IN THE CIRCUIT COURT OF THE THIRTEENTH JUDICIAL CIRCUIT
IN AND FOR HILLSBOROUGH COUNTY, FLORIDA

Pamela Clark,

JURY TRIAL DEMANDED

Plaintiff,

v. Case No:

Navvis & Company, LLC,

Defendant,
_____/

COMPLAINT

COMES NOW Plaintiff Pamela Clark ("Plaintiff"), and sues Defendant Navvis & Company, LLC ("Defendant"), alleging as follows:

NATURE OF THE ACTION

1. Plaintiff brings this action against Defendant for its failure to properly secure and safeguard personally identifiable and financial information ("PII") of Plaintiff including, without limitation: medical information, insurance information, name(s), date of birth, home address(es), phone number(s), Social Security number, and email address(es).
2. Defendant is a health management service provider duly licensed to transact business in the State of Florida. Defendant does business, has offices, and/or maintains agents for the transaction of its customary business in Hillsborough County, Florida.
3. Defendant is entrusted with an extensive amount of Plaintiff's PII.
4. By obtaining, collecting, using, and deriving a benefit from Plaintiff's PII, Defendant assumed legal and equitable duties to Plaintiff.

5. In or around July 2023, an intruder gained entry to Defendant's database, accessed Plaintiff's PII, and exfiltrated information from Defendant's systems (the "Data Breach Incident").
6. Defendant was notified of the Data Breach Incident at least as early as July 25, 2023, but did not notify Plaintiff of the incident until February 14, 2024.
7. Plaintiff's PII that was acquired in the Data Breach Incident can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiff faces a lifetime risk of identity theft, which is heightened here by the theft of Plaintiff's Social Security Number.
8. Plaintiff's PII was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect Plaintiff's PII.
9. Until notified of the Data Breach Incident, Plaintiff had no idea Plaintiff's PII had been stolen, and that Plaintiff was, and continues to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for Plaintiff's lifetime.
10. Defendant disregarded Plaintiff's rights by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure Plaintiff's PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff was compromised through access to and exfiltration by an unknown and unauthorized third party.

11. Defendant's failure to: (i) adequately protect Plaintiff's PII; (ii) warn of Defendant's inadequate information security practices; and (iii) effectively secure the equipment and database containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents amounts to negligence and violates state and federal.

12. Plaintiff has suffered actual and imminent injuries as a direct result of the Data Breach, including: (a) theft of PII; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of the Data Breach Incident; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach Incident; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft posed by personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damages to and diminution in value of personal data entrusted to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's PII against theft and not allow access and misuse of personal data by others; and (h) the continued risk to PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's PII, and, is entitled to damages.

13. Plaintiff has a continuing interest in ensuring that Plaintiff's information is and remains safe, and is entitled to injunctive and other equitable relief.

PARTIES

14. Plaintiff is, and at all times relevant hereto was, a citizen and resident of Hillsborough County, Florida.

15. Defendant is, and at all times relevant hereto was, duly licensed to transact business in the State of Florida. Defendant does business, has offices, and/or maintains agents for the transaction of its customary business in Hillsborough County, Florida.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction pursuant to Fla. Stat. § 26.012(2). This is an action for equitable relief and damages, the sum or value of which exceed $50,000.00 exclusive of interest, costs, and attorney's fees.

17. This Court has personal jurisdiction over Defendant under Florida Stat. § 48.193, because Defendant personally or through its agents operated, conducted, engaged in, or carried on a business or business venture in Florida; had offices in Florida; committed tortious acts in Florida; and/or breached a contract in Florida by failing to perform acts required by the contract to be performed in Florida.

18. Venue for this action is proper in this Court pursuant to Fla. Stat. § 47.051 because the cause of action accrued in this County.

FACTS

19. At the time of the Data Breach Incident, Defendant maintained Plaintiff's PII in its database and systems.

20. By obtaining, collecting, and storing Plaintiff's PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's PII from disclosure.

21. Plaintiff relied on Defendant to keep Plaintiff's PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

22. Defendant had a duty to adopt reasonable measures to protect Plaintiff's PII from involuntary disclosure to third parties.

23. Prior to the Data Breach Incident, Defendant should have (i) encrypted or tokenized the sensitive PII of Plaintiff, (ii) deleted such PII that it no longer had reason to maintain, (iii) eliminated the potential accessibility of the PII from the internet and its website where such accessibility was not justified, and (iv) otherwise reviewed and improved the security of its network system that contained the PII.

24. Prior to the Data Breach Incident, on information and belief, Defendant did not (i) encrypt or tokenize the sensitive PII of Plaintiff, (ii) delete such PII that it no longer had reason to maintain, (iii) eliminate the potential accessibility of the PII from the internet and its website where such accessibility was not justified, and/or (iv) otherwise review and improve the security of its network system that contained the PII.

25. On the dates detailed above, an intruder gained unauthorized access to Defendant's database, after which Defendant sent Plaintiff a form notice attempting to minimize the Data Breach Event, while admitting that sensitive PII had been compromised and stolen.

