AOC-E-105 Sum Code: CI
Rev. 9-14

Commonwealth of Kentucky
Court of Justice *Courts.ky.gov*

CR 4.02; Cr Official Form 1

Case #: **18-CI-01449**
Court: **CIRCUIT**
County: **FAYETTE**

CIVIL SUMMONS

Plantiff, **MCKENZIE, METTEKJISTINE, ET AL VS. ALLCONNECT, INC.**, *Defendant*

TO: **CORPORATION SERVICE COMPANY**
421 W. MAIN STREET
FRANKFORT, KY 40601

Memo: Related party is ALLCONNECT, INC.

The Commonwealth of Kentucky to Defendant:
ALLCONNECT, INC.

You are hereby notified that a **legal action has been filed against you** in this Court demanding relief as shown on the document delivered to you with this Summons. **Unless a written defense is made by you or by an attorney on your behalf within twenty (20) days** following the day this paper is delivered to you, judgment by default may be taken against you for the relief demanded in the attached complaint.

The name(s) and address(es) of the party or parties demanding relief against you or his/her (their) attorney(s) are shown on the document delivered to you with this Summons.

/s/ Vincent Riggs, Fayette Circuit Clerk
Date: **04/17/2018**

Proof of Service

This Summons was:

☐ Served by delivering a true copy and the Complaint (or other initiating document)

To: _____

☐ Not Served because: _____

Date: _____, 20_____

_____
Served By

_____
Title

Summons ID: @00000802646
CIRCUIT: 18-CI-01449 Return to Filer for Service
MCKENZIE, METTEKJISTINE, ET AL VS. ALLCONNECT, INC.

COMMONWEALTH OF KENTUCKY
FAYETTE CIRCUIT COURT
DIVISION_____
CIVIL ACTION NO. _____
Electronically Filed

METTEKJISTINE MCKENZIE and CHASITY COMBS on behalf of themselves and all others similarly situated — PLAINTIFFS

v.

CLASS ACTION COMPLAINT
JURY TRIAL DEMANDED

ALLCONNECT, INC. — DEFENDANT

SERVE: Corporation Service Company
421 W. Main Street
Frankfort, Kentucky 40601

*** *** *** *** ***

Plaintiffs MetteKjistine McKenzie and Chasity Combs ("Plaintiffs"), individually and on behalf of all others similarly situated, by and through counsel, bring this action against Defendant Allconnect, Inc. ("Allconnect"), and allege as follows based upon personal knowledge, investigation of counsel, and information and belief:

NATURE OF THE ACTION

1. Allconnect operates a multi-channel marketplace that connects consumers with home services. The company provides a single source for consumers to compare and connect integrated media, broadband, home protection, energy, and green products. Allconnect has offices, including sales and customer care centers, in Georgia, Kentucky, Texas, and Utah.

2. On or about April 2, 2018, Allconnect sent an email to its current and former employees advising that their 2017 W-2 tax form information had been stolen in "an email

spoofing attack on February 14, 2018."

3. According to Allconnect's email notification, "an individual pretending to be [Steven Sibley], in [his] capacity as President of Allconnect" emailed an Allconnect employee requesting "all 2017 Allconnect employee W-2 information."

4. Falling for a well-known "phishing" or scam email scheme which human resources and accounting professionals have been warned about, the Allconnect employee complied with the email request to send unknown cyber criminals a data file which contained copies of W-2 statements or all of the sensitive personally identifying information ("PII") needed to fill out a W-2, including names, mailing addresses, Social Security numbers, and wage and withholding information (the "Data Disclosure"). The stolen data contained PII for every W-2 employee[1] (as categorized by the Internal Revenue Service ("IRS")) who worked at and received wages from Allconnect during the time period of January 1, 2017 through December 31, 2017.

5. On April 6, 2018, Allconnect mailed letters to Plaintiffs and Class Members that contained much of the same information from the April 2nd email, however, the letter also disclosed that Allconnect didn't even discover the Data Disclosure until March 28, or over a month after it occurred.

6. As a consequence of the Data Disclosure, Plaintiffs and Class Members have suffered damages by taking measures to both deter and detect identity theft. Class Members have been required to take the time, which they otherwise would have dedicated to other life demands (such as work), and effort to mitigate the actual and potential impact of the Data

[1] In simplest terms, the IRS has two categories for workers: employees and independent contractors. For employees, payroll taxes are automatically deducted from paychecks and paid to the government through the employer. The employer reports the wages to the IRS at the end of the year on a W-2 form. Independent contractors are responsible for calculating and submitting their own payroll taxes. Companies report the wages paid to independent contractors on a Form 1099. *See*, *IRS Publication 15-A*, *available at* https://www.irs.gov/publications/p15a/ar02.html (last visited April 11, 2018).

