Except as admitted, Wallace & Pittman denies the allegations of Paragraph 18.

19. Denied.

20. Denied.

21. Wallace & Pittman admits that the beneficiary identified in the wire transfer order was listed as being located in Moscow, Russia. Defendant lacks knowledge or information sufficient to form a belief about the remaining allegations of Paragraph 21.

22. Admitted.

23. Wallace & Pittman admits that the Bank had been made aware of electronic intrusions on its computers and that keylogger malware was placed on one or more of its computers. Wallace & Pittman deny the remaining allegations of Paragraph 23.

24. Wallace & Pittman lacks knowledge or information sufficient to form a belief regarding the allegations of Paragraph 24.

25. Wallace & Pittman admits that, at some point after being notified of the suspicious transaction, the Bank attempted to reverse the transfer order and to retrieve the funds but was unable to do so. Wallace & Pittman further admits that funds were

transferred out of the IOLTA account on May 9, 2012. Except as admitted, Wallace & Pittman denies the allegations of Paragraph 25.

26. Denied.

27. Admitted.

28. Admitted.

29. Admitted.

30. Wallace & Pittman admits that it sent a letter to the Bank dated June 21, 2012, which letter is in writing, speaks for itself, and is the best evidence of its contents. Wallace & Pittman further admits that the Bank closed the IOLTA Trust Account, operating account, and escrow account after receipt of the letter. Except as admitted, Wallace & Pittman denies the allegations of Paragraph 30.

31. Denied.

FIRST CLAIM
(Breach of Contract)

32. The allegations of the preceding paragraphs are incorporated herein as if set forth in full.

33. Wallace & Pittman admits the existence of the Treasury Management Products Agreement, which is in writing, speaks for itself and is the best evidence of its contents. Except as admitted, Wallace & Pittman denies the allegations of Paragraph 33.

34. Wallace & Pittman admits the existence of the Treasury Management Products Agreement, which is in writing, speaks for itself and is the best evidence of its contents. Except as admitted, Wallace & Pittman denies the allegations of Paragraph 34.

35. Admitted.

36. Denied.

37. Denied.

SECOND CLAIM
(Conversion)

38. The allegations of the preceding paragraphs are incorporated herein as if set forth in full.

39. Denied.

40. Denied.

FIRST AFFIRMATIVE DEFENSE

The Bank's claims are barred by its preceding, material breaches of contract.

SECOND AFFIRMATIVE DEFENSE

The Bank's claims are barred by its failure to maintain commercially reasonable security measures for its online banking services and/or its negligent maintenance or performance of any security measures that were in place on its online banking systems.

THIRD AFFIRMATIVE DEFENSE

The Bank's claims are barred by the public policy of North Carolina.

FOURTH AFFIRMATIVE DEFENSE

The Bank's claims are barred because of its failure to comply with standards and guidelines set forth by the Federal Deposit Insurance Corporation ("FDIC") and the Federal Financial Institution Examination Council ("FFIEC").

FIFTH AFFIRMATIVE DEFENSE

The Bank's claims are barred by its preceding breaches of fiduciary duty.

SIXTH AFFIRMATIVE DEFENSE

The Bank's claims are barred by its failure to mitigate damages.

SEVENTH AFFIRMATIVE DEFENSE

The Bank's claims are barred by the equitable doctrines of unclean hands, waiver, and/or estoppel.

COUNTERCLAIMS

Complaining of Plaintiff/Counterclaim Park Sterling Bank (the "Bank"), Defendant/Counterclaim Plaintiff Wallace & Pittman, PLLC ("Wallace & Pittman") states as follows:

BACKGROUND

41. Wallace & Pittman is a law firm that provides, among other things, real estate services to clients.

42. In connection with its law practice, Wallace & Pittman maintains an IOLTA Trust Account with the Bank (the "Trust Account").

43. The Trust Account was established and maintained in order to segregate funds entrusted to the lawyers that work for Wallace & Pittman, in accordance with Rule 1.15 of the North Carolina State Bar's Rules of Professional Conduct.

44. The Trust Account is solely comprised of "trust funds" and "fiduciary funds" as defined in Rule 1.15 and, as such, the funds belong to persons other than Wallace & Pittman, including, without limitation, clients of Wallace & Pittman and other persons depositing funds in connection with real estate closings.

45. All funds in the Trust Account are held by Wallace & Pittman in trust for the benefit of those parties depositing the funds, and Wallace & Pittman only has the authority to use those funds as authorized by the depositing parties and in a representative capacity.

46. At all relevant times, the Bank was aware of the nature of the Trust Account and that the funds deposited therein by Wallace & Pittman were held by Wallace & Pittman solely in a representative capacity.

47. Wallace & Pittman used online banking services provided by the Bank in furtherance of Wallace & Pittman's provision of real estate services to its clients.

48. The online banking services provided by the Bank to Wallace & Pittman included the ability for the user to generate online wire transfer requests to wire funds from the Trust Account to third-party accounts in connection with Wallace & Pittman's provision of real estate services to its clients.

49. At all relevant times the Bank held out its online banking services for wire transfers as being as secure or substantially as secure as those of similarly situated financial institutions.

50. The Bank held out its online banking services for wire transfers as being as safe or substantially as safe as those of similarly situated size despite the fact that, upon

information and belief, the Bank's online banking services for wire transfers were significantly less secure than those of similarly situated financial institutions.

THE FALSE WIRE TRANSFER

51. At 10:09 AM, EDT, on May 5, 2012, Wallace & Pittman initiated a wire transfer with the Bank in the amount of $386,600.61 for the benefit of a client of Wallace & Pittman, in connection with a real estate closing. This wire went to a beneficiary bank located in Virginia Beach, Virginia.

52. At 2:58 PM, EDT, on May 5, 2012, unbeknownst to Wallace & Pittman, a "malware" program that had infected Wallace & Pittman's computer system caused another wire transfer request to be delivered to the Bank (the "False Wire Transfer").

53. As shown on the Outgoing Wire Notice attached hereto as **Exhibit A**, the beneficiary of the False Wire Transfer was an account in Moscow, Russia.

54. The False Wire Transfer was for $336,600.61 (exactly $50,000 less than the legitimate wire sent earlier that day).

55. The False Wire Transfer was not authorized by Wallace & Pittman or its agents.

56. Upon information and belief, the False Wire Transfer originated from a computer whose identifying information including IP address indicated that it was not in the offices of Wallace & Pittman in Charlotte, North Carolina.

57. Despite the obvious suspicious nature of the wire request, the Bank processed the False Wire Transfer without contacting Wallace & Pittman to confirm if the request was legitimate.

58. Upon information and belief, the Bank's processing of an international wire transfer without contacting its client to verify the validity of such international wire transfer request was contrary to the procedures of similarly situated financial institutions when processing wire transfer requests.

59. Upon information and belief, the Bank knew or should have known that the False Wire Transfer request was illegitimate because malware or fraudulent wire transfer schemes are a common occurrence involving banks and trust accounts, and Russia is known as a source of such schemes.

60. The Bank was aware or should have been aware of various schemes involving fraudulent fund transfers, particularly those involving parties located in Russia.

61. The Bank knew the nature of Wallace & Pittman's law practice and should have questioned the legitimacy of an international wire transfer.

62. Wallace & Pittman had never before wired funds from the Trust Account to Russia or to any other location outside the United States.

63. Upon information and belief, an employee of the Bank was required to manually type information into the Bank's wire transfer system in order to complete wire transfers.

64. Upon information and belief, the same Bank employee manually typed information for both the valid wire transfer request from Wallace & Pittman at 10:09 AM, EDT, on May 5, 2012 and the False Wire Transfer into the Bank's wire transfer system.

65. Upon information and belief, an employee of the Bank manually typed information into the Bank's wire transfer system that clearly indicated the suspicious

nature of the False Wire transfer, including the location of the account in Moscow, Russia.

