STEIN, MITCHELL, CIPOLLONE, BEATO & MISSNER LLP
JONATHAN L. MISSNER, ESQ. (application for admission *pro hac vice* forthcoming)
ROBERT B. GILMORE, ESQ. (application for admission *pro hac vice* forthcoming)
1100 Connecticut Avenue
Washington, D.C. 20036
Telephone: (202) 737-7777
Facsimile: (202) 296-8312
jmissner@steinmitchell.com
rgilmore@steinmitchell.com

REID RUBINSTEIN & BOGATZ
I. SCOTT BOGATZ, ESQ.
Nevada Bar No. 3367
CHARLES M. VLASIC III, ESQ.
Nevada Bar No. 11308
3883 Howard Hughes Parkway, Suite 790
Las Vegas, Nevada 89169
Telephone: (702) 776-7000
Facsimile: (702) 776-7900
sbogatz@rrblf.com
cvlasic@rrblf.com]

Attorneys for Plaintiff Affinity Gaming

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

AFFINITY GAMING, a Nevada corporation, Plaintiff, vs. TRUSTWAVE HOLDINGS, INC., a Delaware corporation, Defendant.	**Case No.: 2:15-cv-2464**

COMPLAINT

Plaintiff, Affinity Gaming (sometimes referred to herein as "Affinity"), by and through the law firms of Stein, Mitchell, Cipollone, Beato & Missner LLP and Reid Rubinstein & Bogatz, respectfully sets forth its Complaint against Defendant, Trustwave Holdings, Inc. ("Trustwave"), and alleges as follows:

REID RUBINSTEIN & BOGATZ
3883 Howard Hughes Parkway, Suite 790
Las Vegas, Nevada 89169
(702) 776-7000 FAX: (702) 776-7900

PRELIMINARY STATEMENT

1. Beginning in October 2013, Trustwave, a firm that holds itself out to be a premier data security company, repeatedly assured Affinity Gaming (the owner of several casinos in Nevada) that Trustwave would investigate, diagnose and help remedy the data breach Affinity Gaming suffered. Relying on these assurances, Affinity Gaming hired Trustwave.

2. At the conclusion of its investigation, Trustwave represented to Affinity Gaming that the data breach was "contained" and purported to provide recommendations for Affinity Gaming to implement that would help fend off future data attacks.

3. Trustwave's representations were false. After Trustwave's engagement had concluded, Affinity Gaming learned that it had suffered an ongoing data breach. This discovery required Affinity Gaming to retain a second data security consulting firm, Mandiant.

4. Mandiant's forthright and thorough investigation concluded that Trustwave's representations were untrue, and Trustwave's prior work was woefully inadequate. In reality, Trustwave lied when it claimed that its so-called investigation would diagnose and help remedy the data breach, when it represented that the data breach was "contained," and when it claimed that the recommendations it was offering would address the data breach. Trustwave knew (or recklessly disregarded) that it was going to, and did, examine only a small subset of Affinity Gaming's data systems, and had failed to identify the means by which the attacker had breached Affinity Gaming's data security. Thus, Trustwave could not in good faith have made the foregoing representations to Affinity Gaming.

5. Trustwave's misrepresentations and grossly negligent performance resulted in Affinity Gaming suffering significant out of pocket losses. Affinity Gaming's ongoing data security breach also has drawn scrutiny from gaming and consumer protection regulators.

6. Trustwave has failed to accept responsibility for its misconduct and to compensate Affinity Gaming for its resulting losses. Accordingly, Affinity Gaming brings this action against Trustwave to recover the damages Trustwave has caused.

REID RUBINSTEIN & BOGATZ
3883 Howard Hughes Parkway, Suite 790
Las Vegas, Nevada 89169
(702) 776-7000 FAX: (702) 776-7900

JURISDICTION

7. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(a), because Affinity Gaming and Trustwave are citizens of different states, and the amount in controversy exceeds $75,000.

8. The court has personal jurisdiction over Trustwave, because it has purposefully availed itself of the benefits of the state, and because it regularly transacts business within the state, including specifically with respect to the present dispute by contracting with Affinity Gaming, a Nevada corporation, and by making its representations and conducting its services at Affinity Gaming's business premises within the state.

9. Venue is proper under 28 U.S.C. § 1391(b)(2) because a substantial part of the events and omissions giving rise to the underlying dispute occurred in this jurisdiction.

THE PARTIES

10. Affinity Gaming is a corporation organized under the laws of Nevada, with its principal place of business at 3755 Breakthrough Way, Suite 300, Las Vegas, Nevada, 89135. Affinity Gaming owns and operates 11 casinos in four states, including five casinos in Nevada.

11. Trustwave Holdings, Inc. is a corporation organized under the laws of Delaware with its principal place of business at 70 W. Madison Street, Suite 1050, Chicago, Illinois 60602. Trustwave represents itself as a firm that is highly experienced and capable in the field of data security. For example, Trustwave's website states:

> Trustwave helps businesses fight cybercrime, protect data and reduce security risk. With cloud and managed security services, integrated technologies and a team of security experts, ethical hackers and researchers, we enable businesses to transform the way they manage their information security and compliance programs.

FACTUAL BACKGROUND

A. AFFINITY GAMING INITIALLY LEARNS OF A DATA BREACH.

12. Over the course of 2012 through 2013, Affinity Gaming made various changes to its information technology ("IT") network security, as part of an overall ongoing upgrade of its IT

REID RUBINSTEIN & BOGATZ
3883 Howard Hughes Parkway, Suite 790
Las Vegas, Nevada 89169
(702) 776-7000 FAX: (702) 776-7900

network systems in connection with the company's acquisition of several properties and contemporaneous separation from a shared services arrangement with a former affiliate.

13. Despite Affinity Gaming's efforts at ensuring the security of its network and data, outside hackers were able to compromise the company's security.