Disclosure on their lives including, *inter alia*; placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, scheduling and attending appointments with the IRS, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports.

7. No one can know what else the cyber criminals will do with the employees' PII. However, what is known is that Allconnect employees are now, and for the rest of their lives will be, at a heightened risk of further identity theft and fraud. Indeed, some Allconnect employees have already uncovered identity theft, such as fraudulent tax returns filed using the very W-2 information that was disclosed by Allconnect.

8. For all Class Members, fear and anxiety of identity theft or fraud is the new norm.

9. Plaintiffs bring this class action against Allconnect for failing to adequately secure and safeguard the PII of Plaintiffs and the Class, for failing to comply with industry standards regarding electronic transmission of PII, and for failing to provide accurate and adequate notice to Plaintiffs and other Class members as to precisely how their sensitive personal information had been given to unknown persons.

10. Allconnect disregarded the rights of Plaintiffs and Class members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that the data it stores was safeguarded, failing to take available steps to prevent the disclosure from happening, and failing to follow applicable, required and appropriate protocols, policies and procedures. As the result, the PII of Plaintiffs and Class Members was compromised and disclosed to an unknown and unauthorized third party. However, as this same information remains stored in Allconnect computer systems, Plaintiffs and Class members have an interest in ensuring that their information is and remains safe, and

they should be entitled to injunctive and other equitable relief.

PARTIES

Plaintiff MetteKjistine McKenzie

11. Plaintiff MetteKjistine McKenzie is a citizen and resident of Littlefield, Arizona.

12. Plaintiff McKenzie began working for Allconnect in sales in February 2016. After leaving the company for approximately two months, she applied and was rehired in October 2016. Plaintiff McKenzie worked at Allconnect's Utah-based call center throughout 2017

13. Plaintiff McKenzie was an employee at Allconnect whose PII was disclosed without her authorization to an unknown third party as a result of the Data Disclosure.

14. Plaintiff McKenzie received the April 2 email and April 6 letter from Allconnect regarding the Data Disclosure.

15. Due to the lack of information from Allconnect regarding the Data Disclosure, and the concern regarding the fraudulent use of her W-2 information, Plaintiff McKenzie sought additional details from Allconnect about the Data Disclosure.

16. Because her personal information was disclosed as a result of the Data Disclosure, Plaintiff McKenzie signed up for the AllClear ID credit monitoring service offered by Allconnect and called the IRS for guidance on protecting herself from false tax returns. Plaintiff McKenzie was also forced to place freezes on her credit, which required her to pay $9.99 to TransUnion.

17. As a result of the Data Disclosure, Plaintiff McKenzie has spent, and will continue to spend, time and effort attempting to mitigate the dangers and continuing risk of identity theft and tax fraud.

Plaintiff Chasity Combs

18. Plaintiff Chasity Combs is a citizen and resident of Georgetown, Kentucky.

19. Plaintiff Combs worked at Allconnect's Kentucky-based call center from 2014 until April 2018.

20. Plaintiff Combs was an employee at Allconnect whose PII was disclosed without her authorization to an unknown third party as a result of the Data Disclosure.

21. Plaintiff McKenzie received the April 6 letter from Allconnect regarding the Data Disclosure.

22. Due to the lack of information from Allconnect regarding the Data Disclosure, and the concern regarding the fraudulent use of her W-2 information, Plaintiff Combs sought additional details from Allconnect about the Data Disclosure.

23. Because her personal information was disclosed as a result of the Data Disclosure, Plaintiff Combs signed up for the AllClear ID credit monitoring service offered by Allconnect and called the IRS for guidance on protecting herself from false tax returns. At the direction of the IRS, she went to the IRS's website and requested a pin to be used for the filing of her 2017 taxes. Plaintiff Combs also checks her credit with Credit Karma daily as a result of the Data Disclosure.

24. As a result of the Data Disclosure, Plaintiff Combs has spent time and effort attempting to mitigate the dangers and continuing risk of identity theft and tax fraud.

Defendant

25. Defendant Allconnect, Inc. is a Delaware corporation with its headquarters in

Atlanta, Georgia and is therefore a citizen of both Delaware and Georgia.

26. Defendant Allconnect, Inc. has a call center located and therefore does business in Lexington, Fayette County, Kentucky.

JURISDICTION AND VENUE

27. Plaintiffs' causes of action against Allconnect arise under a common nucleus of facts and are brought pursuant to the common law of the Commonwealth of Kentucky.