66. Upon information and belief, an employee of the Bank manually typed information into the Bank's wire transfer system that clearly indicated the suspicious nature of the False Wire transfer, including the fact that the False Wire Transfer was for exactly $50,000 less than the valid wire transfer request from Wallace & Pittman at 10:09 AM, EDT, on May 5, 2012.The Bank should have noticed the suspicious nature of a request involving both a wire transfer to Russia and an amount exactly $50,000 less than the legitimate wire sent earlier that day.

67. Upon information and belief, this employee proceeded with processing the False Wire Transfer using the Bank's ordinary procedures, despite the unusual nature of the False Wire Transfer.

68. At the time of the transfer, the Bank had actual notice that false and fraudulent online banking transfers were often for the benefit of accounts in Russia.

69. Despite having actual notice that false and fraudulent online banking transfers were often for the benefit of accounts in Russia, the Bank processed the False Wire Transfer.

70. The Bank did not contact Wallace & Pittman regarding the False Wire Transfer prior to processing it.The Bank did nothing to try to stop the False Wire Transfer until Wallace & Pittman saw the wire confirmation generated by the Bank later that day.

71. Immediately after receiving the False Wire Transfer confirmation, Wallace & Pittman contacted the Bank and informed it of the fraudulent request.

72. An employee of the Bank told Judith Roberts, an employee of Wallace & Pittman, that the False Wire Transfer should never have been processed. Upon information and belief, the Bank did not act with due speed to reverse to False Wire Transfer.

73. Upon information and belief, the Bank unreasonably delayed its attempts to reverse the False Wire Transfer.

74. Upon information and belief, when the Bank attempted to reverse the False Wire Transfer, it was unsuccessful.

75. Later that day, the Bank returned the $336,600.61 to the Trust Account.

76. On the online transaction ledger for the Trust Account (attached hereto as **Exhibit B**), the return of the $336,600.61 is classified as "Reverse previous wire entry."

77. At no time prior to the return of the funds to the Trust Account did the Bank state that it was providing Wallace & Pittman with "provisional credit" in the amount of the Fraudulent Wire Transfer.

78. The Bank did not call the return of the funds to the Trust Account "provisional credit" during a meeting between representatives of Wallace & Pittman and the Bank on May 18, 2012 to discuss the False Wire Transfer.

79. Although the Bank indicated its desire that Wallace & Pittman provide $336,600.61 to the Bank at the May 18 meeting, the Bank did not inform Wallace & Pittman that it intended to debit the amount of the False Wire Transfer from the Trust Account during that meeting.

80. Upon information and belief, at some point after the return of the funds and after the May 18 meeting the Bank decided to attempt to re-characterize the return of

the funds to the Trust Account as the Bank providing "provisional credit" to Wallace & Pittman.

81. The attempted re-characterization of the return of the funds to the Trust Account as provisional credit first appeared in an undated letter from Nancy J. Foster, Chief Risk Officer for the Bank to Wallace & Pittman, which letter is attached hereto as **Exhibit C** (the "Debit Notice").

82. Wallace & Pittman received the Debit Notice on via Federal Express on the morning of Tuesday, May 29, 2012, the day after Memorial Day.

83. In the Debit Notice, the Bank informed Wallace & Pittman that it would be debiting the Trust Account in the amount of the False Wire Transfer on May 31, 2012, only two business days after the date Wallace & Pittman received the Debit Notice via Federal Express.

84. The Bank had no legal or contractual right to re-characterize the return of the funds to the Trust Account as "provisional credit."

85. The Bank was aware that Wallace & Pittman held the funds in the Trust Account solely in a representative capacity and had no ownership rights therein.

86. Upon information and belief, the Bank's attempt to re-characterize the return of the funds as "provisional credit" was because the Bank has no contractual or other right of setoff in the Trust Account because the funds in the Trust Account are held solely in a representative capacity.

87. The Bank had no contractual or other right to setoff any obligation of Wallace & Pittman against funds held solely for the benefit of the clients of Wallace & Pittman.

88. The Bank was aware or should have been aware of the North Carolina Rules of Professional Conduct governing Wallace & Pittman's safekeeping of trust and fiduciary funds such as those deposited in the Trust Account.

89. The Bank was aware or should have been aware of the potential for serious professional sanctions against Wallace & Pittman in the event that the Bank drained the Trust Account.

90. As a result of the Bank's actions in attempting to re-characterize the return of the funds as "provisional credit" and in threatening to drain the Trust Account of $336,600.61 on two days notice, Wallace & Pittman was forced to retain counsel and file an action in this Court in order to seek injunctive relief to protect the funds in its Trust Account and to prevent irreparable harm to its law practice and its clients

91. Subsequently, and with full knowledge of the Bank, Wallace & Pittman removed all funds from the Trust Account and moved all its accounts from the Bank to another financial institution.

92. As a result, the Bank then filed its complaint against Wallace & Pittman seeking to recover from Wallace & Pittman the $336,600.61 that the Bank had erroneously transferred to Russia.

FAILURES BY THE BANK LEADING UP TO THE FALSE WIRE TRANSFER

93. Prior to Wallace & Pittman's use of the online banking services provided by the Bank, Wallace & Pittman received training from the Bank at Wallace & Pittman's office on the operation of the online banking system, including without limitation how to generate online wire transfer requests (the "Training").

94. At no point in the Training or thereafter did the Bank inform Wallace & Pittman of the possibility that the Trust Account could be taken over and drained by fraudsters.

95. At no point in the Training or thereafter did the Bank provide Wallace & Pittman with a Cash Management User Manual as alleged in the Complaint.

96. At no point in the Training or thereafter did the Bank inform Wallace & Pittman of the risks of phishing attacks.

97. At no point in the Training or thereafter did the Bank inform Wallace & Pittman of additional security measures Wallace & Pittman could take to avoid phishing attacks (such as, *e.g.*, having a computer dedicated solely to online banking, use of key fobs with changing log-in information and 2 person authentication of wire transfer requests).

98. The Bank failed to inform Wallace & Pittman of these risks or of possible means to avoid such risks despite knowing of the nature of the Trust Account and that the funds therein were held by Wallace & Pittman solely in a representative capacity.

99. After the Training, Wallace & Pittman regularly generated online wire transfer requests from the Trust Account.

100. Such requests were generated by visiting the Bank's web site at www.parksterlingbank.com. After entering in an "online banking i.d.," the user would enter information regarding the specific wire transfer request, and enter a four-number "wire code" that, upon information and belief, is never changed.

101. After the wire transfer request is initially submitted by the user, the system generates two challenge questions.

102. The two challenge questions never change.

103. The answers to both challenge questions were pre-programmed by the Bank to the same common and intuitive four-letter word.

104. This pre-programmed answer is in no way responsive to either challenge question, but rather, relates to the Bank itself.

105. Upon information and belief, the Bank has pre-programmed the answers to the challenge questions to this same common and intuitive four-letter word for many of its online banking customers.

106. The procedure for operating online wire transfer requests does not provide layered security controls or minimum effect controls to ensure that fraudulent wire transfer requests, such as the False Wire Transfer, are not processed by the Bank.

107. At no point during the Training did the Bank instruct Wallace & Pittman that it could change the challenge questions or the pre-programmed answers to those questions.

108. At no point during the Training did the Bank instruct Wallace & Pittman on how to change the challenge questions or the pre-programmed answers to those questions.

109. The Bank did not inform Wallace & Pittman that the pre-programmed challenge questions and answers did not provide a reasonable level of security to Wallace & Pittman.

110. At no point prior to the False Wire Transfer did the Bank inform or warn Wallace & Pittman of the dangers of phishing attacks and fraudulent banking transactions despite clear regulatory requirements and guidance that it should do so.

111. At no point prior to the False Wire Transfer did the Bank inform or warn Wallace & Pittman of the dangers of phishing attacks and fraudulent banking transactions despite knowing of the entrusted and fiduciary nature of the funds held in the Trust Account.

