IN THE CIRCUIT COURT OF THE NINTH JUDICIAL CIRCUIT
IN AND FOR ORANGE COUNTY, FLORIDA
CIVIL DIVISION

JEREMIAH HUGHLEY, ANTHONY FURBUSH, LOGAN BERKOWITZ, BENJAMIN HELLER, and MAX PALOMBO individually and on behalf of all others similarly situated, Plaintiff, v. UNIVERSITY OF CENTRAL FLORIDA BOARD OF TRUSTEES, Defendant.	Case No. 2016-CA-001654-O **Jury Trial Demanded**

AMENDED CLASS ACTION COMPLAINT

Plaintiffs Jeremiah Hughley, Anthony Furbush, Logan Berkowitz, Benjamin Heller, and Max Palombo, bring this Amended Class Action Complaint ("Complaint") against Defendant University of Central Florida Board of Trustees, on behalf of themselves and all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiffs bring this class action against Defendant University of Central Florida Board of Trustees (referred to herein as "UCF" or "Defendant") for its failure to secure and safeguard personally identifiable information, including social security numbers, student identification numbers, student athletic information, student study and academic information, and other yet to be fully known sensitive identifiable student information and data, of past and present UCF employees and students, which UCF collected at the time Plaintiffs enrolled at UCF (collectively, "Private Information"), and for failing to provide timely, accurate and adequate

notice to Plaintiffs and other Class members that their Private Information had been stolen and precisely the scope and what types of information were stolen.

2. Beginning at a point in time presently unknown, hackers utilizing malicious malware accessed the computer systems at UCF and stole copies of past and present UCF employees' and students' Private Information. UCF failed to provide adequate computer and network security measures, which allowed for an intrusion in to UCF's computer network. Such failure resulted in the unauthorized access to personal, confidential and sensitive data of approximately 63,000 current and former students and employees. (the "Data Breach").

3. On February 4, 2016, UCF announced that it had discovered an unauthorized access of its computer system which resulted in the loss of Private Information of both present and former students and employees of the university. Specifically, it stated:

> Intrusion into UCF Network Involves Personal Data
>
> February 4, 2016
>
> Today I am sharing news that a recent outside intrusion into UCF's computer network compromised the personally identifiable information of some members of our university community.
>
> UCF discovered the unauthorized access in January. University officials reported the incident to law enforcement and launched an internal investigation with the assistance of a national digital forensics firm.
>
> To date, our investigation has indicated unauthorized access to Social Security numbers but not credit card information, financial records, medical records, or grades for approximately 63,000 current and former UCF students and staff and faculty members.
>
> We have launched this web page devoted to this incident that includes descriptions for the groups of current and former students and employees, as well as recommendations for how to best protect your identity.

> We have established a call center that you can contact at 877-752-5527 between 9 a.m. and 9 p.m. EST Monday through Friday if you have questions about this incident.
>
> Those who are affected will soon receive a letter by mail that explains how to sign up for one year of free credit monitoring and identity-protection services.
>
> Moving Forward
>
> Safeguarding your personal information is of the utmost importance at UCF. To ensure our vigilance, I have called for a thorough review of our online systems, policies and training to determine what improvements we can make in light of this recent incident.
>
> Every day, people and groups attempt to illegally access secure data from institutions around the world. Higher education institutions are popular targets.
> UCF will continue to work diligently to protect this important information from those who would break the law to get it.
>
> John C. Hitt
> President

4. UCF could have prevented this Data Breach. While many public entities, including universities, retailers, banks and credit card companies responded to recent breaches by adopting technology that helps make information in their respective possessions more secure, UCF has acknowledged that its systems was obviously lacking. The quality of the measures in place is suspect and the need for judicial intervention and consumer and independent oversight is mandated by the circumstances described herein. UCF's failure to maintain reasonable and adequate procedures to protect and secure Plaintiffs' and the Class Members' Private Information, and failure to provide Plaintiffs and the Class Members with timely notice of the Data Breach, has resulted in Plaintiffs and the Class being placed in danger of identity theft and other fraud and abuse.

5. UCF disregarded Plaintiffs' and Class members' rights by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected, failing to take available steps to prevent and stop the breach from ever happening, and failing to disclose to its employees and students the material facts that it did not have adequate computer systems and security practices to safeguard employees' and students' Private Information. On information and belief, Plaintiffs' and Class members' Private Information was improperly handled and stored, was unencrypted, and was not kept in accordance with applicable, required, and appropriate cyber-security protocols, policies, and procedures. As a result, Plaintiffs' and Class Members' Private Information was compromised and stolen, their privacy invaded, they have incurred or will incur out-of-pocket costs, and have otherwise suffered damages. However, as this same information remains stored in UCF's computer systems, Plaintiffs and Class Members have an interest in ensuring that their information is safe, and they should be entitled to seek injunctive and other equitable relief, including independent oversight of UCF's security systems.

PARTIES

6. Plaintiff, Jeremiah Hugely is a resident of the state of Florida. On February 4, 2016, Plaintiff contacted UCF and was informed that his Private Information had been hacked and stolen in the Data Breach. Plaintiff has taken steps to protect his identity and purchased identity theft protection at his own costs. The identity theft protection offered by Defendant is of lesser a quality and of too short a duration to provide adequate protection to him.

7. Plaintiff, Anthony Furbush, is a resident of the state of Florida. On February 4, 2016, Plaintiff Furbush contacted UCF and was informed that his Private Information had been hacked and stolen in the Data Breach. Plaintiff Furbush has taken steps to protect his identity and

purchased identity theft protection at his own costs. The identity theft protection offered by Defendant is of lesser a quality and of too short a duration to provide adequate protection to him.

8. Plaintiff, Logan Berkowitz, is a resident of the state of Florida. On February 4, 2016, Plaintiff Berkowitz contacted UCF and was informed that his Private Information had been hacked and stolen in the Data Breach. Plaintiff Berkowitz has taken steps to protect his identity and purchased identity theft protection at his own costs. The identity theft protection offered by Defendant is of lesser a quality and of too short a duration to provide adequate protection to him.

9. Plaintiff, Benjamin Heller, a resident of the state of North Carolina. Plaintiff Heller contacted UCF and was informed that his Private Information had been hacked and stolen in the Data Breach. Plaintiff Heller has taken steps to protect his identity by enrolling in the program offered by Defendant. However, the identity theft protection offered by Defendant is of lesser a quality compared to many other programs that Plaintiff Heller was unable to afford and of too short a duration to provide adequate protection to him.

10. Plaintiff, Max Palombo, is a resident of the state of Florida. Plaintiff Palombo contacted UCF and was informed that his Private Information had been hacked and stolen in the Data Breach. However, before UCF notified Plaintiff Palombo of the breach, but after the breach had occurred, Plaintiff Palombo learned that his Personal Information had been stolen and various fraudulent credit cards were opened in his name. Plaintiff Palombo spent countless hours on the telephone with the various credit card issues and credit reporting agencies, as well as law enforcement. As a result of the fraudulent accounts being opening, Plaintiff Palombo's credit profile was frozen, and his credit score materially dropped. Additionally, Plaintiff Palombo was unable to timely secure and activate credit monitoring as a result of the fraud notice placed on his credit profile. Plaintiff Palombo's efforts to repair his credit are on-going. Plaintiff Palombo has

taken steps to protect his identity and purchased identity theft protection at his own costs. The identity theft protection offered by Defendant is of lesser a quality and of too short a duration to provide adequate protection to him.