14. On or about October 24, 2013, Affinity Gaming learned of information that led it to believe it had suffered a data breach.

15. Specifically, a small number of Affinity Gaming's customers, as well as local law enforcement, contacted the company regarding potential fraudulent credit card activity. Affinity Gaming's IT personnel responded to these reports and, based on their preliminary assessment, concluded that the company's data systems may have been compromised.

16. Affinity Gaming quickly reported this suspected data breach to its cyber insurance carrier, ACE, as well as to interested entities such as card-issuing banks.

17. ACE recommended that Affinity Gaming retain the services of a professional forensic data security investigators ("PFI"), and listed Trustwave as one of its panel of PFIs.

B. AFFINITY GAMING HIRES TRUSTWAVE.

18. Affinity Gaming quickly contacted Trustwave to inquire whether Trustwave could help Affinity to identify and remedy the apparent data breach.

19. From October 28-31, 2013, Trustwave personnel, including Chris Hague, Grayson Lenik and Matthew Aronson, had multiple direct and indirect conversations with Affinity Gaming personnel (including its Vice President of Insurance and Benefits and Vice President of Information Technology).

20. During those conversations, Trustwave personnel represented that the company had the capabilities to, and would, identify and help remedy the causes of the data breach, as well as facilitate Affinity Gaming's implementation of measures to help prevent further such breaches.

21. Hiring a firm with the proper data breach response expertise, such as Trustwave held itself out to be, was of paramount importance for Affinity Gaming, because, while Affinity

REID RUBINSTEIN & BOGATZ
3883 Howard Hughes Parkway, Suite 790
Las Vegas, Nevada 89169
(702) 776-7000 FAX: (702) 776-7900

takes seriously its data security obligations, and has implemented commercially reasonable and appropriate measures to protect its and its customers' data, Affinity is not an IT security firm and lacks the level of expertise and know-how in the technical aspects of data security that a firm like Trustwave purports to possess.

22. Thus, with respect to the apparent data breach, Affinity Gaming was wholly dependent on, and subordinate in terms of its knowledge, understanding, and capabilities, to Trustwave, relying on Trustwave to investigate, diagnose, and prescribe appropriate measures to address, Affinity's apparently compromised data security.

23. Moreover, Trustwave knew that it was important to Affinity's business relationships with its customers and credit card companies, as well as its relationships with its governmental regulators, that Affinity swiftly identify and resolve the data breach problem, so that Affinity could minimize the risk that it would suffer fines, penalties and monetary claims as a result of the breach.

24. Relying on Trustwave's representations, in October 2013, Affinity Gaming hired Trustwave to investigate and help remedy the data breach.

25. Trustwave drafted and presented to Affinity Gaming an Incident Response Agreement (the "Agreement"), which the parties signed on October 31, 2013.

26. In the Agreement, Trustwave agreed to undertake a "PCI [Payment Card Industry] Forensic Investigation." Trustwave represented that "PCI Forensic Investigations are conducted on behalf of organizations that have a suspected compromise of their cardholder data environment," and that "PCI Forensic Investigations are designed to identify if, how, what, and for how long cardholder data has been compromised and to provide recommendations to increase security."

27. In the Agreement, Trustwave promised to provide a "PCI Forensic Investigation [PFI] Report." That PFI Report had as its deliverables a description of the techniques and forensic analysis performed, the "technical findings," and "the conclusions of the investigation;

REID RUBINSTEIN & BOGATZ
3883 Howard Hughes Parkway, Suite 790
Las Vegas, Nevada 89169
(702) 776-7000 FAX: (702) 776-7900

has a compromise occurred; if so, what the evidence shows was the cause of the compromise; what data is at risk."

28. In the Agreement, Trustwave represented that its "[w]ork will be conducted in accordance with an agreement between Trustwave and the client," and that it would use "[a] rigorous quality assurance process."

29. Trustwave expressly warrantied in the Agreement that its "Services provided under this Agreement shall be performed with that degree of skill and judgment normally exercised by recognized professional firms performing services of the same or substantially similar nature."

C. TRUSTWAVE PERFORMS A WOEFULLY INADEQUATE "INVESTIGATION" AND SUBMITS A MISLEADING REPORT TO AFFINITY.

30. Trustwave investigators arrived at Affinity's offices on November 1, 2013. After more than two months meeting with Affinity personnel, analyzing Affinity's data systems, and providing a supposed diagnosis and suggested remedial measures for the data breach, on January 13, 2014, Trustwave submitted its PFI Report, describing its findings and activities.

31. Trustwave stated in its PFI Report that "[t]he goal of the investigation was to ***determine the extent to which a breach may have occurred***." (Emphasis added.)

32. In its PFI Report, Trustwave defined the "initial scope of the engagement" as inspection of only 10 servers and systems and Affinity Gaming's "physical security" and "network topology."

33. Affinity Gaming trusted, and was dependent on, Trustwave's assessment on what the proper scope of its engagement should be, given Trustwave's data security expertise, and in no way limited or restricted Trustwave's investigation of Affinity Gaming's data systems.

34. In its PFI Report, Trustwave made numerous representations to Affinity, including, among other things, that:

- "Trustwave has completed 100% of [its] investigative efforts,"

REID RUBINSTEIN & BOGATZ
3883 Howard Hughes Parkway, Suite 790
Las Vegas, Nevada 89169
(702) 776-7000 FAX: (702) 776-7900

- that the data breach "***compromise has been contained***," and
- that a "backdoor[1] component appears to exist within the code base, ***but appears to be inert***." (Emphases added.)

35. Trustwave also stated that it "believe[d] that the attacker became aware of the security upgrades that were taking place and took several steps to remove both the malware and evidence of the attack itself. Almost all components of the malware[2] were deactivated and/or removed from the systems on October 16, 2013. ***This activity ended the breach.***" (Emphasis added.)