112. At no point prior to the False Wire Transfer did the Bank inform or warn Wallace & Pittman of the dangers of phishing attacks and fraudulent banking transactions despite knowing of the serious professional sanctions Wallace & Pittman could face if the Trust Account were drained.

THE MALWARE

113. Upon information and belief, the malware used to generate the False Wire Transfer may have infected Wallace & Pittman's computer by way of an email appearing to have originated from the National Automated Clearing House Association ("NACHA").

114. NACHA has previously issued warnings to banks regarding the fact that fraudulent emails appearing to originate from NACHA were being used in phishing attacks. Upon information and belief, the Bank received these warnings from NACHA.

115. The FBI's web site describes the phishing scheme as follows:

> Typically, you receive an unsolicited e-mail from NACHA, the Federal Reserve, or the FDIC telling you that there's a problem with your bank account or a recent ACH transaction. (ACH stands for Automated Clearing House, a network for a wide variety of financial transactions in the U.S.) The sender has included a link in the e-mail for you that will supposedly help you resolve whatever the issue is. Unfortunately, the link goes to a phony website, and once you're there, you inadvertently download the Gameover malware, which promptly infects your computer and steals your banking information.

See Malware Targets Bank accounts: "Gameover Delivered Via Phishing Emails, *at* http://www.fbi.gov/news/stories/january/malware_010612/malware_010612 (attached hereto as **Exhibit D**).

116. Prior to the date of the False Wire Transfer, Wallace & Pittman received a series of emails that appeared to originate with NACHA and to call into question ACH transfers made by Wallace & Pittman.

117. As a result, Wallace & Pittman contacted the Bank to discuss possible issues with its ACH transfers.

118. Although the Bank informed Wallace & Pittman that the NACHA emails were not legitimate, the Bank did not inform Wallace & Pittman of the specific dangers associated with the fraudulent NACHA email scheme, or the possibility that Wallace & Pittman's computer could have been infected with malware that could generate fraudulent banking transactions like the False Wire Transfer.

119. Despite being aware that Wallace & Pittman had received the fraudulent NACHA emails, the Bank did not suggest any additional security measures to Wallace & Pittman or undertake to institute additional security measures on the Trust Account.

THE BANK'S FAILURE TO COMPLY WITH REGULATORY GUIDANCE

120. Upon information and belief, at the time of the False Wire Transfer, the Bank's security measures for its online banking services were outdated, inadequate, unsafe, unsound, negligence and commercially unreasonable based upon requirements and guidance from the Federal Financial Institutions Examination Council (the "FFIEC") and the Federal Deposit Insurance Corporation (the "FDIC").

121. The FFIEC is comprised of regulatory agencies including the FDIC, which regulates the Bank.

122. The FFIEC is empowered to prescribe uniform principles and standards for the federal examination of financial institutions including the Bank.

123. As an FDIC-insured financial institution, the Bank receives periodic guidance and regulatory standards from the FFIEC and FDIC.

124. Upon information and belief, the Bank received and/or was aware of the "Supplement to Authentication in and Internet Banking Environment" issued by the FFIEC on June 28, 2011 (the "FFIEC 2011 Guidance"). A true and correct copy of the FFIEC Guidance is attached hereto as **Exhibit E.**

125. The FFIEC 2011 Guidance "identified minimum control expectations for certain online banking activities and identifies controls that are less effective in the current environment."

126. The FFIEC 2011 Guidance also "identifies certain minimum elements that should be part of an institution's customer awareness and education program."

127. The FFIEC 2011 Guidance was the subject of an FDIC Financial Institution Letter, FIL-50-2011 that was disseminated to all FDIC-insured institutions on or about June 29, 2011.

128. FIL-50-2011 is attached hereto as **Exhibit F.**

129. Pursuant to FIL-50-2011, "Financial institutions will be expected to comply with the [FFIEC 2011 Guidance] no later than January 1, 2012."

130. The Bank had actual notice of FIL-50-2011 and the FFIEC Guidance prior to the date of the False Wire Transfer.

131. Thus, the FDIC required the Bank to comply with the FFIEC 2011 Guidance more than four months prior to the date of the False Wire Transfer.

132. At the time of the False Wire Transfer, the Bank did not comply with the FFIEC 2011 Guidance because, *inter alia*, it did not institute minimum effective controls for its online banking services.

133. At the time of the False Wire Transfer, the Bank did not comply with the FFIEC 2011 Guidance because, *inter alia*, it did not provide layered security controls consistent with the increased level of risk posed by business accounts.

134. At the time of the False Wire Transfer, the Bank did not comply with the FFIEC 2011 Guidance because, *inter alia*, it did not provide any customer awareness or education programs to Wallace & Pittman or, upon information and belief, its other online business banking customers.

135. Upon information and belief, at the time of the False Wire Transfer, the Bank did not comply with other relevant regulatory requirements and guidance, including without limitation the following:

a. The FFIEC's 2005 "Authentication in an Internet Banking Environment;"

b. The FFIEC's 2006 Frequently Asked Questions issued to help financial institutions understand the FFIEC 2005 Guidance;

c. The FDIC's 2007 Financial Institutions Letter entitled "Supervisory Policy on Identity Theft (FIL-32-2007); and

d. The FDIC's August 2009 Special Alert (SA-147-2009) to all CEOs of FDIC-insured financial institutions including the Bank.

136. The Bank's failures to comply with the FFIEC 2011 Guidance were not commercially reasonable.

137. The Bank's failures to comply with other regulatory requirements and guidance from the FDIC and FFIEC were not commercially reasonable.

138. The Bank did not employ commercially reasonable security measures for the online banking services provided to Wallace & Pittman.

139. Because it wholly failed to comply with the FFIEC 2011 Guidance and other regulatory requirements and guidance from the FDIC and FFIEC, the Bank did not act in good faith in connection with its processing of the False Wire Transfer.

140. As a result of the Bank's failure to employ commercially reasonable security measures for the online banking services provided to Wallace & Pittman, the False Wire Transfer was not effective as a payment order of Wallace & Pittman under N.C. Gen. Stat. § 25-4A-202.

141. As a result of the Bank's failure to accept the False Wire Transfer in good faith, the False Wire Transfer was not effective as a payment order of Wallace & Pittman under N.C. Gen. Stat. § 25-4A-202.

142. As a result of these failures, Wallace & Pittman has no liability to the Bank for the False Wire Transfer.

THE BANK'S ATTEMPTS TO LIMIT LIABILITY IN CONTRAVENTION OF NORTH CAROLINA LAW & PUBLIC POLICY

143. Upon information and belief, the Bank did not employ commercially reasonable security measures for its online banking services because it contends that the contractual limitations of liability in its contracts with its online banking customers relieve it of the duty to comply with regulatory requirements and guidance.

144. Upon information and belief, the Bank provided no customer education whatsoever regarding the risks involved in use of its online banking services because it contends that the contractual limitations of liability in its contracts with its online banking customers relieve it of the duty to comply with regulatory requirements and guidance.

145. The Bank utilized contracts of adhesion for its online banking services, including the services provided to Wallace & Pittman.

146. On or about January 7, 2009, Wallace & Pittman entered into the Park Sterling Bank-Treasury Management Products Customer Agreement attached to the Complaint as Exhibit B (the "TMP Customer Agreement").

147. No representative of the Bank ever discussed the specific terms of the TMP Customer Agreement with Wallace & Pittman.

148. No representative of the Bank ever disclosed to Wallace & Pittman the Bank's position that the TMP Customer Agreement relieved the Bank from any obligation to comply with the regulatory requirements and guidance issued by the FDIC and FFIEC relating to the security of its online banking services.

149. Upon information and belief, the contractual limitations of liability in the Bank's contracts for online banking services violate the public policy of the State of North Carolina in that they purport to relieve the Bank from the duty to use due care in the provision of online banking services.