11. UCF is an American public research university in Orlando, Florida. It is the largest university in the United States by undergraduate enrollment, and the second largest by total enrollment. Founded in 1963, UCF opened with a mission of providing personnel to support the U.S. space program at the Kennedy Space Center and Cape Canaveral Air Force Station on Florida's Space Coast. As its academic scope surpassed this original focus on engineering and technology, however, it was renamed from Florida Technological University to the University of Central Florida in 1978. Enrollment today amounts to some 60,821 students from 140 countries and all 50 states, including Washington, D.C. The majority of the student population is located on the university's main campus just 13 miles (21 km) east-northeast of downtown Orlando, and 55 miles (89 km) southwest of Daytona Beach. The university offers over 200 degrees through thirteen colleges and twelve satellite campuses in Central Florida. Since its founding, UCF has awarded almost 280,000 degrees, including 50,000 graduate and professional degrees, to over 240,000 alumni worldwide. UCF is ranked as one of the "Most Innovative" universities by *U.S. News & World Report*, a best-value university by The Princeton Review and *Kiplinger's*, and one of the nation's most affordable colleges by *Forbes*.[1]

JURISDICTION AND VENUE

12. This Court has jurisdiction over this action as the amount in controversy exceeds $15,000.00.

[1] *See* UCF Website, available at http://www.ucf.edu/about-ucf/ (last visited Feb. 4, 2016).

13. Venue is proper in this Circuit because, as alleged in this Complaint, Defendant conducted and transacted business in this Circuit, and a substantial portion of the events and conduct giving rise to the violations complained of in this action occurred in this Circuit.

FACTUAL BACKGROUND

A. UCF's Privacy Policies

14. As one of the most technologically advanced public universities in the nation, UCF obtained and stored its students' and employees' personal, identifiable information, on its computers and servers. Recognizing the sanctity of this information, UCF maintains and represents that the privacy of its students and employees is important. It maintains an Identity Theft Prevention Program pursuant to the Federal Trade Commission's Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. A fully copy of this policy is attached as Exhibit A.

15. The UCF Division of Information Technologies & Resources, Information Security Office is responsible for computer system security of restricted personal information.

16. UFC policy defines restricted personal information as a person's first name or first initial and last name in combination with data elements such as Social Security number when the data elements are *not encrypted.*

17. If a data security breach of restricted personal data (or Personal Information) stored on the UCF computer system is suspected, the College, Department of Business Unit responsible for the affected data is to immediately inform the Information Security Office and the Security Incident Response Team assigned to the breach.

18. The Information Security Office then reports the breach to the Vice Provost for Information Technology and Resources, which in turn notifies the UCF executives (President, Vice Presidents and General Counsel's Office, etc.

19. The UCF executives then determine whether the breach involves the acquisition of personal information by an unauthorized person and whether to notify persons affected.

20. The UCF policy notes that Florida state statutes define security "breach" and "breach of the security of the system" as "the unlawful and unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the person [UCF]."

21. The procedures for notice of a data security breach include, press release, posting on a UCF website and U.S. mail.

B. "But he that filches from me my good name / robs me of that which not enriches him and makes me poor indeed." - Shakespeare, Othello, Act III, Scene 3.

22. It is well known and the subject of many media reports that Private Information data is highly coveted and a frequent target of hackers, as it was here, for exploitation and misuse for the monetary gain of the hackers. Private Information data is often easily taken because it may be less protected and regulated than payment card data. UCF acknowledges the sensitivity of Private Information and states that it is committed to ensuring the privacy of confidential information it collects and maintains on students, employees, and others. It further acknowledges that Social Security Numbers are sensitive data that are required by many university business processes but whose misuse or inadvertent disclosure can pose privacy risks to individuals as well as compliance or reputational risks to the university. It states that it is UCF's policy to request and use Social Security numbers only as required for the performance of the university's duties and responsibilities and to secure this information from inappropriate release or

disclosure. A copy of this policy is attached as Exhibit B. Despite the frequent public announcements of data breaches, UCF opted to maintain an insufficient and inadequate system to protect the Private Information of Plaintiffs and Class Members.

23. Legitimate organizations and the criminal underground alike recognize the value in Private Information. Otherwise, they would not aggressively seek or pay for it. For example, in "one of 2013's largest breaches . . . not only did hackers compromise the [card holder data] of three million customers, they also took registration data from 38 million users."[2] Similarly, in the Target data breach, in addition to payment card information (PCI) data pertaining to 40,000 credit and debit cards, hackers stole Private Information pertaining to 70,000 customers.

24. Biographical data is also highly sought after by data thieves. "Increasingly, criminals are using biographical data gained from multiple sources to perpetrate more and larger thefts." *Id*. Private Information has been stolen and sold by the criminal underground on many occasions in the past, and the accounts of thefts and unauthorized access have been the subject of many media reports. One form of identity theft has been branded as "synthetic identity theft," and occurs when thieves create new identities by combining real and fake identifying information then using those identities to open new accounts. "This is where they'll take your Social Security number, my name and address, someone else's birthday and they will combine them into the equivalent of a bionic person," said Adam Levin, chairman of IDT911, which helps businesses recover from identity theft. Synthetic identity theft is harder to unravel than traditional identity theft: "It's tougher than even the toughest identity theft cases to deal with because they can't necessarily peg it to any one person," Levin said. In fact, the fraud might not

[2] Verizon 2014 PCI Compliance Report, available at <http://www.nocash.info.ro/wp-content/uploads/2014/02/ Verizon_pci-report-2014.pdf> (hereafter "2014 Verizon Report"), at 54 (last visited Sept. 24, 2014).

be discovered until an account goes to collections and a collection agency researches the Social Security number.

25. Unfortunately, and as is alleged below, despite all of this publicly available knowledge of the continued compromises of Private Information in the hands of other third parties, such as retailers, UCF's approach at maintaining the privacy of Plaintiffs' and Class Members' Private Information was lackadaisical, cavalier, reckless, or at the very least, negligent. In fact, UCF was aware that they did not have the proper safeguards in place and that continued data breaches was expected.

26. On January 15, 2015, the Information Security Office at UCF, issued an internal report titled Security Incident Report for Year End 2014 ("2014 Report"). This report outlines how many security incidents occurred from 2007-2014; what types of incidents occurred; how many data security breaches occurred from 2007-2014; which systems were successfully attacked and the impact that the incidents have.

27. According to the 2014 Report, security incidents were at an all-time high and the report noted that "[a]n increase in account compromises and improved reporting capabilities account for the higher than average number of incidents in 2014. SIRT predicts this will become the 'new normal'."

28. The 2014 Report further stated that Account compromises increased 8% and system compromises increased 4% during mid-2014 to the end of 2014. Specifically with respect to data breaches, the 2014 Report stated that :

> Most known UCF data breaches occur due to human error. Without enterprise content checking precautions (Data Loss Prevention or "DLP" for short), SIRT anticipates the number of data breaches to remain consistent.

29. The 2014 Report indicated that at the last SIRT committee meeting, it was discussed to recommend the purchase of a "security awareness module with multiple delivery methods and learning metrics." Apparently this was never purchased since the report states that "SIRT recommends continuing this discussion".

30. Finally, the 2014 Report acknowledged that UCF needs better intrusion/prevention sensors. The report stated:

> Third party detection is up 20% this year which is typical with industry averages. SIRT hopes the 2015 Security Incident and Event Management (SIEM) project will positively impact the "IT noticed" category, however, better intrusion/prevention sensors are needed.