28. This Court has personal jurisdiction over Allconnect pursuant to Ky. Rev. Stat. § 23A.010(1) and Ky. Rev. Stat. Ann. § 452.450 because the company has a place of business situated in this County.

29. Venue is proper in this Circuit pursuant to Ky. Rev. Stat. § 24A.120(1) because the amount in controversy exceeds $5,000, exclusive of interests and costs.

FACTUAL ALLEGATIONS

30. As a condition of employment, Allconnect requires that employees entrust it with certain personal information. In its ordinary course of business, Allconnect maintains personal and tax information, including the name, address, zip code, date of birth, wage and withholding information, and Social Security number, of each current and former employee.

31. Plaintiffs and members of the proposed Class, as current and former employers, relied on Allconnect to keep this information confidential and securely maintained.

32. On or about April 2, 2018, Allconnect sent an email to some current and former employees, advising that Allconnect had been involved in a data breach resulting from an email phishing scam, which the company referred to as an "email spoofing attack" and an "impersonation attack."

33. The email stated that Allconnect employees' 2017 W-2 tax information, including

names, addresses, social security numbers and wage information, had been involved in the breach. The email advised employees that the company would be providing two years of "Identity Protection" service provided by AllClear ID, and that employees could sign up for the service beginning the next day, April 3, 2018.

34. The data breach referred to in Allconnect's email notification was actually a voluntary disclosure of employees' PII by an Allconnect employee. On or about February 14, 2018, the Allconnect employee responded to an email request for a file containing the 2017 W-2 tax information of all employees, seemingly originating from Allconnect President Steve Sibley. Allconnect stated in its email notification that it "first discovered the fraudulent nature of the request on March 28, 2018," or well over a month after the Data Disclosure.

35. This Data Disclosure occurred at a time in the calendar year when W-2 information is most vital and valuable.

36. Allconnect could have prevented this Data Disclosure. Allconnect was not without warning of this phishing email scam, which was publicly available, yet it failed to implement adequate measures to protect its employees' PII.

37. Allconnect's negligence in safeguarding its employees' PII is exacerbated by the repeated warnings and alerts, not only of the increasing risk of general email scams, but of the actual W-2 phishing email scam it chose to ignore and, thus, fell prey to.

38. Business Email Compromise or spoofing is the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source. For example, spoofed email may purport to be from someone in a position of authority within a company asking for sensitive data such as passwords or employee information that can be used for a variety of criminal purposes. A telltale sign of a spoofing e-mail is an "urgent"

request from a company "executive" requesting that confidential information be provided via email.

39. As noted by cybersecurity journalist Brian Krebs, this type of fraud "usually begins with the thieves either phishing an executive and gaining access to that individual's email account or emailing employees from a look-alike domain that is one or two letters off from the company's true domain name."[2]

40. Spoofing fraud has been steadily increasing in recent years. The FBI recently issued an alert stating that from October 2013 through February 2016, law enforcement received reports from over 17,000 victims of "spoofing" scams, which resulted in more than $2.3 billion in losses. Since January 2015, the FBI has seen a 270% increase in identified victims and exposed loss from spoofing scams.[3]

41. Companies can mount two primary defenses to spoofing scams: employee education and technical security barriers. Employee education is the process of adequately making employees aware of common spoofing scams and implementing company-wide policies requiring the request or transfer of sensitive personal or financial information only through secure sources to known recipients. Employee education and secure file-transfer protocols provide the easiest method to assist employees in properly identifying fraudulent e-mails and prevent unauthorized access of personal and tax information.

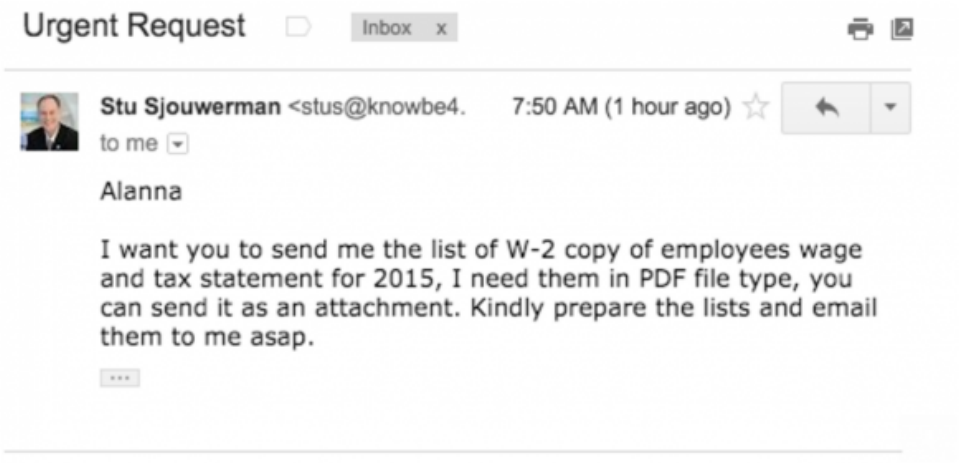
42. From a technical perspective, companies can also greatly reduce the flow of spoofing e-mails by implementing certain security measures governing e-mail transmissions.