150. The contractual limitations of liability in the TMP Customer Agreement violate the public policy of the State of North Carolina in that they purport to relieve the Bank from the duty to use due care in the provision of online banking services.

151. The contractual limitations in the Bank's contracts for online banking services do not relieve the Bank from the duty to use due care in the provision of online banking duties.

152. The contractual limitations in the TMP Customer Agreement do not relieve the Bank from the duty to use due care in the provision of online banking duties.

153. The contractual limitations in the Bank's contracts for online banking services do not relieve the Bank from the duty to comply with regulatory requirements and guidance from the FDIC and FFIEC.

154. The contractual limitations in the TMP Customer Agreement do not relieve the Bank from the duty to comply with regulatory requirements and guidance from the FDIC and FFIEC.

155. Customers of the Bank are entitled to rely on the Bank's compliance with regulatory requirements and guidance from the FDIC and FFIEC.

156. Wallace & Pittman was entitled to rely on the Bank's compliance with regulatory requirements and guidance from the FDIC and FFIEC.

CLAIM I
(Breach of Fiduciary Duty)

157. The allegations of the preceding paragraphs are incorporated herein as if set forth in full.

158. By, among other things, maintaining the Trust Account for the benefit of Wallace & Pittman and acting as Wallace & Pittman's agent in processing wire transfers, the Bank owes fiduciary duties to Wallace & Pittman to act in Wallace & Pittman's best interest, in good faith, and with due care.

159. The above referenced actions of the Bank constitute breaches of the Bank's fiduciary duties of care and loyalty to Wallace & Pittman, including without limitation the following:

a. The attempted re-characterization of the return of the $336,600.61 to the Trust Account as "provisional credit" in order to circumvent the Bank's contractual inability to setoff alleged obligations of Wallace & Pittman against funds held by Wallace & Pittman solely in a representative capacity;

b. The Bank's threats to drain the $336,600.61 from the Trust Account despite the Bank's knowledge that funds in the Trust Account were held solely in a representative capacity;

c. The Bank's threats to drain the $336,600.61 from the Trust Account despite the Bank's knowledge of the serious professional sanctions Wallace & Pittman would face were the Bank to do so;

d. The Bank's failures to comply with regulatory requirements and guidance from the FDIC and FFIEC in not maintaining commercially reasonable security measures for its online banking services;

e. The Bank's failures to comply with regulatory requirements and guidance from the FDIC and FFIEC in providing no customer education regarding the risks inherent in the use of online banking services;

f. The Bank's failure to suggest additional security measures to Wallace & Pittman or to institute additional security measures on the Trust Account upon being notified by Wallace & Pittman that it had received the fraudulent NACHA emails; and

g. The Bank's use of contractual limitations of liability in an effort to relieve itself of any duty to its to comply with regulatory requirements and guidance from the FDIC and FFIEC.

160. As a direct and proximate result of the actions of the Bank in violation of its fiduciary duties of care and loyalty to Wallace & Pittman, the Bank profited at Wallace & Pittman's expense.

161. As a direct and proximate result of the actions of the Bank in violation of its fiduciary duties of care and loyalty to Wallace & Pittman, Wallace & Pittman sustained damages in an amount to be proven at trial, which Wallace & Pittman is entitled to recover from the Bank.

CLAIM II
(Unfair and Deceptive Trade Practices--N.C. Gen. Stat. § 75-1.1)

1. The allegations of the preceding paragraphs are incorporated herein as if set forth in full.

2. The actions of the Bank were in commerce or affected commerce.

3. The above referenced actions of the Bank constitute unfair and deceptive trade practices in violation of Chapter 75 of the North Carolina General Statutes, including without limitation the following:

a. The attempted re-characterization of the return of the $336,600.61 to the Trust Account as "provisional credit" in order to circumvent the Bank's contractual inability to setoff alleged obligations of Wallace & Pittman against funds held by Wallace & Pittman solely in a representative capacity;

b. The Bank's threats to drain the $336,600.61 from the Trust Account despite the Bank's knowledge that funds in the Trust Account were held solely in a representative capacity;

c. The Bank's threats to drain the $336,600.61 from the Trust Account despite the Bank's knowledge of the serious professional sanctions Wallace & Pittman would face were the Bank to do so;

d. The Bank's failures to comply with regulatory requirements and guidance from the FDIC and FFIEC in not maintaining commercially reasonable security measures for its online banking services;

e. The Bank's failures to comply with regulatory requirements and guidance from the FDIC and FFIEC in providing no customer education regarding the risks inherent in the use of online banking services;

f. The Bank's failure to suggest additional security measures to Wallace & Pittman or to institute additional security measures on the Trust Account upon being notified by Wallace & Pittman that it had received the fraudulent NACHA emails; and

g. The Bank's use of contractual limitations of liability in an effort to relieve itself of any duty to comply with regulatory requirements and guidance from the FDIC and FFIEC.

4. As a direct and proximate result of the actions of the Bank for its own benefit, Wallace & Pittman sustained damages in an amount to be proven at trial, which Wallace & Pittman is entitled to recover from the Bank.

5. Pursuant to N.C.G.S. §75-16, Wallace & Pittman is entitled to recover from the Bank treble its compensatory damages.

6. Pursuant to N.C.G.S. §75-16.1, Wallace & Pittman is entitled to recover from the Bank its reasonable attorneys' fees.

CLAIM III
(Punitive Damages)

162. The allegations of the preceding paragraphs are incorporated herein as if set forth in full.

163. The above referenced actions of the Bank were willful and wanton, including without limitation the following:

a. The attempted re-characterization of the return of the $336,600.61 to the Trust Account as "provisional credit" in order to circumvent the Bank's contractual inability to setoff alleged obligations of Wallace & Pittman against funds held by Wallace & Pittman solely in a representative capacity;

b. The Bank's threats to drain the $336,600.61 from the Trust Account despite the Bank's knowledge that funds in the Trust Account were held solely in a representative capacity;

c. The Bank's threats to drain the $336,600.61 from the Trust Account despite the Bank's knowledge of the serious professional sanctions Wallace & Pittman would face were the Bank to do so;

d. The Bank's failures to comply with regulatory requirements and guidance from the FDIC and FFIEC in not maintaining commercially reasonable security measures for its online banking services;

e. The Bank's failures to comply with regulatory requirements and guidance from the FDIC and FFIEC in providing no customer education regarding the risks inherent in the use of online banking services;

f. The Bank's failure to suggest additional security measures to Wallace & Pittman or to institute additional security measures on the Trust Account upon being notified by Wallace & Pittman that it had received the fraudulent NACHA emails; and

g. The Bank's use of contractual limitations of liability in an effort to relieve itself of any duty to its to comply with regulatory requirements and guidance from the FDIC and FFIEC.

164. Wallace & Pittman is entitled to recover punitive damages from the Bank pursuant to Chapter 1D of the North Carolina General Statutes.

WHEREFORE, Wallace & Pittman respectfully requests:

1) That the Bank's Complaint be dismissed with prejudice;

2) That the Bank have and recover nothing from Wallace & Pittman;

3) That the Court enter judgment in favor of Wallace & Pittman and against the Bank in an amount greater than $10,000 as may be proven at trial;

4) Trebling of its damages pursuant to Counterclaim No. II;

5) Its attorneys fees pursuant to Counterclaim No. II or as otherwise allowed by law;

6) For punitive damages pursuant to Counterclaim No. III;

7) Interest as allowed by law;

8) That all costs be taxed to Plaintiffs;

9) That these matters be tried before a jury; and

10) That the Court award such other and further relief as the Court deems just and proper.

This ___ day of September, 2012.

HAMILTON, STEPHENS,
STEELE, & MARTIN, PLLC

By: _____

George W. Sistrunk (NC Bar No. 25648)
Adrianne Huffman Chillemi (NC Bar No. 30714)
Attorneys for Wallace & Pittman, PLLC
201 South College Street, Suite 2020
Charlotte, North Carolina 28244-2020
Telephone: (704) 344-1117

EXHIBIT A

Judith Roberts

From: cbc@pcbb.com
Sent: Wednesday, May 09, 2012 3:13 PM
To: jroberts@wallaceandpittman.com
Subject: New OUTGOING wire notice.