31. Despite the vulnerabilities revealed by these reports, Defendant ignored the recommendations and the warning contained in the reports.

C. The 2016 Data Breach at UCF

32. As set forth above, on February 4, 2016, UCF disclosed on its website that it had discovered a data breach. The UCF President's letter is set forth above.

33. Additional information revealed by UCF to date establishes that the Data Breach centered around two main groups of individuals: (1) current and former UCF student-athletes as well as student staff members, such as managers, supporting UCF teams (Group 1), and (2) current and former university employees in a category known as OPS, or Other Personal Services, which includes undergraduate student employees (including those in work-study positions), graduate assistants, housing resident assistants, adjunct faculty instructors, student government leaders and faculty members who have been paid for dual compensation/overload (for example, teaching additional classes) (Group 2).[3]

[3] *See* University of Central Florida, Data Security, *Intrusion into UCF Network Involves Personal Data* (Feb. 4, 2016), http://www.ucf.edu/datasecurity/ (last visited Feb. 16, 2016).

34. For those individuals in Group 1, disclosed data included first and last names, Social Security numbers, student ID numbers, sport, whether they were walk-ons or recruited, and number of credit hours taken and in progress. Group 2 disclosures included first and last names, Social Security numbers and UCF-issued Employee Identification Numbers. *Id.*

35. Nonetheless UCF has failed to provide a cogent picture of how the Data Breach occurred and its full effects on Plaintiffs' and Class Members' Private Information.

36. A UCF Police Department Incident Report, case number 2016-0534, dated February 2, 2016 ("Police Report"), and subsequently posted on a UCF webpage, www.ucf.edu/datasecurity/, states that "In January 2016, UCF discovered a recent intrusion into UCF's computer network which compromised the [PII] of come members of the [UCF] Community." The Police Report indicates that the intrusion occurred *throughout the month of January*. The Police Report further states that UCF commenced an investigation and that law enforcement officials were currently investigating the source of the intrusion.

37. There has been no announcement by UCF that its investigation is complete or that the estimated number of current and former UCF students and employees whose Personal Information was compromised will not rise as the investigation continues.

38. The Police Report states that disposition of the investigation remains "open."

39. A UCF posting on www.ucf.edu/datasecurity/ states "[w]e are mailing notices to individuals who may have been affected by the incident *so <u>they</u> can take steps to safeguard their personal information going forward*. (Emphasis added) UCF further warns:

> we recommend that you carefully check credit reports for accounts or inquiries you do not recognize. If you see anything you do not understand, call the credit agency immediately. If you find any suspicious activity on the credit reports, call your local police or sheriff's office, and file a police report for identity theft and get a

> copy of it. You may need to give copies of the police report to creditors to clear up credit records.
>
> We also recommend that you carefully review credit and debit card account statements as soon as possible in order to determine if there are any discrepancies or unusual activity listed. You should remain vigilant and continue to monitor statements for unusual activity going forward. If you see anything you do not understand or that looks odd, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued the credit or debit card immediately to let them know what happened.

40. UCF goes on to say in its web posting: "We regret any inconvenience or stress this incident may cause . . ." UCF says that it will use the intrusion of its students' and employees' PII as "an opportunity to educate our campus community about how to protect information and identities in a variety of online situations."

41. Hacking is often accomplished in a series of phases to include reconnaissance, scanning for vulnerabilities and enumeration of the network, gaining access, escalation of user, computer and network privileges, maintaining access, covering tracks and placing backdoors. On information and belief, hackers scoured UCF's networks to find a way to access Private Information that had been collected and accessed on its networks.

42. The Data Breach was caused and enabled by UCF's knowing violation of its obligations to abide by best practices and industry standards in protecting its employees' and students' Private Information, and its decision to ignore earlier reports of the weaknesses in its cyber security system. .

D. This Data Breach Will Result in Additional Identity Theft and Identify Fraud

43. UCF failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the data

breach. UCF's failure to provide adequate cyber security measures has resulted in the exposure of sensitive and highly confidential personal data.

44. The ramifications of UCF's failure to keep Plaintiffs' and Class members' Private Information data secure is severe.

45. According to a Social Security Administration ("SSA") pamphlet titled "Identity Theft and Your Social Security Number", your Social Security number is confidential. "The Social Security Administration protects your Social Security number and keeps your records confidential. We don't give your number to anyone, except when authorized by law. You should be careful about sharing your number, even when you're asked for it." The SSA pamphlet warns, "Be careful with your Social Security card and number. Keep your card and any other document that shows your Social Security number in a safe place.

46. The SSA pamphlet further states that a hacker that has obtained:

> your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.

47. Plaintiffs provided their Social Security numbers to UCF with the understanding and expectation that UCF would keep that Social Security number confidential.

48. The confidentiality of their Social Security numbers and other personal information had real economic value to Plaintiffs and Class Members.

49. In fact, stolen Social Security numbers, particularly when connected with a Social Security cardholder's name and other identifying information, have cash value on the black market.

50. Loss of confidentiality of one's Social Security number is a lifelong, expensive and potentially devastating problem.

51. In its article titled, "Here's Why Your Social Security Number Is Holy Grail for Hackers" Bloomberg Business reported that Social Security numbers issued by the U.S. government typically follow people from birth to death. Unlike payment-card numbers that can be canceled, a Social Security number is ubiquitous and hard to change. It is used as the main authentication mechanism for many essential services, especially ones provided by the government.

52. On February 11, 2015, National Public Radio reported that getting a new Social Security number requires a lot of paperwork, including evidence of problems caused by misuse. Even then, according to Julie Fergerson, chair of the Identity Theft Resource Center, a new number is not always helpful. "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number," she says. "So even when you go through the painful effort of doing it, it really doesn't help the victim of identity theft."

53. The information UCF compromised, including Plaintiffs' and Class Members' identifying information is "as good as gold" to identity thieves, in the words of the Federal Trade Commission ("FTC"). Identity theft occurs when someone uses another's personal identifying information, such as that person's name, address, credit card number, credit card expiration

dates, and other information, without permission, to commit fraud or other crimes. The FTC estimates that as many as 10 million Americans have their identities stolen each year.

54. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[4]

55. According to Javelin Strategy and Research, "1 in 4 data breach notification recipients became a victim of identity fraud."[5] Nearly half (46%) of consumers with a breached debit card became fraud victims within the same year.

56. Identity thieves can use personal information, such as that of Plaintiffs and Class Members, which UCF failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund. Some of this activity may not come to light for years. The IRS paid out 43.6 billion in potentially fraudulent returns in 2012, and the IRS identified more than 2.9 million incidents if identity theft in 2013. The IRS has described identity theft as the number one tax scam for 2014.

E. Annual Monetary Losses From Identity Theft Are In The Billions Of Dollars.

57. Javelin Strategy and Research reports that those losses increased to $21 billion in 2013.[6] There may be a time lag between when harm occurs versus when it is discovered, and

[4] FTC, Signs of Identity Theft, available at <http://www.consumer.ftc.gov/articles/ 0271-signs-identity-theft> (last visited Sept. 24, 2014).

[5] *See* 2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters, available at <www.javelinstrategy.com/brochure/ 276> (last visited Sept. 24, 2014) (the "2013 Identity Fraud Report").

also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[7]

58. It is incorrect to assume that reimbursing a consumer for a financial loss due to fraud makes that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."[8] In fact, the BJS reported, "resolving the problems caused by identity theft [could] take more than a year for some victims." *Id*. at 11.