36. On the "Incident Dashboard" in the front of its PFI Report, Trustwave explicitly stated to Affinity Gaming: "Compromise Status – Contained: Malware removed"

37. Finally, Trustwave presented Affinity Gaming with a number of recommendations on how to improve the company's data security measures. Following the conclusion of Trustwave's engagement, Affinity Gaming began to implement Trustwave's recommendations.

D. DESPITE TRUSTWAVE'S REPRESENTATIONS, AFFINITY GAMING LEARNS THAT ITS DATA BREACH HAD NOT BEEN CONTAINED, AND THAT ITS DATA SYSTEMS REMAINED UNSECURE.

38. However, the truth was something quite different than what Trustwave represented.

39. Shortly after Trustwave's engagement ended, and after Trustwave had promised that the data breach had been "contained" and the suspected backdoor(s) "inert," Affinity Gaming learned that its data systems still were compromised.

40. Affinity Gaming hired Ernst & Young to perform penetration testing pursuant to new regulations from the Missouri Gaming Commission. On April 16, 2014, in the course of performing such a test, Ernst & Young identified suspicious activity, including ongoing activity

[1] A "backdoor" is a method, often secret, of bypassing normal security authentication in a computer, network, or other data system. Backdoors are often used for securing unauthorized remote access.
[2] "Malware" is an umbrella term for hostile or intrusive software that infects or attacks data systems.

REID RUBINSTEIN & BOGATZ
3883 Howard Hughes Parkway, Suite 790
Las Vegas, Nevada 89169
(702) 776-7000 FAX: (702) 776-7900

from a malware program named "Framepkg.exe," which Trustwave had found, but apparently had not contained or sought to remediate, during its investigation in 2013.

41. Concerned that Trustwave's so-called "forensic investigation" had not lived up to what Trustwave had represented, Affinity Gaming was forced once again to conduct a forensic investigation into its data security, retaining a second data security firm, Mandiant. Affinity Gaming contracted with Mandiant on April 19, 2014 to investigative the newly-discovered suspicious activity.

42. Mandiant, like Trustwave was supposed to have done before, undertook an investigation to identify the source of the potential breach, ensure the breach was contained, and identify any security deficiencies. On April 23, 2014, Mandiant identified an ongoing incident affecting Affinity Gaming's cardholder data environment and initiated its own PFI.

43. Mandiant's investigation initially focused on a period of attacker activity between December 6, 2013 and April 27, 2014. The scope of the investigation expanded to include the "previous" data breach that had occurred between March and October, 2013 – the data breach Trustwave supposedly had investigated – after Mandiant determined that Trustwave had failed to identify the entire extent of the breach.

44. On April 28, 2014, Mandiant submitted a Preliminary PFI Report to Affinity Gaming and credit card companies, and submitted its final PFI Report on July 1, 2014 (the "Mandiant PFI Report").

45. Mandiant's conclusions were startling to Affinity Gaming.

46. Mandiant's far more thorough and forthright investigation correctly diagnosed the true cause of the data breach – a cause that Trustwave could have and should have identified and helped remedy originally.

47. Trustwave had failed to diagnose that the data breach actually was the result of unidentified outside persons or organizations who were able to compromise Affinity's data

REID RUBINSTEIN & BOGATZ
3883 Howard Hughes Parkway, Suite 790
Las Vegas, Nevada 89169
(702) 776-7000 FAX: (702) 776-7900

through Affinity Gaming's Virtual Private Network ("VPN"),[3] and that the "backdoor" these persons/organizations had created – which Trustwave had speculated may have existed but concluded was "inert" – was very real and accessible.

48. While Trustwave had concluded that the last data breach activity occurred in October 2013, Mandiant's investigation revealed that these persons/organizations again compromised Affinity Gaming's data in December 2013, ***while Trustwave's supposed investigation and remediation efforts were still ongoing***.

49. Mandiant also determined that the unauthorized access and renewed data breach occurred on a continuous basis both before and after Trustwave claimed that the data breach had been "contained."

50. In that report, among other things, Mandiant specifically criticized Trustwave for performing an incomplete investigation that did not determine how the outside attacker was maintaining its ability to breach Affinity Gaming's security:

> [Trustwave] failed to identify the full scope of the previous incident, which left the Affinity network vulnerable to future attacks. The previous PFI [Trustwave] chose to investigate 7 systems and did not determine how the attacker maintained access to the environment via the VPN [virtual private network] and the two backdoors installed on October 16, 2013.

51. Mandiant's investigation revealed a long list of Trustwave misrepresentations, omissions, and failures.

52. Despite indications that Trustwave should have expanded its scope of engagement – such as Trustwave's suspicion of a backdoor component, and identification of an open communication link that led outside of Affinity Gaming's systems – Trustwave did not do so, nor did Trustwave recommend any such expansion to Affinity Gaming.

53. Trustwave claimed that the firm suspected remote access was the means by which the hacker penetrated Affinity Gaming's system. However, Trustwave did not review Affinity

[3] A "virtual private network (VPN)" extends a private network across a public network, such as the Internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

REID RUBINSTEIN & BOGATZ
3883 Howard Hughes Parkway, Suite 790
Las Vegas, Nevada 89169
(702) 776-7000 FAX: (702) 776-7900

Gaming's Remote Access Logs, and failed to identify the evidence in those logs, demonstrating that remote access (through Affinity Gaming's VPN portal) was the means by which the attacker breached Affinity Gaming's systems.

54. Trustwave failed to note, and identify, two malware programs (LsaExt.dll and pwsrv.exe) on one of the servers (HSJADS01) that the firm had imaged and analyzed. The attacker used these programs to obtain additional valid, internal passwords to Affinity Gaming's systems.

55. Trustwave noted, but inexplicably failed to investigate, an open communication link to an external system outside of Affinity Gaming's control. The communication link was "initiated through another piece of malware" which Trustwave did not identify. The attacker created the link after the date by which, according to Trustwave, the attacker supposedly had withdrawn from Affinity Gaming's systems.