PARK STERLING BANK

1043 East Morehead Street, Suite 201 • Charlotte, NC 28204

OUTGOING WIRE NOTICE

Received Date	05/09/2012 02:58 PM EDT
Amount	336,600.61
Identifying Account	053012728
Business Function	CTR

Beneficiary
DXXXXX8618 VTB 24 MOSCOW RUSSIA

Originator
DXXX9281 WALLACE & PITTMAN PLLC 6230 FAIRVIEW RD STE 270 CHARLOTTE NC XXXXX0000

Delivery Instructions	
Sender DI	121042484PAC COS BKRS BK SF*
Receiver DI	021000021JPMCHASE*
Correspondent Service Provider	Pacific Coast Bankers' Bank, San Francisco, CA

Additional Information	
IMAD	20120509L1B7832F000449
OMAD	0509B1QGC01R038808050914587T03
Originator to Beneficiary Info	FOR FURTHER CREDIT TO ACC:*XXXXXXXXXXX6418*KONSTANTIN POMOGALOV, INVOICE SALAR*
FI to FI Info	
Beneficiary's Adv Info	
Beneficiary's FI	
Beneficiary's FI Info	
Originator's FI	FXXXXX2728*Park Sterling Bank*
Instructing FI	
Intermediary FI	
Receiver's FI	
Sender Reference	
Ref for Beneficiary	
Info to Beneficiary	

EXHIBIT B

PARK STERLING BANK

To change the number of transactions you see by default select Options and then Display.

View Transactions for: WP IOLTA 9281

Current Balance: $1,048,224.10
Available Balance: $1,048,224.10

Transactions from 05/09/2012 to 05/09/2012

Disable Offers

View Range: Since Last Statement | 7 Days | 15 Days | 30 Days | All

Date:	Ref/Check No:	Description:	Debit:	Credit:	Balance
05/09/2012	14222	Check 14222	-$238,219.85		$103,687.22
05/09/2012	14218	Check 14218	-$3,780.00		$341,907.07
05/09/2012	14195	Check 14195	-$65.00		$345,687.07
05/09/2012	14184	Check 14184	-$35.00		$345,752.07
05/09/2012	14176	Check 14176	-$35.00		$345,787.07
05/09/2012	14164	Check 14164	-$1,700.00		$345,822.07
05/09/2012	14163	Check 14163	-$65.00		$347,522.07
05/09/2012	14157	Check 14157	-$1,101.00		$347,587.07
05/09/2012	14148	Check 14148	-$65.00		$348,688.07
05/09/2012	14138	Check 14138	-$50.00		$348,753.07
05/09/2012	14132	Check 14132	-$65.00		$348,803.07
05/09/2012	14123	Check 14123	-$50.00		$348,868.07
05/09/2012	14121	Check 14121	-$216.06		$348,918.07
05/09/2012	14111	Check 14111	-$399.00		$349,134.13
05/09/2012	14097	Check 14097	-$50.00		$349,533.13
05/09/2012	14093	Check 14093	-$15.00		$349,583.13
05/09/2012	14083	Check 14083	-$75.00		$349,598.13
05/09/2012	14241	Check 14241	-$4,020.00		$349,673.13
05/09/2012	14226	Check 14226	-$14,925.00		$353,693.13
05/09/2012		Wire Transfer Debit	-$386,600.61		$368,618.13

	NEW YORK, NY Fu		
05/09/2012	Wire Transfer Debit VTB 24 021000021 400938618 Moscow Russia JPMCHASE NEW YORK, NY For further credit to acc: 4272300005626418 Konstantin Pomogalov, invoice	-$336,600.61	$755,218.74
05/09/2012	Reverse previous entry for wir e	$336,600.61	$1,091,819.35
Totals (this page):	***Transactions: 22***	***Debits: -$988,132.13***	***Credits: $336,600.61***

Print Preview

StatementRewards

See rewards | What is this?

FDIC EQUAL HOUSING LENDER

EXHIBIT C

PARK STERLING
CORPORATION

James G. Wallace, Esq.
Wallace & Pittman, PLLC
6230 Fairview Road, Suite 270
Charlotte, NC 28210

Dear Mr. Wallace:

I am writing to follow up on the recent discussions between Park Sterling Bank (PSB) and your firm regarding the wire transfer order that PSB received and processed on May 9, 2012. We have appreciated the opportunity to discuss the matter with various personnel from your firm, including our meeting with you on May 18.

As you know, the wire transfer order (in the amount of $336,600.61) was received through our online cash management system, NetTeller, by someone who was able to access your account through means of the legitimate user name, password, pin number, and challenge question information for an authorized account user. We now understand from the firm that there appears to have been an intrusion on your firm's computers and that someone obtained all of that information through keylogger malware (such as Zeuz/Zbot) placed on one or more firm computers. We also understand that someone apparently used that information to access a firm account and place the wire order, and in so doing appeared to be acting from a computer with the same internet protocol address used by your firm to place wire transfer orders on other occasions. We understand as well that your firm's IT personnel first detected the malware on the firm's computer(s) several days after PSB had received and processed the suspicious wire transfer order.

Once notified of the suspicious transfer, PSB personnel moved quickly to attempt to reverse the transfer, but as we have previously notified you, the attempt was unsuccessful. (We do note that PSB blocked a second attempted suspicious wire transfer order regarding your account that was received later on May 9.) The funds in question were sent to the beneficiary bank, JP Morgan Chase, and then presumably on to the beneficiary. Although the funds were paid out from your account on May 9, PSB agreed to provide provisional credit in order to avoid an overdraft to your IOLTA account and allow some time for possible return of wire transfer proceeds.

We have now determined that the funds will not be recovered and that with respect to the wire transfer order, PSB has acted in accordance with the Treasury Management Products Customer Agreement (dated January 7, 2009) and other applicable standards. We will therefore be debiting the amount of the wire transfer against your account (no. 1009281) on May 31, 2012.

This is an unfortunate situation, and it is regrettable that someone appears to have gained access to your account through an intrusion on your computer system. We ask that you preserve all computer forensic information relating to the malware and the intrusion and share with us any information or analysis you receive relating to the intrusion or the wire transfer order.

If our understanding of the nature of the intrusion is in error, please let us know. In addition, if you would like to discuss the timing of the planned debit or need to address cash flow concerns in that regard, please let us know as soon as possible.

Sincerely,

Nancy J. Foster
Chief Risk Officer

Cc: Bryan Kennedy, President, Park Sterling Bank
Charlie Stewart, Senior Vice President, Park Sterling Bank

EXHIBIT D

FBI

Stories

Home • News • Stories • 2012 • January • 'Gameover' Malware Targets Bank Accounts

Malware Targets Bank Accounts

'Gameover' Delivered Via Phishing E-Mails

01/06/12

Cyber criminals have found yet another way to steal your hard-earned money: a recent phishing scheme involves spam e-mails—purportedly from the National Automated Clearing House Association (NACHA), the Federal Reserve Bank, or the Federal Deposit Insurance Corporation (FDIC)—that can infect recipients' computers with malware and allow access to their bank accounts.

The malware is appropriately called "Gameover" because once it's on your computer, it can steal usernames and passwords and defeat common methods of user authentication employed by financial institutions. And once the crooks get into your bank account, it's definitely "game over."

Gameover is a newer variant of the Zeus malware, which was created several years ago and specifically targeted banking information.

How the scheme works: Typically, you receive an unsolicited e-mail from NACHA, the Federal Reserve, or the FDIC telling you that there's a problem with your bank account or a recent ACH transaction. (ACH stands for Automated Clearing House, a network for a wide variety of financial transactions in the U.S.) The sender has included a link in the e-mail for you that will supposedly help you resolve whatever the issue is. Unfortunately, the link goes to a phony website, and once you're there, you inadvertently download the Gameover malware, which promptly infects your computer and steals your banking information.