F. Plaintiffs and Class Members Suffered Damages

59. The Data Breach was a direct and proximate result of UCF's failure to properly safeguard and protect Plaintiffs' and Class Members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including UCF's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class Members' Private Information to protect against reasonably foreseeable threats to the security or integrity of such information.

---

[6] *See* 2013 Identity Fraud Report.

[7] GAO, Report to Congressional Requesters, at p.33 (June 2007), available at <http://www.gao.gov/new.items/d07737.pdf> (emphases added) (last visited Sept. 24, 2014).

[8] Victims of Identity Theft, 2012 (Dec. 2013) at 10, available at <http://www.bjs.gov/content/pub/pdf/vit12. pdf> (last visited Sept. 24, 2014).

60. Plaintiffs' and Class Members' Private Information is private and sensitive in nature and was left inadequately protected by UCF. UCF did not obtain Plaintiffs' and Class Members' consent to disclose their Private Information to any other person as required by applicable law and industry standards.

61. As a direct and proximate result of UCF's wrongful actions and inaction and the resulting Data Breach, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports and accounts and IRS returns for unauthorized activity.

62. UCF's wrongful action and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class Members' Private Information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of their Private Information;

b. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Private Information being placed in the hands of criminals and already misused via the sale of Plaintiffs' and Class Members' information on the Internet black market;

c. the untimely and inadequate notification of the Data Breach;

d. the improper disclosure of their Private Information;

e. loss of privacy;

f. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

g. ascertainable losses in the form of deprivation of the value of their Private Information, for which there is a well-established national and international market;

h. deprivation of rights they possess under the Florida Deceptive and Unfair Trade Practices Act (FDUTPA); and

i. Plaintiffs' economic injury is also described above.

63. Moreover, this breakdown in UCF's protection of online systems, policies and training resulted in the breach of protected student and education records protected by The Federal Educational Rights and Privacy Act ("FERPA") (20 U.S.C. § 1232g; 34 CFR Part 99). FERPA protects the privacy of student education records.

64. FERPA's protections are reinforced under Florida law, which requires all public postsecondary institutions to comply with the FERPA. See Fla. Stat. § 1002.225. UCF's failure to protect Plaintiffs' and the Class Members' protected educational records entitles them to an immediate right of action to enforce their rights by injunction.

65. Acknowledging the repercussions from its wrongful actions and inaction and the resulting Data Breach, UCF has offered its employees and students only one year of credit monitoring and identity theft protection services and also a low quality one, despite the fact that it is well known, and acknowledged by government that damage and fraud from a data breach can take years to occur. UCF has instead opted to save the cost of such services to ensure its

revenues remain essentially unaffected by limiting this protection to only one year. As a result, Plaintiffs and Class Members are left to their own actions to protect themselves from the financial carnage UCF has allowed to occur. The additional cost of adequate and appropriate coverage, or insurance, against the losses and exposure that UCF has placed Plaintiffs and Class Members in, is ascertainable and is a determination appropriate for the trier of fact. UCF has also not offered to cover any of the damage sustained by Plaintiffs or Class Members.

66. While the Private Information of Plaintiffs and members of the Class has been stolen, the same or a copy of the Private Information continues to be held by UCF. Plaintiffs and members of the Class have an undeniable interest in insuring that this information is secure, remains secure, and not subject to further theft.

CLASS ACTION ALLEGATIONS

67. Plaintiffs seek relief in their individual capacity and as representatives of all others who are similarly situated. Pursuant to Florida Rules of Civil Procedure 1.220(a) (b)(2), and (b)(3) Plaintiffs seek certification of a Nationwide class and a Florida class. The national class is initially defined as follows:

> **All persons residing in the United States whose personal information was disclosed in the data breach affecting UCF in 2016 (the "Nationwide Class").**

68. The Florida Class is initially defined as follows:

> **All persons residing in Florida whose personal information was disclosed in the data breach affecting UCF in 2016 (the "Florida Class").**

69. Excluded from each of the above Classes are UCF, including any entity in which UCF has a controlling interest, as well as successors and assigns of UCF. Also excluded are the judges and court personnel in this case and any members of their immediate families.

70. **Numerosity**. Fla R. Civ. P. 1.220(a)(1). The members of the Class are so numerous that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiffs at this time, UCF has acknowledged that the Private Information of approximately 63,000 individuals was affected by the breach, and cannot be contested that Defendants' records contain information of not only the names and contact information of the persons whose information was stolen, but also what information for each person was stolen.

71. **Commonality**. Fla. R. Civ. P. 1.220(a)(2) and (b)(3). There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether UCF violated the Florida Deceptive and Unfair Trade Practices Act (FDUTPA) by failing to implement reasonable security procedures and practices;

b. Whether UCF violated FDUTPA by failing to promptly notify class members their Private Information had been compromised;

c. Whether class members may obtain injunctive relief against UCF under FDUTPA to require that it safeguard, or destroy rather than retain the Private Information of Plaintiffs and Class Members;

d. What security procedures and data-breach notification procedures UCF should be required to implement as part of any injunctive relief ordered by the Court;

e. Whether UCF has an implied contractual obligation to use reasonable security measures;

f. Whether UCF has complied with any implied contractual obligation to use reasonable security measures;

g. What security measures, if any, must be implemented by UCF to comply with its implied contractual obligations;

h. Whether UCF violated FDUTPA in connection with the actions described herein;

i. The nature of the relief, including equitable relief, to which Plaintiffs and the Class Members are entitled;

j. Whether UCF had a duty to protect Plaintiffs' and Class Members' Personal Information; and

k. Whether UCF breached any such duty to protect Plaintiffs' and Class Members' Personal Information.

72. All members of the purposed Classes are readily ascertainable. UCF has access to addresses and other contact information for tens of thousands of members of the Classes, which can be used for providing notice to many Class members.

73. **Typicality.** Fla.. R. Civ. P. 1.220(a)(3). Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' information, like that of every other class member, was misused and/or disclosed and/or unsecured by UCF.

74. **Adequacy of Representation.** Fla. R. Civ. P. 1.220(a)(4). Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions, including privacy litigation.

75. **Superiority of Class Action.** Fla. R. Civ. P. 1.220(b)(3). A class action is superior to other available methods for the fair and efficient adjudication of this controversy

since joinder of all the members of the Class is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

76. Damages for any individual class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class treatment, UCF's violations of law inflicting substantial damages in the aggregate would go un-remedied without certification of the Class.

77. Class certification is also appropriate under Fla. R. Civ. P. 1.220(a) and (b)(2), because UCF has acted or has refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

COUNT I
Breach of Contract
(On Behalf of Plaintiffs and the Nationwide Class)

78. Plaintiffs incorporate the substantive allegations contained in Paragraphs 1 through 77 as if fully set forth herein.

79. UCF solicited and invited Plaintiffs and Class Members to enroll or apply for employment at its facility. Plaintiffs and Class members accepted UCF's offers and provided their Private Information during the period of the Data Breach.

80. When Plaintiffs and Class Members enrolled or applied to enroll at UCF, or sought and/or obtained employment with UCF, they provided their Private Information. In so doing, Plaintiffs and Class Members entered into contracts with UCF pursuant to which UCF, including but not limited to the Policies attached as Exhibit's A and B, pursuant to which UCF

agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and Class Members if their data had been breached and compromised.

81. Plaintiffs and Class Members would not have provided and entrusted their Private Information, to UCF in the absence of the implied contract between them and UCF.