[2] Brian Krebs, *FBI: $2.3 Billion Lost to CEO Email Scams*, KREBS ON SECURITY (April 7, 2016), *available at* http://krebsonsecurity.com/2016/04/fbi-2-3-billion-lost-to-ceo-email-scams/ (last visited April 11, 2018).

[3] *FBI Warns of Dramatic Increase in Business E-Mail Scams* (April 4, 2016), *available at* https://www.fbi.gov/contact-us/field-offices/phoenix/news/press-releases/fbi-warns-of-dramatic-increase-in-business-e-mail-scams (last visited April 11, 2018).

Companies can use a simple email validation system that allows domain owners to publish a list of IP addresses that are authorized to send email on their behalf to reduce the amount of spam and fraud by making it much harder for malicious senders to disguise their identities. Companies can also use email authentication that blocks email streams that have not been properly authenticated.

43. On February 24, 2016, cybersecurity journalist Brian Krebs warned of the precise scam which snared Allconnect in a blog that said all it needed to say in its title: Phishers Spoof CEO, Request W2 Forms.[4] Krebs warned that cybercriminals were attempting to scam companies by sending false emails, purportedly from the company's chief executive officer, to individuals in the human resources or accounting department asking for copies of W-2 data for all employees. Krebs even provided an example of such an email that had been sent to another company:



44. Further, on March 1, 2016, the IRS issued an alert to payroll and human resources professionals warning of the same scheme. In precise detail, the alert stated:

[4] Brian Krebs, *Phishers Spoof CEO, Request W2 Forms*, KREBS ON SECURITY *available at* http://krebsonsecurity.com/2016/02/phishers-spoof-ceo-request-w2-forms/ (last visited April 11, 2018).

> The Internal Revenue Service today issued an alert to payroll and human resources professionals to beware of an emerging phishing email scheme that purports to be from company executives and requests personal information on employees.
>
> The IRS has learned this scheme — part of the surge in phishing emails seen this year — already has claimed several victims as payroll and human resources offices mistakenly email payroll data including Forms W-2 that contain Social Security numbers and other personally identifiable information to cybercriminals posing as company executives.
>
> "This is a new twist on an old scheme using the cover of the tax season and W-2 filings to try tricking people into sharing personal data. Now the criminals are focusing their schemes on company payroll departments," said IRS Commissioner John Koskinen. "If your CEO appears to be emailing you for a list of company employees, check it out before you respond. Everyone has a responsibility to remain diligent about confirming the identity of people requesting personal information about employees." [5]

45. On February 18, 2016, the IRS renewed this alert for HR and Accounting professionals.

46. Again on January 25, 2017, the IRS renewed the alert specifically cautioning, "company payroll officials to double check any executive-level or unusual requests for lists of Forms W-2 or Social Security number." [6]

47. Again on January 12, 2018, the IRS renewed the alert. [7]

48. A simple phone call to verify this request would have prevented the Data Disclosure.

49. Despite the widespread prevalence of spoofing aimed at obtaining confidential

[5] IRS, *IRS Alerts Payroll and HR Professionals to Phishing Scheme Involving W-2s*, IR-2016-34 (March 1, 2016), *available at* https://www.irs.gov/uac/Newsroom/IRS-Alerts-Payroll-and-HR-Professionals-to-Phishing-Scheme-Involving-W2s (last visited April 11, 2018).

[6] IRS, *IRS, States and Tax Industry Renew Alert about Form W-2 Scam Targeting Payroll, Human Resource Departments*, IR-2017-10 (Jan. 25, 2017), *available at*: https://www.irs.gov/uac/newsroom/irs-states-and-tax-industry-renew-alert-about-form-w2-scam-targeting-payroll-human-resource-departments (last visited April 11, 2018).

[7] IRS, *IRS Alerts Payroll and HR Professionals to Phishing Scheme Involving W-2s*, IR-2016-34 (Updated Jan. 12, 2018), *available at* https://www.irs.gov/uac/Newsroom/IRS-Alerts-Payroll-and-HR-Professionals-to-Phishing-Scheme-Involving-W2s (last visited April 13, 2018).

information from employers and despite the warnings of the W-2 email scam from the 2015 tax season and renewed alerts for the 2016, 2017, and 2018 tax seasons, Allconnect provided its employees with unreasonably deficient training on cybersecurity and information transfer protocols prior to the Data Disclosure.