56. Trustwave's report contains inconsistencies regarding the ongoing existence of malware on Affinity Gaming's systems. As noted above, in its "Incident Dashboard" Trustwave asserted that the malware had been removed. However, elsewhere in the Report, Trustwave states that one particular piece of malware, Framepkg.exe, was still "running on the system at the time of acquisition" which occurred on November 1 and 2, 2013.

57. Trustwave willfully disregarded further evidence that the breach was likely more widespread than what the firm found through its review of the limited systems it examined. In its report, the firm stated that the absence of certain evidence "[led] us to believe that data exfiltration took place manually, or via some undiscovered avenue." This finding and belief should have required Trustwave to expand the scope of the investigation to determine whether additional systems, not collected and analyzed in the "initial scope," were also compromised.

58. Trustwave willfully disregarded other evidence that the breach was more widespread than first believed. One of the Affinity Gaming servers from which Trustwave had collected data – HG-DLRSONNET – reflected a file – Default.rdp – that was created on March

REID RUBINSTEIN & BOGATZ
3883 Howard Hughes Parkway, Suite 790
Las Vegas, Nevada 89169
(702) 776-7000 FAX: (702) 776-7900

13, 2013, the date of the initial breach. That type of file is created when a person uses a certain program to remotely access a different workstation or server in the same network. The existence of the file, with the same creation date as the date of the breach, on a known, compromised server should have led Trustwave to investigate whether additional systems were also compromised.

59. Trustwave also failed, in connection with the same HG_DLRSONNET server, to determine and identify that it had been compromised with the "rd.exe" malware, which is a "cardholder data harvesting malware."

60. Trustwave failed to identify any malware on three of the systems it collected – TRCMICROS, HMT-MICROS and HLKMICROS – despite these systems also having been attacked with malware.

61. Had Trustwave discovered these systems were also compromised, the firm could have and should have expanded the scope of the investigation and helped remediate the breach.

62. Trustwave concluded that the attacker removed the malware and exited the system on October 16, 2013. However, Trustwave disregarded, or did not properly investigate, a file – debuglogex.txt – that was created on a compromised system which it had collected – HSJADS01 – on that same date. Had Trustwave investigated this file, the firm should have discovered that the attacker had deployed a backdoor malware on two other Affinity Gaming systems.

63. Unlike Trustwave, Mandiant diagnosed the means by which the attacking persons/organizations breached Affinity's data systems, assessed the extent of the breach itself and the affected Affinity Gaming data systems, and formulated and helped Affinity implement successful remedies to correct the compromised security and prevent further breaches.

64. Mandiant determined that, over the course of two days – March 13-14, 2013 – the "attacker accessed at least 93 systems [and] deployed cardholder data harvesting malware to at least 76 systems." (Emphasis added.) Additionally, Mandiant found the attacker specifically "deployed and executed cardholder data harvesting malware on 12 systems within the PCI environment" on March 14, 2013. Among these systems are four that Trustwave supposedly

REID RUBINSTEIN & BOGATZ
3883 Howard Hughes Parkway, Suite 790
Las Vegas, Nevada 89169
(702) 776-7000 FAX: (702) 776-7900

collected and examined, and as stated above, Trustwave failed to determine that three of the four had been compromised by the attacker.

65. Mandiant's report also concluded that the various recommendations Trustwave had presented to improve Affinity Gaming's data security were pointless: none addressed the source of the data breach, and none would have prevented the attacker from again accessing Affinity Gaming's data systems (for instance, through the backdoors that Trustwave failed to find and close).

66. Mandiant's investigation and remediation confirmed that Trustwave's representations were clearly inaccurate, and its efforts woefully lacking. Had Trustwave performed the investigation and data security measures it represented to have taken, it could have, and should have, identified the causes and extent of the data breach during its engagement, and identified measures that would actually have remedied the breach and prevented the attacker from again accessing Affinity Gaming's systems.

E. TRUSTWAVE HAS CAUSED AFFINITY GAMING SIGNIFICANT HARM.

67. Trustwave's misrepresentations, omissions, and failures directly led to Affinity Gaming incurring significant monetary damages.

68. Affinity Gaming paid Trustwave fees that proved entirely wasted.

69. But beyond that, Trustwave's wrongful conduct caused Affinity Gaming to incur significant internal and third-party costs to remedy the ongoing data breach, including paying the second data security firm, Mandiant, as well as outside counsel and other outside consultants.

70. Affinity Gaming also has had to pay assessments from credit card companies and banks to reissue new credit cards to customers whose data had been stolen through the "second breach," and to cover fraudulent charges made using the stolen credit card data.

71. And the company incurred further costs by having to publish notice of the "second breach" both on its various subsidiaries' websites, and in virtual publications nationwide. This notice was reported by media in various locations where Affinity Gaming conducts business,

REID RUBINSTEIN & BOGATZ
3883 Howard Hughes Parkway, Suite 790
Las Vegas, Nevada 89169
(702) 776-7000 FAX: (702) 776-7900

causing damage to its reputation on top of the substantial costs associated with providing such widespread notice.

72. Affinity Gaming would have avoided these costs had Trustwave not misrepresented its work and performed its investigation properly.

73. In addition, Affinity Gaming has had to brief its gaming regulators in the four states in which it operates, as well as various states attorneys general, on multiple occasions regarding the circumstances involving the data breaches and the investigations and remedial measures the company has taken. As of the date of this Complaint, the attorneys general continue to investigate the two data breach events, and Affinity Gaming could face further sanctions as a result, as well as further damage to its reputation.

74. In short, had Trustwave lived up to its representations, Affinity Gaming would have avoided all of these financial and reputational injuries. Affinity Gaming's monetary harm is considerably in excess of $100,000.