82. Plaintiffs and Class Members fully performed their obligations under the contracts with UCF.

83. UCF breached the contracts it made with Plaintiffs and Class Members by failing to safeguard and protect the Private Information of Plaintiffs and Class Members and by failing to provide timely and accurate notice to them that their Private Information was compromised in and as a result of the Data Breach.

84. As a direct and proximate result of UCF's breaches of the contracts between UCF and Plaintiffs and Class Members, Plaintiffs and Class Members sustained actual losses and damages as described above.

COUNT II
Negligence
(On Behalf of Plaintiffs and the Nationwide Class)

85. Plaintiffs repeat and fully incorporate the allegations contained in paragraphs 1 through 77 as if fully set forth in this Count.

86. Upon accepting and storing Plaintiffs' and Class Members' Private Information in their respective computer database systems, UCF undertook and owed a duty to Plaintiffs and Class Members to exercise reasonable care to secure and safeguard that information and to utilize commercially reasonable methods to do so. UCF knew, acknowledged, and agreed that the Private Information was private and confidential and would be protected as private and confidential.

87. The law imposes an affirmative duty on UCF to timely disclose the unauthorized access and theft of the Private Information to Plaintiffs and the Class so that Plaintiffs and Class Members could take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Private Information.

88. UCF breached its duty to notify Plaintiffs and Class Members of the unauthorized access by waiting an unreasonable amount of time after learning of the breach to notify Plaintiffs and Class Members and then by failing to provide Plaintiffs and Class Members with sufficient information regarding the breach until February 2016. To date, UCF has not provided sufficient information to Plaintiffs and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiffs and the Class.

89. Moreover, upon information and belief, UCF's method of providing notice to affected individuals was to mail letters to former students' and employees' addresses on file when they last attended the university, majority of which are outdated and no longer accurate. Therefore, a significant portion of the members of the Class are yet to receive notification of the breach, and as a result, are unaware that they must take protective measures to safeguard their compromised information.

90. Although the scope of injury flowing from this breach affects former students nationwide, the breach had a substantial effect in Florida, as approximately 55,000 out of the 63,000 individuals affected by the breach reside in Florida.

91. UCF also breached its duty to Plaintiffs and the Class Members to adequately protect and safeguard this information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information. Furthering its dilatory practices, UCF failed to provide adequate

supervision and oversight of the Private Information with which it is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a third party to gather Plaintiffs' and Class Members' Private Information, misuse the Private Information and intentionally disclose it to others without consent.

92. Through UCF's acts and omissions described in this Complaint, including UCF's failure to provide adequate security and its failure to protect Plaintiffs' and Class Members' Private Information from being foreseeably captured, accessed, disseminated, stolen and misused, UCF unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiffs' and Class Members' Private Information during the time it was within UCF's possession or control.

93. Further, through its failure to provide timely and clear notification of the Data Breach to consumers, UCF prevented Plaintiffs and Class Members from taking meaningful, proactive steps to secure their financial data and bank accounts.

94. Upon information and belief, UCF improperly and inadequately safeguarded Private Information of Plaintiffs and Class Members in deviation from standard industry rules, regulations, and practices at the time of the unauthorized access.

95. UCF's failure to take proper security measures to protect Plaintiffs' and Class Members' sensitive Private Information as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiffs' and Class Members' Private Information.

96. UCF's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the Private Information; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of

persons having access to Plaintiffs' and Class Members' Private Information; and failing to provide Plaintiffs and Class Members with timely and sufficient notice that their sensitive Private Information had been compromised.

97. Neither Plaintiffs nor the other Class Members contributed to the data breach and subsequent misuse of their Private Information as described in this Complaint.

98. As a direct and proximate cause of UCF's conduct, Plaintiffs and the Class Members are now exposed to damages including, but not limited to the types of damages alleged above which arise from the misuse of fraudulently obtained Private Information of Plaintiffs and Class Members and/or filing false tax returns; and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse, and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

COUNT III
Violations of Florida's Unfair and Deceptive Trade Practices Act
(On behalf of Plaintiffs and the Florida Class)

99. Plaintiffs repeat and incorporates the allegations contained in paragraphs 1 through 77 as if fully set forth in this Count.

100. The Florida Deceptive and Unfair Trade Practices Act (hereinafter "FDUTPA") is expressly intended to protect "consumers" like Plaintiffs and Class Members from unfair or deceptive trade practices.

101. Plaintiffs and Class Members have a vested interest in the privacy, security and integrity of their Private Information, therefore, this interest is a "thing of value" as contemplated by FUDTPA.

102. UCF is a "person" within the meaning of the FDUTPA and, at all pertinent times, was subject to the requirements and proscriptions of the FDUTPA with respect to all of their business and trade practices described herein.

103. Plaintiffs and Class Members are "consumers" "likely to be damaged" by UCF's ongoing deceptive trade practices.

104. Plaintiffs and Class Members have a vested interest in the privacy, security and integrity of their Private Information, therefore, this interest is a "thing of value" as contemplated by FDUTPA.

105. Plaintiffs and Class Members are "consumers" "likely to be damaged" by Defendant's ongoing deceptive trade practices.

106. UCF's unlawful conduct as described in this Complaint, was facilitated, directed, and emanated from UCF to the detriment of Plaintiffs and Class Members.

107. UCF engaged in unfair and deceptive trade practices by holding itself out as providing a secure environment and by actively promoting trust online with its employees and students, which created in their minds a reasonable expectation of privacy to all consumers by promising that consumers' Private Information is safe with UCF, but then failed to take commercially reasonable steps to protect the Private Information with which it is entrusted.

108. UCF violated FDUTPA by failing to properly implement adequate, commercially reasonable security measures to protect consumers' sensitive Private Information.

109. UCF also violated FDUTPA by failing to immediately notify Plaintiffs and affected Class Members of the nature and extent of the Data Breach.

110. UCF's acts, omissions, and conduct also violate the unfair component of FDUTPA because UCF's acts, omissions and conduct, as alleged herein, offended public policy

and constitute immoral, unethical, oppressive, and unscrupulous activities that caused substantial injury, including to Plaintiffs and other Class members. The gravity of UCF's conduct outweighs any potential benefits attributable to such conduct and there were reasonably available alternatives to further UCF legitimate business interests, other than UCF's conduct described herein.

111. UCF failed to properly implement adequate, commercially reasonable security measures to hold this information in strict confidence, failed to safeguard Plaintiffs' and Class Members' Private Information, and failed to protect against the foreseeable loss and misuse of this information.

112. Plaintiffs and Class Members have suffered ascertainable losses as a direct result of UCF's employment of unconscionable acts or practices, and unfair or deceptive acts or practices.

113. By failing to disclose that it does not enlist industry standard security practices, which render UCF particularly vulnerable to data breaches, UCF engaged in a deceptive business practice that is likely to deceive a reasonable consumer.

114. A reasonable consumer would not have provided their Private Information to UCF had he known the truth about UCF's security procedures. By withholding material information about its security practices, UCF was able to convince employees and students to provide and entrust their Private Information to UCF. Had Plaintiffs known truth about UCF's security procedures, they would not have entrusted their Private Information with UCF.

115. UCF's failure to disclose that it does not enlist industry standard security practices also constitutes an unfair business practice under the FDUTPA. UCF's conduct is unethical, unscrupulous, and substantially injurious to the Florida Class.