50. Allconnect failed to adequately train its employees on even the most basic of cybersecurity protocols, including:

a. How to detect phishing and spoofing emails and other scams including providing employees examples of these scams and guidance on how to verify if emails are legitimate;

b. Effective password management and encryption protocols for internal and external emails;

c. Avoidance of responding to emails that are suspicious or from unknown sources;

d. Locking, encrypting and limiting access to computers and files containing sensitive information;

e. Implementing guidelines for maintaining and communicating sensitive data; and

f. Protecting sensitive employee information, including personal and financial information, by implementing protocols on how to request and respond to requests for the transfer of such information and how to securely send such information through a secure file transfer system to only known recipients.

51. Allconnect's failures handed criminals the PII of Plaintiffs and other Class Members and put Plaintiffs and the Class at serious, immediate and ongoing risk for identity theft and fraud.

52. While there is a market for this PII for other long term scams, the immediate and

short term practice with such breaches is that the cyber criminals will use the PII to file false tax returns, and indeed Allconnect employees are already discovering the filing of false tax returns. Access to W-2 information permits identity thieves to quickly and easily file fraudulent tax returns, using the victim's information to obtain a fraudulent refund. The IRS will direct deposit the refund to the bank account or prepaid debit card (which are virtually untraceable) provided by the thief.

53. The Data Disclosure was caused by Allconnect's violation of its obligation to abide by best practices and industry standards concerning the security of its computer and payroll processing systems. Allconnect failed to comply with security standards and allowed its employees' PII to be stolen by failing to implement security measures that could have prevented or mitigated the Data Disclosure.

54. Allconnect failed to ensure that all personnel in its human resources and payroll departments were made aware of this well-known and well-publicized phishing email scam.

55. The ramifications of Allconnect's failure to keep its employees' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

56. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[8] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport

[8] 17 C.F.R. § 248.201 (2013).

number, employer or taxpayer identification number."[9]

57. Social Security numbers, for example, are among the worst 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.

58. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later.[10]

59. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

60. What is more, 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.

61. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center: "The credit bureaus and banks are able to link

[9] *Id.*

[10] Social Security Administration, Identity Theft and Your Social Security Number, *available at* http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited April 11, 2018).

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."[11]

62. Based on the foregoing, the information stolen in the Data Disclosure is significantly more valuable than the loss of, say, credit card information in a large retailer data breach such as those that occurred at Target and Home Depot. Victims affected by those retailer breaches could avoid much of the potential future harm by cancelling credit or debit cards and obtaining replacements. The information stolen in the Data Disclosure is difficult, if not impossible, to change—Social Security number, name, employment information, income data, etc.

63. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[12]

64. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police during an arrest.

65. The fraudulent activity resulting from the Data Disclosure may not come to light for years.

66. Despite all of the publicly available knowledge of the continued compromises of PII, and alerts regarding the actual W-2 phishing email scam perpetrated, Allconnect's approach

[11] *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015, *available at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited April 11, 2018).

[12] *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, Feb. 6, 2015, *available at* http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited April 11, 2018).

to maintaining the privacy of its employees PII was lackadaisical, cavalier, reckless, or in the very least, negligent.

67. Allconnect has failed to provide compensation to Plaintiffs and Class Members victimized in this Data Disclosure. Allconnect has not offered to provide any assistance or compensation for the costs and burdens – current and future – associated with the identity theft and fraud resulting from the Data Disclosure. Allconnect has not offered employees any assistance in dealing with the IRS or state tax agencies.

68. It is incorrect to assume that reimbursing a consumer for financial loss due to fraud makes that individual whole again. On the contrary, after conducting a study, the U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims." [13]

69. To date, Allconnect has offered its employees only two years of "Identity Protection" service through AllClear ID. The offered AllClear ID service is inadequate to protect the Plaintiffs and Class Members from the threats they face, particularly in light of the PII stolen. Websites that rank identity theft protection services are critical of AllClear ID's service. In its review of the "Best Identity Theft Protection Services," NextAdvisor ranks 7 other services, and does not even list AllClear ID among its "top-rated services."[14] BestIDTheftCompanys.com ranks AllClear ID at number 12 on its list of 20 ranked companies

[13] Victims of Identity Theft, 2012 (Dec. 2013) at 10, 11, *available at* https://www.bjs.gov/content/pub/pdf/vit12.pdf (last visited April 11, 2018).