How Can You Protect Yourself?

- Obviously, make sure your computer's anti-virus software is up to date.
- Don't click on e-mail attachments from unsolicited senders, NACHA, FDIC, and the Federal Reserve all say they don't send out unsolicited e-mails to bank account holders. If you want to confirm there's a problem with your account or one of your recent transactions, contact your financial institution directly.
- Don't accept unsolicited jobs online that require you to receive funds from prospective bank accounts and then wire the money to overseas accounts—you could get caught up in a criminal investigation.

After the perpetrators access your account, they conduct what's called a distributed denial of service, or DDoS, attack using a botnet, which involves multiple computers flooding the financial institution's server with traffic in an effort to deny legitimate users access to the site—probably in an attempt to deflect attention from what the bad guys are doing.

But that's not the end of the scheme: Recent investigations have shown that some of the funds stolen from bank accounts go towards the purchase of precious stones and expensive watches from high-end jewelry stores. The criminals contact these jewelry stores, tell them what they'd like to buy, and promise they will wire the money the next day. So the next day, a person involved in the money laundering aspect of the crime—called a "money mule"—comes into the store to pick up the merchandise. After verifying that the money is in the store's account, the jewelry is turned over to the mule, who then gives the items to the organizers of the scheme or converts them for cash and uses money transfer services to launder the funds.

In many cases, these money mules are willing participants in the criminal scheme. But increasingly, as part of the scheme, we see an increasing number of unsuspecting mules hired via "work at home" advertisements who end up laundering some of the funds stolen from bank accounts. The criminals e-mail prospective candidates claiming to have seen their resumes on job websites and offer them a job. The hired employees are provided long and seemingly legitimate work contracts and actual websites to log into. They're instructed to either open a bank account or use their own bank account in order to receive funds via wire and ACH transactions from overseas banks... and then use money remitting services to send the money overseas.

If you think you've been victimized by this type of scheme, contact your financial institution to report it, and file a complaint with the FBI's Internet Crime Complaint Center.

Resources:
- Scams & Safety

Story Index

By Date

By Subject
- Art Theft
- Civil Rights
- Counterterrorism
- Crimes Against Children
- Criminal Justice Information Services
- Cyber Crimes
- Director/FBI Leadership
- Field Cases
- Foreign Counterintelligence
- General
- History
- Intelligence
- International
- Lab/Operational Technology
- Linguist/Translation Program
- Major Thefts/Violent Crime
- Organized Crime/Drugs
- Partnerships
- Public/Community Outreach
- Public Corruption
- Recruiting/Diversity
- Responding to Your Concerns
- Technology
- Training
- White-Collar Crime

- FBI Cyber Division

Close

EXHIBIT E

Federal Financial Institutions Examination Council

3501 Fairfax Drive • Room B7081a • Arlington, VA 22226-3550 • (703) 516-5588 • FAX (703) 562-6446 • http://www.ffiec.gov

Supplement to Authentication in an Internet Banking Environment

Purpose

On October 12, 2005, the FFIEC agencies[1] (Agencies) issued guidance entitled *Authentication in an Internet Banking Environment* (2005 Guidance or Guidance).[2] The 2005 Guidance provided a risk management framework for financial institutions offering Internet-based products and services to their customers. It stated that institutions should use effective methods to authenticate the identity of customers and that the techniques employed should be commensurate with the risks associated with the products and services offered and the protection of sensitive customer information. The Guidance provided minimum supervisory expectations for effective authentication controls applicable to high-risk online transactions involving access to customer information or the movement of funds to other parties. The 2005 Guidance also provided that institutions should perform periodic risk assessments and adjust their control mechanisms as appropriate in response to changing internal and external threats.

The purpose of this Supplement to the 2005 Guidance (Supplement) is to reinforce the Guidance's risk management framework and update the Agencies' expectations regarding customer authentication, layered security, or other controls in the increasingly hostile online environment. The Supplement reiterates and reinforces the expectations described in the 2005 Guidance that financial institutions should perform periodic risk assessments considering new and evolving threats to online accounts and adjust their customer authentication, layered security, and other controls as appropriate in response to identified risks. It establishes minimum control expectations for certain online banking activities and identifies controls that are less effective in the current environment. It also identifies certain specific minimum elements that should be part of an institution's customer awareness and education program.

---

[1] Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision.

[2] FRS SR Letter 05-19, October 13, 2005; FDIC Financial Institution Letter 103-2005, October 12, 2005; NCUA Letter to Credit Unions 05-CU-18, November 2005; OCC Bulletin 2005-35, October 2005; OTS CEO Memorandum 228, October 12, 2005.

Background

Since 2005, there have been significant changes in the threat landscape. Fraudsters have continued to develop and deploy more sophisticated, effective, and malicious methods to compromise authentication mechanisms and gain unauthorized access to customers' online accounts. Rapidly growing organized criminal groups have become more specialized in financial fraud and have been successful in compromising an increasing array of controls. Various complicated types of attack tools have been developed and automated into downloadable kits, increasing availability and permitting their use by less experienced fraudsters. Rootkit-based malware surreptitiously installed on a personal computer (PC) can monitor a customer's activities and facilitate the theft and misuse of their login credentials. Such malware can compromise some of the most robust online authentication techniques, including some forms of multi-factor authentication. Cyber crime complaints have risen substantially each year since 2005, particularly with respect to commercial accounts. Fraudsters are responsible for losses of hundreds of millions of dollars resulting from online account takeovers and unauthorized funds transfers.[3]

The Agencies are concerned that customer authentication methods and controls implemented in conformance with the Guidance several years ago have become less effective. Hence, the institution and its customers may face significant risk where periodic risk assessments and appropriate control enhancements have not routinely occurred.

General Supervisory Expectations

The concept of customer authentication, as described in the 2005 Guidance, is broad. It includes more than the initial authentication of the customer when he/she connects to the financial institution at login. Since virtually every authentication technique can be compromised, financial institutions should not rely solely on any single control for authorizing high risk transactions, but rather institute a system of layered security, as described herein.

[3] See IC3 Annual Internet Crime Reports 2005-2009.

Specific Supervisory Expectations

Risk Assessments

The Agencies reiterate and stress the expectation described in the 2005 Guidance that financial institutions should perform periodic risk assessments and adjust their customer authentication controls as appropriate in response to new threats to customers' online accounts. Financial institutions should review and update their existing risk assessments as new information becomes available, prior to implementing new electronic financial services, or at least every twelve months.[4] Updated risk assessments should consider, but not be limited to, the following factors:

- changes in the internal and external threat environment, including those discussed in the Appendix to this Supplement;
- changes in the customer base adopting electronic banking;
- changes in the customer functionality offered through electronic banking; and
- actual incidents of security breaches, identity theft, or fraud experienced by the institution or industry.

Customer Authentication for High-Risk Transactions

The 2005 Guidance's definition of "high-risk transactions" remains unchanged, i.e., electronic transactions involving access to customer information or the movement of funds to other parties. However, since 2005, more customers (both consumers and businesses) are conducting online transactions. The Agencies believe that it is prudent to recognize and address the fact that not every online transaction poses the same level of risk. Therefore, financial institutions should implement more robust controls as the risk level of the transaction increases.

Retail/Consumer Banking

Online consumer transactions generally involve accessing account information, bill payment, intrabank funds transfers, and occasional interbank funds transfers or wire transfers. Since the frequency and dollar amounts of these transactions are generally lower than commercial transactions, they pose a comparatively lower level of risk. Financial institutions should implement layered security, as described herein, consistent with the risk for covered consumer transactions.

---

[4] See *FFIEC IT Examination Handbook*, Information Security Booklet, July 2006, Key Risk Assessment Practices section.