116. As a result of UCF's violations of the FDUTPA, Plaintiffs and the other members of the Florida class are entitled to injunctive relief including, but not limited to: (1) ordering that UCF utilize strong industry-standard encryption algorithms for encryption keys that provide access to stored data; (2) ordering that UCF implement the use of its encryption keys in accordance with industry standards; (3) ordering that UCF, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests and audits on UCF systems on a periodic basis; (4) ordering that UCF engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (5) ordering that UCF audit, test and train its security personnel regarding any new or modified procedures; (6) ordering that UCF, consistent with industry standard practices, segment consumer data by, among other things, creating firewalls and access controls so that if one area of UCF is compromised, hackers cannot gain access to other portions of UCF's systems; (7) ordering that UCF purge, delete, destroy in a reasonable secure manner data not necessary; (8); ordering that UCF, consistent with industry standard practices, conduct regular database scanning and security checks; (9) ordering that UCF, consistent with industry standard practices, evaluate web applications for vulnerabilities to prevent web application threats to employees and students at UCF; (10) ordering that UCF, consistent with industry standard practices, periodically 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; and (11) ordering UCF to meaningfully educate its employees and students about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps UCF employees and students must take to protect themselves.

117. As a result of UCF's violations of the FDUTPA, Plaintiffs and Class Members have suffered injury in fact, as detailed above.

118. Under FDUPTA, Plaintiffs and the Class are entitled to preliminary and permanent injunctive relief without proof of monetary damage, loss of profits, or intent to deceive. Plaintiffs and the Class seek equitable relief and to enjoin UCF on terms that the Court considers appropriate.

119. UCF's conduct caused and continues to cause substantial injury to Plaintiffs and Class Members. Unless preliminary and permanent injunctive relief is granted, Plaintiffs and the Class will suffer harm, Plaintiffs and the Class Members do not have an adequate remedy at law, and the balance of the equities weighs in favor of Plaintiffs and the Class.

120. At all material times, UCF's deceptive trade practices are willful within the meaning of FDUTPA and, accordingly, Plaintiffs and the Class are entitled to an award of attorneys' fees, costs and other recoverable expenses of litigation.

COUNT IV
Violations of Florida Statute, Section 1002.225
(On behalf of Plaintiffs and the Florida Class)

121. Plaintiffs repeat and incorporates the allegations contained in paragraphs 1 through 77 as if fully set forth in this Count.

122. This breakdown in UCF's protection of online systems, policies and training resulted in the breach of protected student and education records protected by The Federal Educational Rights and Privacy Act ("FERPA") (20 U.S.C. § 1232g; 34 CFR Part 99). FERPA protects the privacy of student education records.

123. Florida Statute, section 1002.225 requires that all public postsecondary institutions comply with the FERPA.

124. UCF had a duty to secure and safeguard the personal information of its students and former students pursuant to FERPA and other state law.

125. At all times material hereto, UCF warranted that it would comport with its duties under FERPA.

126. Defendant violated FERPA and state law by failing to secure and safeguard the personal educational records belonging to Plaintiffs and other Class Members.

127. The records accessed and comprised as a result of the breach constitute educational records under FERPA.

128. UCF had a duty under FERPA to timely notify Plaintiffs and the Class.

129. UCF violated FERPA and state law by allowing for the breach of Plaintiffs' and the Class Members' educational records.

130. Plaintiffs and the Class Members have suffered damages as a result of UCF's FERPA and state law violations. As a direct and proximate result of UCF's conduct, Plaintiffs and the Class Members have suffered damages in the past and will suffer future damages,

131. UCF's failure to protect Plaintiffs' and the Class Members' protected educational records entitles them to an immediate right of action to enforce their rights by injunction.

132. Plaintiffs and the Class Members are entitled to be awarded attorney's fees and costs in enforcing their rights pursuant to Florida Statute, section 1002.225(3).

COUNT V
Negligence *Per Se*

133. Plaintiffs repeat and fully incorporate the allegations contained in paragraphs 1 through 77 as if fully set forth in this count.

134. Pursuant to FERPA (20 U.S.C. § 1232g; 34 CFR Part 99), Defendant had a duty to keep and protect the Private Information of the Plaintiffs and other members of the Class.

135. Defendant violated FERPA by failing to adequately protect and maintain the confidentiality of Plaintiffs' and Class Members' Private Information.

136. Defendant's failure to comply with the FERPA, and/or other industry standards and regulations, constitutes negligence per se.

137. Defendant's negligence per se has caused damage to Plaintiffs and Class

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all Class Members proposed in this Complaint, respectfully requests that the Court enter judgment in their favor and against UCF for each of the above Counts, as follows:

A. For an Order certifying the Nationwide Class and Florida Class as defined herein, and appointing Plaintiffs and their Counsel to represent the Nationwide Class and Florida Class;

B. For equitable relief enjoining UCF from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to the Plaintiffs and Class Members;

C. For equitable relief compelling UCF to utilize appropriate methods and policies with respect to consumer data collection, storage and safety and to disclose with specificity to Class Members the type of Private Information compromised.

D. For an award of actual damages, in an amount to be determined;

E. For an award of costs of suit and attorneys' fees, as allowable by law; and

F. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiffs demand a jury trial on all issues so triable.

Dated: March 28, 2017

Respectfully submitted,

/S/ John A. Yanchunis
John A. Yanchunis
Florida Bar No. 324681
Marcio W. Valladares
Florida Bar No. 986917
Patrick A. Barthle, II
Florida Bar No. 99286
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402
jyanchunis@ForThePeople.com

Joshua H. Eggnatz, Esq.
Fla. Bar. No.: 0067926
Michael J. Pascucci, Esq.
Fla. Bar. No.: 83397
EGGNATZ, LOPATIN & PASCUCCI, LLP
5400 S. University Drive, Ste. 417
Davie, FL 33328
Tel: (954) 889-3359
Fax: (954) 889-5913
Mpascucci@ELPLawyers.com
JEggnatz@ELPLawyers.com

Melissa R. Emert. Esq.
Patrick K. Slyne, Esq.
(admitted pro hac vice)
STULL, STULL & BRODY
6 East 45th Street
New York, NY 10017
Tel. (212) 687-7230
Fax (212) 490-2022
memert@ssbny.com
pkslyne@ssbny.com

Attorneys for Plaintiffs
and the Proposed Class

EXHIBIT A

University of Central Florida

Office of the President

SUBJECT: Identity Theft Prevention	Effective Date: 08-24-11	Policy Number: 2-105.1	
	Supersedes: 2-105	Page 1	Of 8
	Responsible Authority: Vice President and General Counsel		

DATE OF INITIAL ADOPTION AND EFFECTIVE DATE: 06-24-09

APPLICABILITY/ACCOUNTABILITY:

This policy applies to all UCF faculty members, Administrative and Professional staff, University Support Personnel System employees, Other Personnel Services employees, and volunteers.

POLICY STATEMENT:

The University of Central Florida maintains an Identity Theft Prevention Program pursuant to the Federal Trade Commission's Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003.

DEFINITIONS:

Identity theft. A fraud committed or attempted using the identifying information of another person without authority.

Red flag. A pattern, practice, or specific activity that indicates the possible existence of identity theft.

Covered account. An account used mostly for personal, family, or household purposes, and that involves multiple payments or transactions. A covered account is also an account for which there is a foreseeable risk of identity theft.

Program administrator. The individual designated with primary responsibility for oversight of the identity theft prevention program.

Identifying information. Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including: name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien

registration number, government passport number, employer or taxpayer identification number, individual identification number, computer's Internet Protocol address, or routing code.