[14] *See* https://www.nextadvisor.com/identity_theft_protection_services/index.php (last visited April 11, 2018).

with a mere score of 3.0 out of 10.[15]

70. As a result of Allconnect's failure to prevent the Data Disclosure, Plaintiffs and Class Members have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety and emotional distress. They have suffered or are at increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise, publication and/or theft of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Disclosure, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII;

h. The continued risk to their PII, which remains in the possession of Allconnect and is subject to further breaches so long as Allconnect fail to undertake appropriate measures to protect the PII in their possession; and

i. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Disclosure for the remainder of the lives of Plaintiffs and Class Members.

[15] *See* https://bestcompany.com/identity-theft?page=2 (last visited April 11, 2018).

CLASS ACTION ALLEGATIONS

71. Plaintiffs bring this suit as a class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23.02(b), 23.02(c) and 23.03(6) of the Kentucky Rules of Civil Procedure.

72. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> All current and former Allconnect employees whose PII was compromised as a result of the Data Disclosure.

73. In the alternative to the Nationwide Class, and pursuant to Kentucky Rule of Civil Procedure 23.03(7), Plaintiffs seek to represent the following state classes only in the event that the Court declines to certify the Nationwide Class above. Specifically, the state classes consists of the following:

> All current and former Allconnect employees who currently reside in Arizona and whose PII was compromised as a result of the Data Disclosure.

and

> All current and former Allconnect employees who currently reside in Kentucky and whose PII was compromised as a result of the Data Disclosure.

74. Excluded from the Class are the officers, directors and legal representatives of Allconnect and the judges and court personnel in this case and any members of their immediate families.

75. Numerosity. Ky. R. Civ. P. 23.01(a). The members of the Class are so numerous that joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiffs at this time, based on information and belief, it is estimated to be at or

above 1,000. The exact number is generally ascertainable by appropriate discovery as Allconnect had knowledge of the employees whose PII was in the data file it disclosed.

76. Commonality. Ky. R. Civ. P. 23.01(b) and 23.02(c). 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 and to what extent Allconnect had a duty to protect the PII of Class Members;

b. Whether Allconnect failed to adequately safeguard the PII of Class Members;

c. Whether Allconnect adequately, and accurately informed Class Members that their PII had been compromised;

d. Whether Allconnect failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Disclosure;

e. Whether Allconnect engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Class Members;

f. Whether Class Members are entitled to actual damages, statutory damages, and/or punitive damages as a result of Allconnect's wrongful conduct;

j. Whether Plaintiffs and the members of the Class are entitled to restitution as a result of Allconnect's wrongful conduct; and,

k. Whether Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Disclosure.

77. Typicality. Ky. R. Civ. P. 23.01(c) Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PII, like that of every other class member, was disclosed by

Allconnect. Plaintiffs' claims are typical of those of the other Class Members because, *inter alia*, all Members of the Class were injured through the common misconduct of Allconnect. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of other Class members arise from the same operative facts and are based on the same legal theories.

78. Adequacy of Representation. Ky. R. Civ. P. 23.01(d). Plaintiffs will fairly and adequately represent and protect the interests of the Class in that they have no disabling conflicts of interest that would be antagonistic to those of the other members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class members. Plaintiffs have retained counsel experienced in complex consumer class action litigation, and Plaintiffs intend to prosecute this action vigorously.

79. Superiority of Class Action. Ky. R. Civ. P. 23.02(c). The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain class members, who could not individually afford to litigate a complex claim against large corporate Allconnect. Further, even for those class members who could afford to litigate such a claim, it would still be economically impractical.

80. The nature of this action and the nature of laws available to Plaintiffs and the Class make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and the Class for the wrongs alleged because Allconnect would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each member of the Class to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

81. The litigation of the claims brought herein is manageable. Allconnect's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

82. Adequate notice can be given to Class Members directly using information maintained in Allconnect's records.

83. Unless a Class-wide injunction is issued, Allconnect may continue in its failure to properly secure the PII of Class Members, Allconnect may continue to refuse to provide proper notification to Class Members regarding the Data Disclosure, and Allconnect may continue to act unlawfully as set forth in this Complaint.

84. Further, Allconnect has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the

members of the Class as a whole is appropriate under Rule 23.02(b) of the Kentucky Rules of Civil Procedure.

85. Likewise, particular issues under Rule 23.03(6)are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Allconnect owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;

b. Whether Allconnect breached a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Allconnect failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Allconnect and the Class and the terms of that implied contract; and

e. Whether Allconnect breached the implied contract.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of the Class)

86. Plaintiffs restate and reallege all preceding paragraphs as if fully set forth herein.

87. As a condition of their employment, employees were obligated to provide Allconnect with certain PII, including their date of birth, mailing addresses and Social Security numbers.