Business/Commercial Banking

Online business transactions generally involve ACH file origination and frequent interbank wire transfers. Since the frequency and dollar amounts of these transactions are generally higher than consumer transactions, they pose a comparatively increased level of risk to the institution and its customer. Financial institutions should implement layered security, as described herein, utilizing controls consistent with the increased level of risk for covered business transactions. Additionally, the Agencies recommend that institutions offer multifactor authentication to their business customers.

Layered Security Programs

Layered security is characterized by the use of different controls at different points in a transaction process so that a weakness in one control is generally compensated for by the strength of a different control. Layered security can substantially strengthen the overall security of Internet-based services and be effective in protecting sensitive customer information, preventing identity theft, and reducing account takeovers and the resulting financial losses. It should be noted that other regulations and guidelines also specifically address financial institutions' responsibilities to protect customer information and prevent identity theft.[5] Financial institutions should implement a layered approach to security for high-risk Internet-based systems.[6]

Effective controls that may be included in a layered security program include, but are not limited to:

- fraud detection and monitoring systems that include consideration of customer history and behavior and enable a timely and effective institution response;
- the use of dual customer authorization through different access devices;
- the use of out-of-band verification for transactions;
- the use of "positive pay," debit blocks, and other techniques to appropriately limit the transactional use of the account;

---

[5] See Interagency Final Regulation and Guidelines on Identity Theft Red Flags, 12 CFR parts 41, 222, 334, 571, and 717; Interagency Guidelines Establishing Information Security Standards, 12 CFR parts 30, 208, 225, 364, and 570, Appendix B.

[6] See *FFIEC IT Examination Handbook*, Information Security Booklet, July 2006, Key Concepts section.

- enhanced controls over account activities; such as transaction value thresholds, payment recipients, number of transactions allowed per day, and allowable payment windows (e.g., days and times);
- internet protocol (IP) reputation-based tools to block connection to banking servers from IP addresses known or suspected to be associated with fraudulent activities;
- policies and practices for addressing customer devices identified as potentially compromised and customers who may be facilitating fraud;
- enhanced control over changes to account maintenance activities performed by customers either online or through customer service channels; and
- enhanced customer education to increase awareness of the fraud risk and effective techniques customers can use to mitigate the risk.

The Agencies expect that an institution's layered security program will contain the following two elements, at a minimum.

Detect and Respond to Suspicious Activity

Layered security controls should include processes designed to detect anomalies and effectively respond to suspicious or anomalous activity related to:

- initial login and authentication of customers requesting access to the institution's electronic banking system; and
- initiation of electronic transactions involving the transfer of funds to other parties.

Based upon the incidents the Agencies have reviewed, manual or automated transaction monitoring or anomaly detection and response could have prevented many of the frauds since the ACH/wire transfers being originated by the fraudsters were anomalous when compared with the customer's established patterns of behavior.

Control of Administrative Functions

For business accounts, layered security should include enhanced controls for system administrators who are granted privileges to set up or change system configurations, such as setting access privileges and application configurations and/or limitations. These enhanced controls should exceed the controls applicable to routine business customer users. For example, a preventive control could include requiring an additional authentication routine or a transaction verification routine prior to final implementation of the access or application changes. An example of a detective control could include a transaction verification notice

immediately following implementation of the submitted access or application changes. As discussed in the Appendix, out-of-band authentication, verification, or alerting can be effective controls. Based upon the incidents the Agencies have reviewed, enhanced controls over administrative access and functions can effectively reduce money transfer fraud.

Effectiveness of Certain Authentication Techniques

Device Identification

In response to the 2005 Guidance, many financial institutions implemented simple device identification. This typically uses a cookie loaded on the customer's PC to confirm that it is the same PC that was enrolled by the customer and matches the logon ID and password that is being provided. However, experience has shown this type of cookie may be copied and moved to a fraudster's PC, allowing the fraudster to impersonate the legitimate customer. Device identification has also been implemented using geo-location or Internet protocol address matching. However, increasing evidence has shown that fraudsters often use proxies, which allow them to hide their actual location and pretend to be the legitimate user.[7]

Simple device identification as described above can be distinguished from a more sophisticated form of this technique which uses "one-time" cookies and creates a more complex digital "fingerprint" by looking at a number of characteristics including PC configuration, Internet protocol address, geo-location, and other factors.[8] Although no device authentication method can mitigate all threats, the Agencies consider complex device identification to be more secure and preferable to simple device identification. Institutions should no longer consider simple device identification, as a primary control, to be an effective risk mitigation technique.

Challenge Questions

Many institutions use challenge questions as a backup in the event that the primary logon authentication technique becomes inoperable or presents an unexpected characteristic. The provision of correct responses to challenge questions can also be used to re-authenticate the customer or verify a specific transaction subsequent to the initial logon. Similar to device identification,

[7] The National Security Agency has developed a patented method, available for public licensing, that can detect the use of a proxy.

[8] Technology vendors have developed "one-time" cookies which expire if stolen from the PC onto which they were originally loaded.

challenge questions can be implemented in a variety of ways that impact their effectiveness as an authentication tool. In its basic form, the user is presented with one or more simple questions from a list that was first presented to the customer when they originally enrolled in the online banking system. These questions can often be easily answered by an impostor who knows the customer or has used an Internet search engine to get information about the customer (e.g., mother's maiden name, high school the customer graduated from, year of graduation from college, etc.). In view of the amount of information about people that is readily available on the Internet and the information that individuals themselves make available on social networking websites, institutions should no longer consider such basic challenge questions, as a primary control, to be an effective risk mitigation technique.

Challenge questions can be implemented more effectively using sophisticated questions. These are commonly referred to as "out of wallet" questions, that do not rely on information that is often publicly available. They are much more difficult for an impostor to answer correctly. Sophisticated challenge question systems usually require that the customer correctly answer more than one question and often include a "red herring" question that is designed to trick the fraudster, but which the legitimate customer will recognize as nonsensical. The Agencies have also found that the number of challenge questions employed has a significant impact on the effectiveness of this control. Solutions that use multiple challenge questions, without exposing all the questions in one session, are more effective. Although no challenge question method can mitigate all threats, the Agencies believe the use of sophisticated questions as described above can be an effective component of a layered security program.

Customer Awareness and Education

A financial institution's customer awareness and educational efforts should address both retail and commercial account holders and, at a minimum, include the following elements:

- An explanation of protections provided, and not provided, to account holders relative to electronic funds transfers under Regulation E, and a related explanation of the applicability of Regulation E to the types of accounts with Internet access;
- An explanation of under what, if any, circumstances and through what means the institution may contact a customer on an unsolicited basis and request the customer's provision of electronic banking credentials;
- A suggestion that commercial online banking customers perform a related risk assessment and controls evaluation periodically;

- A listing of alternative risk control mechanisms that customers may consider implementing to mitigate their own risk, or alternatively, a listing of available resources where such information can be found; and,
- A listing of institutional contacts for customers' discretionary use in the event they notice suspicious account activity or experience customer information security-related events.

The attached Appendix contains an additional discussion of online threats and control methods.

Appendix

Threat Landscape and Compensating Controls

Threats

As noted previously in this Supplement, the Agencies are concerned that fraudsters are utilizing increasingly sophisticated and malicious techniques to thwart existing authentication controls, gain control of customer accounts, and transfer funds to money mules that facilitate the movement of those funds beyond the reach of financial institutions and law enforcement. Many of these schemes target small to medium-sized business customers since their account balances are generally higher than consumer accounts and their transaction activity is generally greater making it easier to hide the fraudulent transfers.

An effective tool in the fraudster's arsenal is keylogging malware. A keylogger is a software program that records the keystrokes entered on the PC on which it is installed and transmits a record of those keystrokes to the person controlling the malware over the Internet. Keyloggers can be surreptitiously installed on a PC by simply visiting an infected website or by clicking on an infected website banner advertisement or email attachment. Keylogging can also be accomplished via a hardware device plugged into the PC which stores the captured data for later use. Keylogger files are generally small in size and adept at hiding themselves on the user's PC. They often go undetected by most antivirus programs. Fraudsters use keyloggers to steal the logon ID, password, and challenge question answers of financial institution customers. This information alone or in conjunction with stolen browser cookies loaded on the fraudster's PC may enable the fraudster to log into the customer's account and transfer funds to accounts controlled by the fraudster, usually through wire or ACH transactions.