PROCEDURES:

I. Fulfilling Requirements of the Red Flags Rule

Under the Red Flags Rule, the university is required to establish an identity theft prevention program tailored to its size, complexity, and the nature of its operation. This program must contain reasonable policies and procedures to:

A. Identify relevant red flags for new and existing covered accounts and incorporate those red flags into the program.

B. Detect red flags that have been incorporated into the program.

C. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft.

D. Ensure the program is updated periodically to reflect changes in risks to individuals or to the safety and soundness of the individuals from identity theft.

II. Identification of Red Flags

In order to identify relevant red flags, the university considers the types of accounts that it offers and maintains, methods it provides to open its accounts, methods it provides to access its accounts, and its previous experiences with identity theft. The university identifies the following red flags in each of the listed categories:

A. Notifications and Warnings from Credit Reporting Agencies

1. Report of fraud accompanying a credit report.

2. Notice or report from a credit agency of a credit freeze on an applicant.

3. Notice or report from a credit agency of an active duty alert for an applicant.

4. Receipt of a notice of address discrepancy in response to a credit report request.

5. Indication from a credit report of activity that is inconsistent with an applicant's usual pattern or activity.

B. Suspicious Documents

1. Identification document or card that appears to be forged, altered, or inauthentic.

P.O. BOX 160002 • Orlando, FL 32816-0002 • (407) 823-1823 • FAX (407) 823-2264
An Equal Opportunity and Affirmative Action Institution

2. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document.

3. Other document with information that is not consistent with existing identifying information.

4. Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

1. Identifying information presented that is inconsistent with other information provided (example: inconsistent birth dates).

2. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a loan application).

3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent.

4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address).

5. Social security number presented that is the same as one given by another person.

6. An address or phone number presented that is the same as that of another person.

7. A person fails to provide complete personal identifying information on an application when reminded to do so.

8. A person's identifying information is not consistent with the information that is on file for that person.

D. Suspicious Covered Account Activity or Unusual Use of Account

1. Change of address for an account followed by a request to change the person's name.

2. Payments stop on an otherwise consistently up-to-date account.

3. Account used in a way that is not consistent with prior use.

4. Mail sent to the individual is repeatedly returned as undeliverable.

5. Notice to the university that a person is not receiving mail sent by the university.

6. Notice to the university that an account has unauthorized activity.

P.O. Box 160002 • Orlando, FL 32816-0002 • (407) 823-1823 • FAX (407) 823-2264
An Equal Opportunity and Affirmative Action Institution

7. Breach in the university's computer system security.

8. Unauthorized access to or use of student account information.

E. Alerts from Others

1. Notice to the university from an individual, identity theft victim, law enforcement official, or other person that the university has opened or is maintaining a fraudulent account for a person engaged in identity theft.

III. Detecting Red Flags

A. Enrollment

To detect any of the red flags identified above associated with the enrollment of an individual, university personnel will take the following steps to obtain and verify the identity of the person opening the account:

1. Require certain identifying information such as name, date of birth, academic records, home address, or other identification.

2. Verify the person's identity at time of issuance of identification card (review of driver's license or other government-issued photo identification).

B. Existing Accounts

To detect any of the red flags identified above for an existing covered account, university personnel will take the following steps to monitor transactions on an account:

1. Verify the identification of the individual if they request information (in person, via telephone, via facsimile, via email).

2. Verify the validity of requests to change billing addresses by mail or email and provide the individual a reasonable means of promptly reporting incorrect billing address changes.

3. Verify changes in banking information given for billing and payment purposes.

C. Consumer (Credit) Report Requests

To detect any of the red flags identified above for an employment or volunteer position for which a credit report is sought, university personnel will take the following steps to assist in identifying address discrepancies:

P.O. BOX 160002 • Orlando, FL 32816-0002 • (407) 823-1823 • FAX (407) 823-2264
An Equal Opportunity and Affirmative Action Institution

1. Require written verification from any applicant that the address provided by the applicant is accurate at the time the request for the credit report is made to the consumer reporting agency.

2. In the event that notice of an address discrepancy is received, verify that the credit report pertains to the applicant for whom the requested report was made and report to the consumer reporting agency an address for the applicant that the university has reasonably confirmed is accurate.

IV. Preventing and Mitigating Identity Theft

In the event that university personnel detect any identified red flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the red flag:

A. Prevent and Mitigate

1. Continue to monitor a covered account for evidence of identity theft.

2. Contact the individual (for which a credit report was run).

3. Change any passwords or other security devices that permit access to covered accounts.

4. Not open a new covered account.

5. Provide a new identification number.

6. Notify the program administrator for determination of the appropriate step(s) to take.

7. Notify law enforcement.

8. File or assist in filing a Suspicious Activities Report.

9. Determine that no response is warranted under the particular circumstances.

B. Protect Identifying Information

In order to further prevent the likelihood of identity theft occurring with respect to covered accounts, the university will take the following steps with respect to its internal operating procedures to protect identifying information:

1. Ensure that its Web site is secure or provide clear notice that the Web site is not secure.

2. Subject to state record retention requirements, ensure complete and secure destruction of paper documents and computer files containing account information when a decision has been made to no longer maintain such information.

P.O. Box 160002 • Orlando, FL 32816-0002 • (407) 823-1823 • FAX (407) 823-2264
An Equal Opportunity and Affirmative Action Institution

3. Ensure that office computers with access to covered account information are password protected.

4. Avoid use of social security numbers.

5. Ensure that computer virus protection is up to date.

6. Require and keep only the kinds of individual information that are necessary for university purposes.

C. Program Administration

1. Oversight

Responsibility for overseeing, developing, implementing, and updating this program lies with the program administrator with guidance from an Identity Theft Committee for the university. The committee is headed by the program administrator who is the University Controller or designee and should include representation from affected units, such as:

a. Finance and Accounting

b. Student Financial Assistance

c. General Counsel

d. Information Technologies and Resources

e. Admissions: Undergraduate Admissions, College of Graduate Studies, College of Medicine

f. UCF Foundation

g. Registrar's Office

h. Business Services

i. Human Resources

j. University Compliance and Ethics

The program administrator will be responsible for ensuring availability of appropriate training on the program. University Audit will be responsible for reviewing any reports regarding the detection of red flags and ensuring that the action taken by management is effective in preventing and mitigating particular circumstances.

P.O. Box 160002 • Orlando, FL 32816-0002 • (407) 823-1823 • FAX (407) 823-2264
An Equal Opportunity and Affirmative Action Institution

2. Staff Training and Reports

University staff responsible for implementing the program shall be trained in the detection of and responses to red flags. University staff shall be trained, as necessary, to effectively implement the program. University employees are expected to notify University Audit once they become aware of an incident of identity theft or of the university's failure to comply with this program (see UCF Policy 2-800 *Fraud Prevention and Detection*). At least annually or as otherwise requested by the program administrator, university staff members responsible for implementation of the program shall report to the committee on compliance with this program. The report should address such issues as effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the opening and maintenance of covered accounts, service provider arrangements, significant incidents involving identity theft, management responses, and recommendations for changes to the program.

3. Service Provider Arrangements

In the event the university engages a service provider in performing an activity in connection with one or more covered accounts, the university will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

a. Require, by contract, that service providers have such policies and procedures in place.

b. Require, by contract, that service providers review the university's program and report any red flags to the program administrator or the university employee with primary oversight of the service provider relationship.