75. Despite Affinity Gaming's requests, Trustwave has refused to agree to compensate Affinity Gaming for the harm it has suffered as a result of Trustwave's misrepresentations, omissions, and utter failure to conduct the investigation it purported to perform.

76. Affinity Gaming therefore brings the instant action to recover for the damages that Trustwave's wrongful conduct has caused.

FIRST CLAIM FOR RELIEF
(Fraudulent Inducement)

77. Affinity Gaming incorporates the foregoing factual background into the averments of this cause of action as if repeated hereinafter verbatim.

78. Prior to Affinity Gaming and Trustwave contracting, and with the intent to induce Affinity Gaming to enter into a contract with Trustwave, Trustwave made the following material misrepresentations and omissions of material information to Affinity Gaming regarding prior or then-existing statements of fact:

a. Trustwave misrepresented that it had the capabilities and experience as a data security service provider to investigate, diagnose, and help remedy the data breach Affinity Gaming had suffered, and omitted that it lacked such capabilities and experience; and

b. Trustwave misrepresented that, if Affinity Gaming entered into a contract with Trustwave, Trustwave would investigate, diagnose, and help remedy the data breach Affinity Gaming had suffered, when Trustwave knew that the contemplated scope of its engagement, and the work it would perform, under the contract, would not be adequate for such purposes, and Trustwave omitted telling Affinity Gaming of such inadequacies.

79. These representations and omissions were false and deceptive. Trustwave lacked the capabilities and experience necessary to perform its data security services under the Agreement and to conduct an appropriate investigation. Trustwave did not perform an adequate investigation, and the contemplated scope of the engagement and nature of the services under the contract were not adequate for investigating, diagnosing, and helping to remedy Affinity Gaming's data breaches.

80. Trustwave made these misrepresentations and omissions with knowledge of, or at least in reckless disregard of, their falsity.

81. Affinity Gaming was ignorant of the falsity of Trustwave's misrepresentations and omissions.

82. Trustwave intended Affinity Gaming to rely on Trustwave's misrepresentations and omissions, in order to induce Affinity Gaming to contract with Trustwave.

83. Affinity Gaming reasonably relied on Trustwave's misrepresentations and omissions, to Affinity Gaming's detriment, in entering into a contract with Trustwave to conduct an investigation and remedy or contain the data breach; in paying Trustwave fees for such contractual services; and in depending on Trustwave to address the data breach sufficiently for Affinity Gaming to avoid the financial and reputational harm, and regulatory scrutiny and action, that would result if the data breach persisted without an adequate investigation, diagnosis, and remedial effort.

84. Affinity Gaming was consequently and proximately injured by these

REID RUBINSTEIN & BOGATZ
3883 Howard Hughes Parkway, Suite 790
Las Vegas, Nevada 89169
(702) 776-7000 FAX: (702) 776-7900

misrepresentations and omissions. Affinity Gaming therefore is entitled to an award of its damages caused by Trustwave's fraudulently inducing Affinity Gaming into contracting with Trustwave, in an amount to be proven at trial but which exceed $100,000.

85. Affinity Gaming also is entitled to punitive and exemplary damages equal to three times its compensatory damages pursuant to NRS § 42.005, by virtue of Trustwave's fraud, malice and oppression.

SECOND CLAIM FOR RELIEF
(Fraud)

86. Affinity Gaming incorporates the foregoing factual background into the averments of this cause of action as if repeated hereinafter verbatim.

87. Trustwave made at least the following material misrepresentations and omissions of material information to Affinity Gaming regarding prior or then-existing statements of fact:

a. Trustwave misrepresented and omitted at the beginning of its engagement that it had the capabilities and experience as a data security service provider to investigate, diagnose, and help remedy the data breach that Affinity Gaming had suffered, and omitted that it lacked such capabilities and experience;

b. Trustwave misrepresented that it had undertaken a proper investigation to determine the cause of Affinity Gaming's data breach, and to contain and help remedy such breach;

c. Trustwave misrepresented at the conclusion of its so-called investigation that the data breach was "contained" and the suspected backdoor was "inert"; and

d. Trustwave misrepresented that its recommendations on improving Affinity Gaming's data security would help to prevent this and further data breaches from occurring.

88. These representations and omissions were false and deceptive. Trustwave lacked the capabilities necessary to perform its data security services under the Agreement and to conduct an appropriate investigation. Trustwave did not perform an adequate investigation. Trustwave knew or should have known it had not diagnosed and remedied the source of the data breach or the suspected backdoors, and therefore there was no basis for Trustwave to represent

REID RUBINSTEIN & BOGATZ
3883 Howard Hughes Parkway, Suite 790
Las Vegas, Nevada 89169
(702) 776-7000 FAX: (702) 776-7900

the data breach was "contained" or the backdoors were "inert." And Trustwave's recommendations on further data security measures, even if fully implemented, would not have rectified Affinity Gaming's data breach, given Trustwave's knowing failure to identify the data breach source or the backdoors.

89. Trustwave made these misrepresentations and omissions with knowledge of, or at least in reckless disregard of, their falsity.

90. Affinity Gaming was ignorant of the falsity of Trustwave's misrepresentations and omissions.

91. Trustwave intended Affinity Gaming to rely on Trustwave's misrepresentations and omissions.

92. Affinity Gaming reasonably relied on Trustwave's misrepresentations and omissions, to Affinity Gaming's detriment, by, among other things, engaging Trustwave to conduct an investigation and remedy or contain the data breach; believing Trustwave's representations that the data breach had been contained and the backdoor inert; representing to customers, vendors, and governmental actors that Affinity Gaming's data breach had been diagnosed and remedied, based on Trustwave's assurances; and implementing measures that Trustwave recommended even though those measures did not rectify the data breach that Affinity Gaming had suffered.