88. Plaintiffs and the Class Members entrusted their PII to Allconnect on the premise and with the understanding that Allconnect would safeguard their information.

89. Allconnect had full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class Members could and would suffer if the PII were wrongfully disclosed.

90. Allconnect 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 Allconnect's security protocols to ensure that Plaintiffs and Class members' information in its possession was adequately secured and protected and that employees tasked with maintaining such information were adequately training on cyber security measures regarding the security of employees' personal and tax information.

91. Plaintiffs and the Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Allconnect knew of should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Class, the critical importance of providing adequate security of that PII, the current cyber scams being perpetrated on companies, and that it had inadequate employee training and education and IT security protocols in place to secure the PII of Plaintiffs and the Class.

92. Allconnect's own conduct created a foreseeable risk of harm to Plaintiffs and Class Members. Allconnect's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Disclosure as set forth herein. Allconnect's misconduct also included its decision not to comply with industry standards for the safekeeping and encrypted authorized disclosure of the PII of Plaintiffs and Class Members.

93. Plaintiffs and the Class Members had no ability to protect their PII that was in Allconnect's possession.

94. Allconnect was in a position to protect against the harm suffered by Plaintiffs and

Class Members as a result of the Data Disclosure.

95. Allconnect had and continues to have a duty to adequately disclose that the PII of Plaintiffs and Class Members within its possession might have been compromised, how it was compromised and precisely the types of information that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class Members to take steps to prevent, mitigate and repair any identity theft and the fraudulent use of their PII by third parties.

96. Allconnect had a duty to have proper procedures in place to prevent the unauthorized dissemination of the PII of Plaintiffs and Class Members.

97. Allconnect has admitted that the PII of Plaintiffs and Class Members was wrongfully disclosed to unauthorized third persons as a result of the Data Disclosure.

98. Allconnect, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding the PII of Plaintiffs and Class Members during the time the PII was within Allconnect's possession or control.

99. Allconnect improperly and inadequately safeguarded the PII of Plaintiffs and Class Members in deviation of standard industry rules, regulations and practices at the time of the Data Disclosure.

100. Allconnect failed to heed industry warnings and alerts issued by the IRS to provide adequate safeguards to protect employees' PII in the face of increased risk of a current phishing email scheme being perpetrated.

101. Allconnect, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its employees' PII.

102. Allconnect, through its actions and/or omissions, unlawfully breached its duty to adequately disclose to Plaintiffs and Class Members the existence, and scope of the Data Disclosure.

103. But for Allconnect's wrongful and negligent breach of duties owed to Plaintiffs and Class Members, the PII of Plaintiffs and Class Members would not have been compromised.

104. There is a close causal connection between Allconnect's failure to implement security measures to protect the PII of current and former employees and the harm suffered or risk of imminent harm suffered by Plaintiffs and the Class.

105. As a result of Allconnect's negligence, Plaintiffs and the Class Members have suffered and will continue to suffer damages and injury including, but not limited to: out-of-pocket expenses associated with addressing false tax returns filed; current and future out-of-pocket costs in connection with preparing and filing tax returns; loss or delay of tax refunds as a result of fraudulently filed tax returns; out-of-pocket expenses associated with procuring robust identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing and correcting the current and future consequences of the Data Disclosure.

SECOND CAUSE OF ACTION
Invasion of Privacy
(On Behalf of the Class)

106. Plaintiffs restate and reallege all preceding paragraphs as if fully set forth herein.

107. Plaintiffs and Class Members had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

108. Allconnect owed a duty to its employees, including Plaintiffs and Class Members,

to keep their PII contained as a part thereof, confidential.

109. Allconnect intentionally released to unknown and unauthorized third parties a file containing the PII of Plaintiffs and Class Members.

110. Allconnect intentionally allowed unauthorized and unknown third parties unfettered access to and examination of the PII of Plaintiffs and Class Members.

111. The unauthorized release to, custody of and examination by unauthorized third parties of the PII of Plaintiffs and Class Members, especially where the information includes Social Security numbers and wage information, would be highly offensive to a reasonable person.

112. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and Class Members disclosed their PII to Allconnect as part of their employment, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and Class Members were reasonable to believe that such information would be kept private and would not be disclosed without their authorization.

113. The Data Disclosure at the hands of Allconnect constitutes an intentional interference with Plaintiffs and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

114. As a proximate result of the above acts and omissions of Allconnect, the PII of Plaintiffs and Class Members was disclosed to and used by third parties without authorization, causing Plaintiffs and Class Members to suffer damages.