26. Contrary to the self-serving narrative in Defendant's form notice, Plaintiff's unencrypted information may end up for sale on the dark web and/or fall into the hands of companies that will use the detailed PII for targeted marketing without the approval.

27. Defendant failed to use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff.

28. Plaintiff has taken reasonable steps to maintain the confidentiality of Plaintiff's PII, relied on Defendant to keep Plaintiff's PII confidential and securely maintained, to use this

information for business purposes only, and to make only authorized disclosures of this information.

29. Defendant could have prevented the Data Breach Incident by properly securing and encrypting Plaintiff's PII, or Defendant could have destroyed the data, especially old data that Defendant had no legal right and/or responsibility to retain.
30. Defendant's negligence in safeguarding Plaintiff's PII is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data, especially in the sector in which Defendant operates.
31. The ramifications of Defendant's failure to keep secure Plaintiff's PII are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.
32. Social Security numbers, for example, are among the most sensitive kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.
33. Even more problematic, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.
34. The PII of Plaintiff was stolen to engage in identity theft and/or to sell it to criminals who will purchase the PII for that purpose.
35. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used.

36. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding Plaintiff's PII, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff as a result of a breach.

37. Plaintiff now faces a lifetime of constant surveillance of financial and personal records, monitoring, and loss of rights. Plaintiff is incurring and will continue to incur such damages in addition to any fraudulent use of Plaintiff's PII.

38. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, potentially amounting to millions of individuals' detailed and confidential personal information and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

39. The injuries to Plaintiff were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Plaintiff's PII.

40. Plaintiff has suffered and will continue to suffer injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from Plaintiff's PII being placed in the hands of unauthorized third-parties and criminals.

41. Plaintiff has a continuing interest in ensuring that Plaintiff's PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

COUNT I – NEGLIGENCE AND NEGLIGENCE *PER SE*

42. Plaintiff re-alleges and incorporates the allegations contained in paragraphs 1-41 as if fully set forth herein.

43. Defendant was provided and entrusted with Plaintiff's PII.

44. Plaintiff entrusted Plaintiff's PII to Defendant on the premise and with the understanding that Defendant would safeguard the information, use the PII for business purposes only, and/or not disclose Plaintiff's PII to unauthorized third parties.
45. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff could and would suffer if the PII were wrongfully disclosed.
46. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of Plaintiff's PII involved an unreasonable risk of harm to Plaintiff, even if the harm occurred through the criminal acts of a third party.
47. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiff's information in Defendant's possession was adequately secured and protected.
48. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII it was no longer required to retain.
49. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's PII.
50. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff. That special relationship arose because Plaintiff entrusted Defendant with confidential PII, a necessary part of obtaining services from Defendant.
51. Defendant was subject to an independent duty, untethered to any contract between Defendant and Plaintiff.

52. A breach of security, unauthorized access, and resulting injury to Plaintiff was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

53. Plaintiff was a foreseeable and probable victim of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing Plaintiff's PII, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

54. Defendant's own conduct created a foreseeable risk of harm to Plaintiff. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach Incident as set forth herein. Defendant's misconduct also included its decision not to comply with industry standards for the safekeeping of Plaintiff's PII, including basic encryption techniques freely available to Defendant.

55. Plaintiff had no ability to protect Plaintiff's PII that was in, and remains in, Defendant's possession.

56. Defendant was in a position to protect against the harm suffered by Plaintiff as a result of the Data Breach Incident.

57. Defendant had and continues to have a duty to adequately disclose that the Plaintiff's PII within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of Plaintiff's PII by third parties.

58. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of Plaintiff's PII.

59. Defendant has admitted that Plaintiff's PII was wrongfully accessed by and exfiltrated by unauthorized third persons.

60. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding Plaintiff's PII during the time the PII was within Defendant's possession or control.

61. Defendant improperly and inadequately safeguarded Plaintiff's PII s in deviation of standard industry rules, regulations, and practices at the time of the Data Breach Incident.

62. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect Plaintiff's PII in the face of increased risk of theft.

63. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's PII.

64. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove Plaintiff's PII it was no longer required to retain.

65. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff the existence and scope of the Data Breach Incident.

66. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff, the PII of Plaintiff would not have been compromised.

67. There is a close causal connection between Defendant's failure to implement security measures to protect Plaintiff's PII and the harm suffered or risk of imminent harm suffered by Plaintiff. Plaintiff's PII was accessed and exfiltrated as the proximate result of

Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

68. Additionally, Section 5 of the FTC Act prohibits "unfair ... practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

69. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff.

70. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se.*

71. Plaintiff is within the class of persons that the FTC Act was intended to protect.

72. The harm that occurred as a result of the Data Breach Incident is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff.

73. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff has suffered and will suffer injury, including but not limited to: (i) threat of identity theft; (ii) the compromise, publication, and/or theft of PII; (iii) out-of- pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of PII; (iv) lost opportunity costs associated with effort expended and the

loss of productivity addressing and attempting to mitigate the present and future consequences of the Data Breach Incident, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (v) costs associated with placing freezes on bank accounts and credit reports; (vi) the continued risk to PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect Plaintiff's PII; and (viii) present and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach Incident for the remainder of Plaintiff's life.

74. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff has suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

75. Additionally, as a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff has suffered and will suffer the continued risks of exposure of Plaintiff's PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the PII in its continued possession.

76. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff is at an increased risk of identity theft or fraud.

77. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff is entitled to and demands actual consequential, and nominal damages and injunctive relief.

COUNT II – VIOLATION OF THE FLORIDA UNFAIR AND DECEPTIVE TRADE PRACTICES ACT ("FDUTPA"), FLA. STAT. § 501.201 *ET SEQ.*

78. Plaintiff re-alleges and incorporates the allegations contained in paragraphs 1-41 as if fully set forth herein.

79. FDUTPA prohibits "unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce." Fla. Stat.§ 501.204.

80. Defendant engaged in the conduct alleged in this Complaint through transactions in and involving trade and commerce. Mainly, the Data Breach Incident occurred through the use of the internet, an instrumentality of interstate commerce.

81. While engaged in trade or commerce, Defendant violated FDUTPA, including, among other things, by:

    a. Failing to implement and maintain appropriate and reasonable security procedures and practices to safeguard and protect Plaintiff's PII from unauthorized access and disclosure;

    b. Failing to disclose that its computer systems and data security practices were inadequate to safeguard and protect Plaintiff's PII from being compromised, stolen, lost, or misused; and

    c. Failing to disclose the Data Breach Incident to Plaintiff in a timely and accurate manner in violation of Fla. Stat. § 501.171.

82. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff's PII entrusted to it, and that risk of a data breach or theft was highly likely.

83. Defendant should have disclosed this information because they were in a superior position to know the true facts related to the defective data security.

84. Defendant's failures constitute false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiff) regarding the security of Defendant's network and aggregation of PII.

85. The representations upon which impacted individuals (including Plaintiff) relied were material representations (e.g., as to Defendant's adequate protection of PII), and consumers (including Plaintiff) relied on those representations to their detriment.

86. Defendant's actions constitute unconscionable, deceptive, or unfair acts or practices because, as alleged herein, Defendant engaged in immoral, unethical, oppressive, and unscrupulous activities that are and were substantially injurious to Plaintiff.

87. In committing the acts alleged above, Defendant engaged in unconscionable, deceptive, and unfair acts and practices acts by omitting, failing to disclose, or inadequately disclosing to Plaintiff that it did not follow industry best practices for the collection, use, and storage of PII.

88. As a direct and proximate result of Defendant's unconscionable, unfair, and deceptive acts and omissions, Plaintiff's PII was disclosed to third parties without authorization, which is causing and will continue to cause Plaintiff damages. Accordingly, Plaintiff is entitled to recover an order providing declaratory and injunctive relief and reasonable attorneys' fees and costs, to the extent permitted by law.

89. Also as a direct result of Defendant's knowing violation of the Florida Deceptive and Unfair Trade Practices Act, Plaintiff is entitled to injunctive relief, including, but not limited to:

a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Defendant segment Plaintiff's PII by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner Plaintiff's PII not necessary for provision of Defendant's services;

f. Ordering that Defendant conduct regular database scanning and securing checks;

g. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

h. Requiring Defendant to thoroughly and regularly evaluate any vendor's or third-party's technology that allows or could allow access to Plaintiff's PII and to promptly migrate to superior or more secure alternatives.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for the following relief:

a) Equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff;

b) Injunctive relief, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff, including but not limited to an order:

   i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

   ii. requiring Defendant to protect, including through encryption, all of Plaintiff's PII collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

   iii. requiring Defendant to delete, destroy, and purge Plaintiff's PII unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff;

   iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's PII;

   v. prohibiting Defendant from maintaining Plaintiff's PII on a cloud-based database;

   vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems that contain Plaintiff's PII on a periodic basis, and ordering Defendant to promptly

correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of its network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting Plaintiff's PII;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting PII;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess

whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate Plaintiff about the threats that it faces face as a result of the loss of Plaintiff's PII to third parties, as well as the steps Plaintiff's must take for protection those threats; and

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from its servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for Plaintiff, and to report any deficiencies with compliance of the Court's final judgment.

c) Declaring that Defendant violated the Florida Deceptive and Unfair Trade Practices Act;

d) For an award of damages, including actual, consequential, nominal damages, and statutory damages as allowed by law in an amount to be determined;

e) For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

f) For pre- and post- judgment interest on all amounts awarded; and

g) Such other and further relief as this Court may deem just and proper.

JURY DEMAND

Plaintiff hereby demand a trial by jury.

DATED: May 2, 2024

Respectfully submitted by:

/s/ *Benjamin W. Raslavich*

BENJAMIN W. RASLAVICH, ESQ.
Florida Bar No.: 0102808
KUHN RASLAVICH, P.A.
2110 West Platt Street
Tampa, Florida 33606
Telephone: (813) 422 - 7782
Facsimile: (813) 422 - 7783
Ben@theKRfirm.com
Counsel for Plaintiff