93. Affinity Gaming was consequently and proximately injured by these misrepresentations and omissions. Affinity Gaming therefore is entitled to an award of its damages caused by Trustwave's fraud, in an amount to be proven at trial but which exceed $100,000.

94. Affinity Gaming also is entitled to punitive and exemplary damages equal to three times its compensatory damages pursuant to NRS § 42.005, by virtue of Trustwave's fraud, malice and oppression.

REID RUBINSTEIN & BOGATZ
3883 Howard Hughes Parkway, Suite 790
Las Vegas, Nevada 89169
(702) 776-7000 FAX: (702) 776-7900

REID RUBINSTEIN & BOGATZ
3883 Howard Hughes Parkway, Suite 790
Las Vegas, Nevada 89169
(702) 776-7000 FAX: (702) 776-7900

THIRD CLAIM FOR RELIEF
(Constructive/Equitable Fraud)

95. Affinity Gaming incorporates the foregoing statements of fact into the averments of this cause of action as if repeated hereinafter verbatim.

96. In the circumstances alleged above, Affinity Gaming had a special relationship with Trustwave.

97. In particular, Trustwave had a duty to deal fairly with Affinity Gaming because:

a. Trustwave claimed to possess specialized knowledge, experience and qualifications regarding security for information technology systems and data;

b. such specialized knowledge, experience and qualifications put Trustwave in a position of superiority over Affinity Gaming;

c. Trustwave knew that Affinity Gaming needed to rely and did rely on Trustwave's claimed specialized knowledge, experience and qualifications, and on information supplied by Trustwave, in making decisions on engaging Trustwave to investigate, diagnose and remedy or contain Affinity Gaming's data breach, and in believing that Trustwave had in fact diagnosed and remedied or contained such breach, because Affinity was not able to detect the falsity and incompleteness of the information supplied by Trustwave;

d. Affinity Gaming was uniquely vulnerable to injury if Trustwave did not supply truthful and accurate information; and

e. Trustwave stood to gain at Affinity Gaming's expense, if Trustwave did not supply truthful and accurate information.

98. Trustwave breached its duty to deal fairly with Affinity Gaming by making at least the following material misrepresentations and omissions of material information regarding prior or then-existing statements of fact:

a. Trustwave misrepresented and omitted at the beginning of its engagement that it had the capabilities as a data security service provider to perform the contemplated work under the Agreement, when in fact it lacked such capabilities and experience;

b. Trustwave misrepresented that it had undertaken a proper investigation to determine the cause of Affinity Gaming's data breach, and to contain and

REID RUBINSTEIN & BOGATZ
3883 Howard Hughes Parkway, Suite 790
Las Vegas, Nevada 89169
(702) 776-7000 FAX: (702) 776-7900

help remedy such breach;

c. Trustwave misrepresented at the conclusion of its so-called investigation that the data breach was "contained" and the suspected backdoor was "inert"; and

d. Trustwave misrepresented that its recommendations on improving Affinity Gaming's data security would help to prevent this and further data breaches from occurring.

99. These representations and omissions were false and deceptive. Trustwave lacked the experience and capabilities necessary to perform its data security services under the Agreement and to conduct an appropriate investigation. Trustwave did not perform an adequate investigation. Trustwave had not diagnosed and remedied the source of the data breach or the suspected backdoors, and therefore there was no basis for Trustwave to represent the data breach was "contained" or the backdoors were "inert." And Trustwave's recommendations on further data security measures, even if fully implemented, would not have rectified Affinity Gaming's data breach, given Trustwave's failure to identify the data breach source or the backdoors.

100. Affinity Gaming was ignorant of the falsity of Trustwave's misrepresentations and omissions.

101. Through its misrepresentations and omissions, Trustwave gained a benefit at Affinity Gaming's expense, because, among other things, Trustwave convinced Affinity Gaming to retain Trustwave and to pay Trustwave for its supposed services.

102. Affinity Gaming reasonably relied on Trustwave's misrepresentations and omissions, to Affinity Gaming's detriment, by, among other things, engaging Trustwave to conduct an investigation and remedy or contain the data breach; believing Trustwave's representations that the data breach had been contained and the backdoor inert; representing to customers, vendors, and governmental actors that Affinity Gaming's data breach had been diagnosed and remedied, based on Trustwave's assurances; and implementing measures that Trustwave recommended even though those measures would not address the underlying causes of the data breach that Affinity Gaming had suffered.

REID RUBINSTEIN & BOGATZ
3883 Howard Hughes Parkway, Suite 790
Las Vegas, Nevada 89169
(702) 776-7000 FAX: (702) 776-7900

103. Affinity Gaming was consequently and proximately injured by these misrepresentations and omissions. Affinity Gaming therefore is entitled to an award of its damages caused by Trustwave's constructive fraud, in an amount to be proven at trial but which exceed $100,000.

104. Affinity Gaming also is entitled to punitive and exemplary damages equal to three times its compensatory damages pursuant to NRS § 42.005, by virtue of Trustwave's fraud, malice and oppression.

FOURTH CLAIM FOR RELIEF
(Violations of NRS Chapter 598; Fraud Upon Purchasers; Misrepresentation)

105. Affinity Gaming incorporates the foregoing factual background into the averments of this cause of action as if repeated hereinafter verbatim.

106. NRS § 598.0923(2) provides that a person engages in a deceptive trade practice when, in the course of his business or occupation, he knowingly fails to disclose a material fact in connection with the sale or lease of goods or services.

107. NRS § 598.0915(15) provides that a person engages in a deceptive trade practice when, in the course of his business or occupation, he knowingly makes a false representation in a transaction.

108. NRS § 598.0915(5) provides that person engages in a deceptive trade practice when, in the course of his business or occupation, he knowingly makes a false representation as to the characteristics of services.