Other types of more sophisticated malware allow fraudsters to perpetrate man-in-the middle (MIM) or man-in-the browser (MIB) attacks on their victims. In a MIM/MIB attack, the fraudster inserts himself between the customer and the financial institution and hijacks the online session. In one scenario, the fraudster is able to intercept the authentication credentials submitted by the customer and log into the customer's account. In another scenario, the fraudster does not intercept the credentials, but modifies the transaction content or inserts additional transactions not authorized by the customer which, in most cases, are funds transfers to accounts controlled by the fraudster. The fraudsters conceal their actions by directing the customer to a fraudulent website that is a mirror image of

the financial institution's website or sending the customer a message claiming that the institution's website is unavailable and to try again later. Fraudsters may have the capacity to delete any trace of their attack from the log files.

MIM/MIB attacks may be used to circumvent some strong authentication methods and other controls, including one-time password (OTP) tokens. OTP tokens have been used for several years and have been considered to be one of the stronger authentication technologies in use. Since the one-time password is generally only good for 30-60 seconds after it is generated, the fraudster must intercept and use it in real time in order to compromise the customer's account.

Controls

The Agencies are aware of a variety of security techniques which can be used to help detect and prevent the types of attacks described above. Some of these techniques have been in use for some time, while others are relatively new. Financial institutions should investigate which of these controls may be more effective in detecting and preventing attacks as part of the institution's layered security program. However, it is important to note, that none of the controls discussed provide absolute assurance in preventing or detecting a successful attack. These controls may include the following:

Anti-malware software may provide a defense against keyloggers and MIM/MIB attacks. Anti-malware is a term that is commonly used to describe various software products that may also be referred to as anti-virus or anti-spyware. Anti-malware software is used to prevent, detect, block, and remove adware, spyware, and other forms of malware such as keyloggers. It is important to note that anti-malware is generally signature based, and some advanced versions of malware continuously alter their signature.

Transaction monitoring/anomaly detection software has been in use for a number of years. Similar to the manner in which the credit card industry detects and blocks fraudulent credit card transactions, systems are now available to monitor online banking activity for suspicious funds transfers. They can stop a suspicious ACH/wire transfer before completion and alert the institution and/or the customer so that the transfer can be further authenticated or dropped. Based upon the incidents the Agencies have reviewed, manual or automated transaction monitoring/anomaly detection could have assisted in preventing many fraudulent money transfers as they were clearly out of the ordinary when compared with the customer's established patterns of behavior. Automated systems may also look at the velocity of a transaction and other similar factors to determine whether it is suspicious.

The Agencies are aware of the fact that a number of institutions are requiring the "out-of-band" authentication or verification of certain high value and/or anomalous transactions. Out-of-band authentication means that a transaction that is initiated via one delivery channel (e.g., Internet) must be re-authenticated or verified via an independent delivery channel (e.g., telephone) in order for the transaction to be completed. Out-of-band authentication is becoming more popular given that customer PCs are increasingly vulnerable to malware attacks. However, out-of-band authentication directed to or input through the same device that initiates the transaction may not be effective since that device may have been compromised. For business customers, the out-of-band authentication or verification can be provided by someone other than the person who first initiated the transaction and can be combined with other administrative controls. Additionally, the use of out-of-band authentication or verification, for administrative changes to online business accounts, can be an effective control to reduce fraudulent funds transfers.

In response to the rising malware infection rates of customer PCs, a number of vendors have developed USB devices that increase session security when plugged into the customer's PC. These devices can function in several ways, but they generally enable a secure link between the customer's PC and the financial institution independent of the PC's operating system and application software. Typically, the device's firmware is "read only" and cannot be altered by the customer or the malware infecting the PC.

The use of restricted funds transfer recipient lists or other controls over the administration of such lists, can reduce funds transfer fraud. Fraudsters must frequently add new funds transfer recipients to an account profile in order to consummate the fraud.

Overall, the Agencies agree with security experts who believe that institutions should no longer rely on one form of customer authentication. A one dimensional customer authentication program is simply not robust enough to provide the level of security that customers expect and that protects institutions from financial and reputation risk. This concept of layered security is consistent with expectations the Agencies have discussed previously.[9] Layered security controls do not have to be complex. For example, implementing time of day restrictions on the customer's authority to execute funds transfers or using restricted funds transfer recipient

[9] See *FFIEC IT Examination Handbook*, Information Security Booklet, July 2006; FFIEC IT Examination Handbook, E-Banking Booklet, August 2003.

lists, in addition to robust logon authentication, can help to reduce the possibility of fraud.

The banking, payment, and security industries have continued to innovate in response to the increasing cyber threat environment. In addition to some of the control methods previously discussed, other examples of customer authentication include keystroke dynamics and biometric based responses. Additionally, institutions can look to traditional and innovative business process controls to improve security over customers' online activities. Some examples include:

- establish, require and periodically review volume and value limitations or parameters for what activities a business customer in the aggregate, and its enrolled users individually, can functionally accomplish while accessing the online system;
- monitor and alert on exception events;
- establish individual transaction and aggregate account exposure limits based on expected account activity;
- establish payee whitelisting (e.g., positive pay) and/or blacklisting;
- require every ACH file originating entity to provide a proactive notice of intent to originate a file prior to its submission; and
- require business customers to deploy dual control routines over higher risk functions performed online.

EXHIBIT F

FDIC

Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990

Financial Institution Letter
FIL-50-2011
June 29, 2011

FFIEC Supplement to *Authentication in an Internet Banking Environment*

Summary: The FDIC, with the other FFIEC agencies, has issued the attached guidance, which describes updated supervisory expectations regarding customer authentication, layered security, and other controls in an increasingly hostile online environment. Financial institutions will be expected to comply with the guidance no later than January 1, 2012.

Statement of Applicability to Institutions with Total Assets under $1 Billion: This Financial Institution Letter applies to all FDIC-supervised institutions offering online banking services.

Suggested Distribution:
FDIC-Supervised Banks (Commercial and Savings)

Suggested Routing:
Chief Executive Officer
Chief Information Security Officer

Related Topics:

- FIL-103-2005, Authentication in an Internet Banking Environment, October 12, 2005

Attachment:
FFIEC Supplement to Authentication in an Internet Banking Environment

Contact:
Jeffrey Kopchik, Senior Policy Analyst, at jkopchik@fdic.gov or (703) 254-0459

Note:
FDIC Financial Institution Letters (FILs) may be accessed from the FDIC's Web site at www.fdic.gov/news/news/financial/2010/index.html.

To receive FILs electronically, please visit http://www.fdic.gov/about/subscriptions/fil.html.

Paper copies of FDIC Financial Institution Letters may be obtained through the FDIC's Public Information Center, 3501 Fairfax Drive, E-1002, Arlington, VA 22226 (1-877-275-3342 or 703-562-2200).

Highlights:

- In 2005, the FFIEC issued guidance entitled *Authentication in an Internet Banking Environment.*
- This FFIEC guidance supplements the FDIC's supervisory expectations regarding customer authentication, layered security, and other controls in an increasingly hostile online environment.
- The FDIC expects institutions to upgrade their controls for high-risk online transactions through:
  - Yearly risk assessments;
  - For consumer accounts, layered security controls;
  - For business accounts, layered security controls consistent with the increased level of risk posed by business accounts; and
  - More active consumer awareness and education efforts.
- Layered security controls should include processes to detect and respond to suspicious or anomalous activity and, for business accounts, administrative controls.
- Certain types of device identification and challenge questions should no longer be considered effective controls.