4. Non-disclosure of Specific Practices

For the effectiveness of this Identity Theft Prevention Program, knowledge about specific red flag identification, detection, mitigation, and prevention practices may need to be limited to the committee members who developed this program and to those employees who need to know them. Any documents that may have been produced or are produced in order to develop or implement this program that list or describe such specific practices and the information those documents contain are considered confidential and should not be shared with other university employees or the public, unless required by applicable law. The program administrator shall identify those documents and practices that should be maintained in a confidential manner.

P.O. Box 160002 • Orlando, FL 32816-0002 • (407) 823-1823 • FAX (407) 823-2264
An Equal Opportunity and Affirmative Action Institution

5. Program Updates

The committee will periodically review and update this program to reflect changes in risks to individuals and the soundness of the university from identity theft. In doing so, the committee will consider the university's experiences with identity theft situations, changes in identity theft methods, changes in identity theft detection and prevention methods, and changes in the university's business arrangements with other entities. After considering these factors, the program administrator will determine whether changes to the program, including the listing of red flags, are warranted. If warranted, the committee will update the program.

RELATED DOCUMENTS:

- Federal Trade Commission's Red Flags Rule, 16 C.F.R. 681
- Section 114 of the Fair and Accurate Credit Transactions Act, 15 U.S.C. 1681m(e)
- University Policy 2-800 *Fraud Prevention and Detection*: http://www.policies.ucf.edu/documents/2-800FraudPreventionandDetectionFINAL.pdf

INITIATING AUTHORITY: Vice President and General Counsel

POLICY APPROVAL
(For use by the Office of the President)

Policy Number: 2-105.1

Initiating Authority: _____ **Date:** 9/2/11

Policies and Procedures Review Committee Chair: _____ **Date:** 8-29-11

President or Designee: _____ **Date:** 8/30/11

P.O. BOX 160002 • Orlando, FL 32816-0002 • (407) 823-1823 • FAX (407) 823-2264
An Equal Opportunity and Affirmative Action Institution

EXHIBIT B

University of Central Florida

Office of the President

SUBJECT:	Effective Date:	Policy Number:	
Collection and Use of Social Security Numbers	12-15-2010	4-012	
	Supersedes:	Page	Of
		1	4
	Responsible Authority: Vice Provost for Information Technologies and Resources		

APPLICABILITY/ACCOUNTABILITY:

This policy applies to all University of Central Florida employees, contractors, consultants, and agents of the above who collect, maintain, or have access to university data or documents containing Social Security Numbers (SSNs).

BACKGROUND:

Using the SSN as an identifier makes its use vulnerable to misuse, including identity theft.

POLICY STATEMENT:

The University of Central Florida is committed to ensuring the privacy of confidential information it collects and maintains on students, employees, and others. Social Security Numbers are sensitive data that are required by many university business processes but whose misuse or inadvertent disclosure can pose privacy risks to individuals as well as compliance or reputational risks to the university. It is the policy of UCF to request and use SSNs only as required for the performance of the university's duties and responsibilities and to secure this information from inappropriate release or disclosure.

DEFINITIONS:

Social Security Number. A unique nine-digit numerical personal identifier assigned by the federal Social Security Administration. The SSN is regarded as restricted data, as described in university policy 4-008, *Data Classification and Protection.*

Pseudo Social Security number. A unique nine-digit numerical personal identifier assigned by the University of Central Florida to foreign nationals and other individuals who do not have a SSN to include those individuals in university business processes that require use of the SSN.

EMPLID. A unique seven-digit numerical identifier assigned to the record of all university personnel in the university's PeopleSoft business system. The Employee Identification Number is regarded as restricted data as defined in university policy 4-008, *Data Classification and Protection.*

NID. A Network Identification Number is a UCF-issued identifier used by university employees and students to access systems that do not contain restricted data. NIDs are classified as unrestricted data. NIDs are the key to accessing the UCF computer network, the internet, the library, and other cyber information.

PID. A Personal Identification Number consisting of an individual's EMPLID with the addition of the first character of his or her first name. The PID is used as the login name in university business systems that contain restricted data. The Personal Identification Number is regarded as restricted data, as described in university policy 4-008, *Data Classification and Protection.*

Personally Identifiable Information. Information from which an individual may be uniquely and reliably identified or contacted.

FERPA. The Family Educational Rights and Privacy Act of 1974, also known as the Buckley Amendment. FERPA is a federal law that protects the privacy of student academic records.

PROCEDURES:

A. Collection of SSNs

1. Florida Statute 119.071(5) requires that state agencies may not collect SSNs unless the university has stated in writing the purpose for such collection and further requires that:
    a. agencies must provide a copy of the written statement to each individual whose SSN is collected
    b. agencies may not use SSNs for purposes other than those for which they were collected
    c. collection of the SSN is imperative for the performance of the agency's duties and responsibilities as prescribed by law

P.O. Box 160002 • Orlando, FL 32816-0002 • (407) 823-1823 • FAX (407) 823-2264
An Equal Opportunity and Affirmative Action Institution

2. When requesting a SSN from an individual, the federal Privacy Act of 1974 requires that any federal, state, or local agency:
    a. tell the individual whether disclosing the SSN is mandatory or voluntary
    b. state the statutory or other authority under which the request is being made, and
    c. state what uses it will make of the individual's SSN
3. SSNs may not be collected for use as a personal identification number. For purposes of UCF identification, the PID or NID should be used.

B. Use of SSNs

1. No part of an SSN may be displayed or distributed electronically via e-mail, whether in the body of the e-mail message or in an attachment.
2. Public display of partial SSNs is not acceptable because of the ease with which the missing digits can be obtained from various sources.
3. Only those individuals with a need to know are authorized to access student or employee SSNs. Prior to accessing SSNs, these individual should receive appropriate information security training and have signed the university's confidentiality statement.
4. Documents containing student or employee SSNs may not be distributed to or viewed by unauthorized individuals. Such documents should be stored only in secured rooms inside locked cabinets. In high-traffic areas, such documents should not be left on desks or other visible areas.
5. SSNs may be contained in historical university records and documents that cannot be altered. Such records should be considered restricted information and stored and handled accordingly.
6. UCF employees are authorized to release SSNs to third parties only as allowed by law, when authorization is granted in writing by an individual, or when the Office of the General Counsel has approved the release. An example would be release of student SSNs to the National Student Loan Clearinghouse.

RELATED DOCUMENTS:

Policy 4-008 *Data Classification and Protection*

Policy 4-007 *Security of Mobile Computing, Data Storage, and Communication Devices*

Policy 2-100 *Florida Public Records Act–Scope and Compliance*

P.O. Box 160002 • Orlando, FL 32816-0002 • (407) 823-1823 • FAX (407) 823-2264
An Equal Opportunity and Affirmative Action Institution

UCF Human Resources Confidentiality Agreement
http://hr.ucf.edu/files/ConfidentialityAgreement.pdf

UCF statement on the collection and use of Social Security Numbers
http://hr.ucf.edu/files/NoticeOfSSNUsage.pdf

INITIATING AUTHORITY: Provost and Vice President for Academic Affairs

POLICY APPROVAL
(For use by the Office of the President)

Policy Number: 4-012

Initiating Authority: _____ Date: 5-19-11

Policies and Procedures Review Committee Chair: _____ Date: 5-16-11

President or Designee: _____ Date: 5/25/11

P.O. Box 160002 • Orlando, FL 32816-0002 • (407) 823-1823 • FAX (407) 823-2264
An Equal Opportunity and Affirmative Action Institution