109. Trustwave engaged in the business of providing forensic data security investigation services to Affinity Gaming.

110. In the course of performing such services, Trustwave made at least the following knowingly deceptive misrepresentations and omissions to Affinity Gaming:

a. Trustwave misrepresented and omitted at the beginning of its engagement that it had the capabilities and experience as a data security service provider to investigate, diagnose, and help remedy the data breaches that

REID RUBINSTEIN & BOGATZ
3883 Howard Hughes Parkway, Suite 790
Las Vegas, Nevada 89169
(702) 776-7000 FAX: (702) 776-7900

Affinity Gaming had suffered, and omitted that it lacked such capabilities and experience;

b. Trustwave misrepresented that it had undertaken a proper investigation to determine the cause of Affinity Gaming's data breach, and to contain and help remedy such breach;

c. Trustwave misrepresented at the conclusion of its so-called investigation that the data breach was "contained" and the suspected backdoor was "inert"; and

d. Trustwave misrepresented that its recommendations on improving Affinity Gaming's data security would help to prevent this and further data breaches from occurring.

111. These representations and omissions were false and deceptive. Trustwave lacked the capabilities necessary to perform its data security services under the Agreement and to conduct an appropriate investigation. Trustwave did not perform an adequate investigation. Trustwave knew or should have known it had not diagnosed and remedied the source of the data breach or the suspected backdoors, and therefore there was no basis for Trustwave to represent the data breach was "contained" or the backdoors were "inert." And Trustwave's recommendations on further data security measures, even if fully implemented, would not have rectified Affinity Gaming's data breach, given Trustwave's knowing failure to identify the data breach source or the backdoors.

112. Affinity Gaming was the victim of Trustwave's deceptive trade practices, in that Affinity Gaming was consequently and proximately harmed by Trustwave's misrepresentations and omissions, through among other things, engaging Trustwave to conduct an investigation and remedy or contain the data breach; believing Trustwave's representations that the data breach had been identified, contained, and remained inert; representing to customers, vendors, and governmental actors that Affinity Gaming's data breach had been diagnosed and remedied, based on Trustwave's assurances; and implementing measures that Trustwave recommended even though those measures did not rectify the data breach that Affinity Gaming had suffered.

113. Violations of NRS Chapter 598 are actionable under NRS § 41.600 by any person (including a corporation) who is a victim of consumer fraud. NRS § 41.600(2)(e) defines

REID RUBINSTEIN & BOGATZ
3883 Howard Hughes Parkway, Suite 790
Las Vegas, Nevada 89169
(702) 776-7000 FAX: (702) 776-7900

consumer fraud to include deceptive trade practices as defined in NRS §§ 598.0915 to 598.0925, inclusive.

114. NRS § 41.600(3) provides that if the claimant is the prevailing party in an action brought for consumer fraud, then "the court ***shall*** award the claimant: (a) any damages that the claimant has sustained; (b) any equitable relief that the court deems appropriate; and (c) the claimant's costs in the action and reasonable attorney's fees." (Emphasis added.)

115. Affinity Gaming therefore is entitled to recover the damages it has sustained (which exceeds $100,000), any equitable relief the Court deems appropriate, and an award of Affinity Gaming's costs and reasonable attorneys' fees, as a result of Trustwave's deceptive trade practices.

116. Affinity Gaming also is entitled to punitive and exemplary damages equal to three times its compensatory damages pursuant to NRS § 42.005, by virtue of Trustwave's fraud, malice and oppression.

FIFTH CLAIM FOR RELIEF
(Gross Negligence)

117. Affinity Gaming incorporates the foregoing factual background into the averments of this cause of action as if repeated hereinafter verbatim.

118. Trustwave owed Affinity Gaming a duty of care in performing its data security services, and in providing information that was truthful and accurate regarding Trustwave's investigation, the causes of Affinity Gaming's data breach, and the remediation or containment of that breach.

119. Trustwave acted recklessly, willfully, wantonly, and without even slight care, in failing to perform the investigation it had represented it would undertake; in asserting that it had diagnosed and contained the data breach when it had not done so; in claiming that the suspected backdoor was inert when it had not even identified, let alone sought to remediate, the backdoor; and in making recommendations to Affinity Gaming that Trustwave claimed would address the

REID RUBINSTEIN & BOGATZ
3883 Howard Hughes Parkway, Suite 790
Las Vegas, Nevada 89169
(702) 776-7000 FAX: (702) 776-7900

data breach when, in reality, the recommended measures would not have secured Affinity Gaming's data systems, given Trustwave's failure to identify the data breach source or the backdoor.

120. Trustwave's grossly negligent conduct consequently and proximately caused Affinity Gaming harm. Affinity Gaming therefore is entitled to an award of damages caused by Trustwave's gross negligence, in an amount to be proven at trial but which exceed $100,000.

SIXTH CLAIM FOR RELIEF
(Negligent Misrepresentation)

121. Affinity Gaming incorporates the foregoing factual background into the averments of this cause of action as if repeated hereinafter verbatim.

122. Trustwave made at least the following material misrepresentations and omissions of material information to Affinity Gaming regarding prior or then-existing statements of fact:

a. Trustwave misrepresented and omitted at the beginning of its engagement that it had the capabilities as a data security service provider to perform the contemplated work under the Agreement, when in fact it evidently lacked such capabilities and experience;

b. Trustwave misrepresented that it had undertaken a proper investigation to determine the cause of Affinity Gaming's data breach, and to contain and help remedy such breach;

c. Trustwave misrepresented at the conclusion of its so-called investigation that the data breach was "contained" and the suspected backdoor was "inert"; and

d. Trustwave misrepresented that its recommendations on improving Affinity Gaming's data security would help to prevent this and further data breaches from occurring.