115. Unless and until enjoined, and restrained by order of this Court, Allconnect's

wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that the PII maintained by Allconnect can be viewed, distributed and used by unauthorized persons. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Class.

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of the Class)

116. Plaintiffs restate and reallege all preceding paragraphs as if fully set forth herein.

117. Plaintiffs and Class members were required to provide their PII, including names, addresses, Social Security numbers, and other personal information, to Allconnect as a condition of their employment.

118. Implicit in the employment agreement between Allconnect and its employees was the obligation that both parties would maintain information confidentially and securely.

119. Allconnect had an implied duty of good faith to ensure that the PII of Plaintiffs and Class members in its possession was only used to provide agreed-upon compensation and other employment benefits from Allconnect.

120. Allconnect had an implied duty to reasonably safeguard and protect the PII of Plaintiffs and Class members from unauthorized disclosure or uses.

121. Additionally, Allconnect implicitly promised to retain this PII only under conditions that kept such information secure and confidential.

122. Plaintiffs and Class members fully performed their obligations under the implied contract with Allconnect. Allconnect did not.

123. Plaintiffs and Class members would not have provided their confidential PII to

Allconnect in the absence of their implied contracts with Allconnect, and would have instead retained the opportunity to control their PII for uses other than compensation and employment benefits from Allconnect.

124. Allconnect breached the implied contracts with Plaintiffs and Class members by failing to reasonably safeguard and protect Plaintiffs' and Class members' PII, which was compromised as a result of the Data Disclosure.

125. Allconnect's acts and omissions have materially affected the intended purpose of the implied contacts requiring Plaintiffs and Class members to provide their PII as a condition of employment in exchange for compensation and benefits.

126. As a direct and proximate result of Allconnect's breach of its implied contacts with Plaintiffs and Class members, Plaintiffs and Class members have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity how their PII is used; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Disclosure, 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 credit reports; (vi) the continued risk to their PII, which remain in Allconnect's possession and is subject to further unauthorized disclosures so long as Allconnect fails to undertake appropriate and adequate measures to protect the PII of employees and former employees in its continued possession; and, (vii) 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 Disclosure for the

remainder of the lives of Plaintiffs and Class members.

FOURTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of the Class)

127. Plaintiffs restate and reallege all preceding paragraphs as if fully set forth herein.

128. Allconnect was a fiduciary, as an employer created by its undertaking, to act primarily for the benefit of its employees, including Plaintiffs and Class members, for the safeguarding of employees' PII and wage information.

129. Allconnect had a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of their employer/employee relationship, in particular to keep secure income records and the PII of its employees.

130. Allconnect breached its duty of care to Plaintiffs and Class members to ensure that their PII and W-2 data was not disclosed without authorization or used for improper purposes by failing to provide adequate protections to the information and by voluntarily disclosing the information, in an unencrypted format, to an unknown and unauthorized third party.

131. As a direct and proximate result of Allconnect's actions alleged above, the Plaintiffs and Class members have suffered actual damages.

PRAYER FOR RELIEF

WHEREFORE Plaintiffs on behalf of themselves and all others similarly situated, pray for relief as follows:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their Counsel to represent the Class;

B. A mandatory injunction directing Allconnect to hereinafter adequately safeguard

the PII of the Class by implementing improved security procedures and measures;

C. A mandatory injunction requiring that Allconnect provide notice to each member of the Class relating to the full nature and extent of the Data Disclosure and the disclosure of PII to unauthorized persons;

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

E. For an award of attorneys' fees and costs;

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

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: April 17, 2018

Respectfully submitted,

BRANSTETTER, STRANCH & JENNINGS, PLLC

/s/ David O'Brien Suetholz
David O'Brien Suetholz
515 Park Avenue
Louisville, KY 40208
Phone: 502-636-4333
Email: davids@bsjfirm.com

J. Gerard Stranch, IV *
BRANSTETTER, STRANCH & JENNINGS, PLLC
223 Rosa L. Parks Avenue, Ste. 200
Nashville, TN 37203
Phone: (615) 254-8801
Fax: (615) 255-5419
Email: gerards@bsjfirm.com

Richard E. Shevitz (Indiana Bar # 12007-49) *
Lynn A. Toops (Indiana Bar # 26386-49) *
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, IN 46204
Telephone: (317) 636-6481
Fax: (317) 636-2593
rshevitz@cohenandmalad.com
ltoops@cohenandmalad.com

Christopher D. Jennings *
THE JOHNSON FIRM
2226 Cottondale Lane, Suite 210
Little Rock, AR 72202
T: (501) 372-1300
F: (888) 505-0909
E: chris@yourattorney.com

Attorneys for Plaintiffs and the Proposed Class

* *pro hac vice* application to be submitted