123. These representations and omissions were false and deceptive. Trustwave lacked the experience and capabilities necessary to perform its data security services under the Agreement and to conduct an appropriate investigation. Trustwave did not perform an adequate investigation. Trustwave had not diagnosed and remedied the source of the data breach or the suspected backdoors, and therefore there was no basis for Trustwave to represent the data breach

REID RUBINSTEIN & BOGATZ
3883 Howard Hughes Parkway, Suite 790
Las Vegas, Nevada 89169
(702) 776-7000 FAX: (702) 776-7900

was "contained" or the backdoors were "inert." And Trustwave's recommendations on further data security measures, even if fully implemented, would not have rectified Affinity Gaming's data breach, given Trustwave's failure to identify the data breach source or the backdoors.

124. Affinity Gaming was ignorant of the falsity of Trustwave's misrepresentations and omissions.

125. Trustwave owed a duty of care to communicate truthful information to Affinity Gaming.

126. Trustwave breached its duty of care to Affinity Gaming by failing to exercise such care and by communicating false information to Affinity Gaming.

127. Affinity Gaming reasonably relied on Trustwave's misrepresentations and omissions, to Affinity Gaming's detriment, by, among other things, engaging Trustwave to conduct an investigation and remedy or contain the data breach; believing Trustwave's representations that the data breach had been identified, contained, and remained inert; representing to customers, vendors, and governmental actors that Affinity Gaming's data breach had been diagnosed and remedied, based on Trustwave's assurances; and implementing measures that Trustwave recommended even though those measures would not address the underlying cause of the data breach that Affinity Gaming had suffered.

128. Affinity Gaming was consequently and proximately injured by these misrepresentations and omissions. Affinity Gaming therefore is entitled to an award of its damages caused by Trustwave's negligent misrepresentations, in an amount to be proven at trial but which exceed $100,000.

SEVENTH CLAIM FOR RELIEF
(Breach of Contract)

129. Affinity Gaming incorporates the foregoing statements of fact into the averments of this cause of action as if repeated hereinafter verbatim.

130. Under the parties' Agreement, Trustwave agreed to perform a forensic

REID RUBINSTEIN & BOGATZ
3883 Howard Hughes Parkway, Suite 790
Las Vegas, Nevada 89169
(702) 776-7000 FAX: (702) 776-7900

investigation to identify, and remedy or contain, the causes of Affinity Gaming's data breach, and to issue recommendations for measures Affinity Gaming would undertake to prevent further breaches in the future.

131. Trustwave also was obligated to perform its services and contractual duties, and to deal with Affinity Gaming, reasonably, prudently, fairly and in good faith, under the implied covenant of good faith and fair dealing.

132. Trustwave failed to perform those services properly, and failed to fulfill its duty of good faith and fair dealing, as described herein in the foregoing statements of fact.

133. Trustwave acted intentionally, willfully, wantonly, recklessly and with gross negligence in breaching its contractual duties to Affinity Gaming. As a result, any purported exculpatory provisions, or limitations on liability and damages, included in the Agreement are not enforceable against Affinity Gaming.

134. Affinity Gaming has been injured as a result of Trustwave's contractual breaches. Affinity Gaming therefore is entitled to an award of its damages caused by Trustwave's breaches of the Agreement, in an amount to be proven at trial but which exceed $100,000.

EIGHTH CLAIM FOR RELIEF
(Declaratory Judgment under 28 U.S.C. §§ 2201-2202)

135. Affinity Gaming incorporates the foregoing statements of fact into the averments of this cause of action as if repeated hereinafter verbatim.

136. An actual, ripe, and justiciable case or controversy exists between Affinity Gaming and Trustwave regarding Trustwave's misrepresentations/omissions, gross negligence, and breaches of contract, and the rights and responsibilities of the parties herein.

137. Because of Trustwave's wrongful conduct, Affinity Gaming faces the prospect of future monetary harm resulting from the fact that the data breach went undiagnosed and uncontained even after Trustwave claimed to have completed its supposed investigation. Such future harm includes, but is not limited to, claims by customers, claims and assessments from

credit card companies, and fines and penalties from government regulators.

138. Affinity Gaming therefore is entitled to a judgment declaring that Trustwave is liable to Affinity Gaming for any and all damages Affinity Gaming suffers in the future resulting from the undiagnosed and uncontained data breach.

PRAYER FOR RELIEF

WHEREFORE, Affinity Gaming requests that the Court grant the following relief:

1. Judgment in Affinity Gaming's favor and against Trustwave on all of Affinity Gaming's claims;

2. An award of general and special damages to Affinity Gaming, in an amount to be proven at trial but which exceed $100,000;

3. Punitive and exemplary damages;

4. A declaration that Trustwave is liable to Affinity Gaming for any and all future losses or injuries arising from Trustwave's misconduct;

5. Pre- and post-judgment interest to the extent permitted by law;

6. Attorneys' fees and costs to the extent permitted by law; and

7. Any other relief that the Court may deem just and proper.

DATED this 24th day of December, 2015.

STEIN, MITCHELL, CIPOLLONE, BEATO & MISSNER LLP

By: */s/ Charles M. Vlasic III, Esq. for:*
Jonathan L. Missner, Esq. (*pro hac vice* forthcoming)
Robert B. Gilmore, Esq. (*pro hac vice* forthcoming)
1100 Connecticut Avenue
Washington, D.C. 20036

-and-

REID RUBINSTEIN & BOGATZ
I. Scott Bogatz, Esq.
Nevada Bar No. 3367
Charles M. Vlasic III, Esq.
Nevada Bar No. 11308
3883 Howard Hughes Parkway, Ste. 790
Las Vegas, Nevada 89169

Attorneys for Plaintiff Affinity Gaming

REID RUBINSTEIN & BOGATZ
3883 Howard Hughes Parkway, Suite 790
Las Vegas, Nevada 89169
(702) 776-7000 FAX: (702) 776-7900

REID RUBINSTEIN & BOGATZ
3883 Howard Hughes Parkway, Suite 790
Las Vegas, Nevada 89169
(702) 776-7000 FAX: (702) 776-7900