**IN THE UNITED STATES DISTRICT COURT**
**FOR THE SOUTHERN DISTRICT OF FLORIDA**
**CASE NO.**

ROBERT BOHANNON and HOLLY BUCKINGHAM, on behalf of themselves and all others similarly situated,

Plaintiffs,

**JURY TRIAL DEMANDED**

v.

COMPLYRIGHT, INC., a Minnesota corporation,

Defendant.
_____/

## CLASS ACTION COMPLAINT

Plaintiffs Robert Bohannon and Holly Buckingham ("Plaintiffs") individually and on behalf of all others similarly situated, upon personal knowledge of the facts pertaining to them and on information and belief as to all other matters, by and through undersigned counsel, hereby bring this Class Action Complaint against defendant ComplyRight, Inc. ("ComplyRight" or "Defendant").

## NATURE OF THE ACTION

1. Plaintiffs bring this action, individually and on behalf of all others similarly situated whose personal and non-public information, including names, addresses, phone numbers, email addresses and Social Security numbers (collectively, "Personal Information") was compromised in a security breach of Defendant's computer servers beginning on or around April 20, 2018 and lasting until May 22, 2018 (the "Data Breach").

2. Defendant ComplyRight is a cloud-based human resources and tax preparation company. Thousands of organizations and businesses use its services to prepare tax forms, such

as 1099s and W2s, on behalf of their employees. Many of these employees whose personal information has been entrusted to ComplyRight have never even heard of the company.

3. As discussed in more detail below, ComplyRight held itself out as an entity that had implemented several layers of data protection. For example, its website claims that "data security is a primary concern," "[w]e use the strongest encryption program available, as recommended by the federal government, to block the interception or interruption of information by a third party," and "[d]ata is encrypted as soon as it's entered on the site, and it says encrypted throughout the entire print, mail and e-file process."

4. Contrary to these claims, ComplyRight did not adequately safeguard the data entrusted to it. Instead, as alleged herein, Defendant's failure to implement or maintain adequate data security measures for customer information, including the Personal Information, directly and proximately caused injuries to Plaintiffs and the Class (defined below).

5. Defendant failed to take reasonable steps to employ adequate security measures or to properly protect sensitive payment Personal Information despite well-publicized data breaches at large companies including Arby's, Wendy's, Target, Chipotle, Home Depot, Sally Beauty, Harbor Freight Tools, P.F. Chang's, Dairy Queen, Kmart, and many others.

6. The Data Breach was the inevitable result of ComplyRight's inadequate data security measures and cavalier approach to data security. Despite the well-publicized and ever-growing threat of security breaches, ComplyRight failed to ensure that it maintained adequate data security measures causing customer Personal Information to be stolen.

7. As a direct and proximate consequence of ComplyRight's misconduct, a massive amount of information was stolen from ComplyRight. Upon information and belief, the ComplyRight Data Breach compromised the Personal Information of hundreds of thousands (if

not more) of Personal Information entrusted to it. Victims of the Data Breach have had their Personal Information compromised, had their privacy rights violated, been exposed to the increased risk of fraud and identify theft, lost control over their personal and financial information, and otherwise been injured.

8. Plaintiffs and Class Members seek to recover damages caused by Defendant's breach of contracts to which Plaintiffs and Class Members are intended third party beneficiaries, negligence, negligence *per se*, breach of implied contract, and violations of state consumer protection and data privacy statutes. Additionally, Plaintiffs seek declaratory and injunctive relief as a result of the conduct of Defendant discussed herein.

## PARTIES

### Plaintiff Robert Bohannon

9. Plaintiff Robert Bohannon is an adult residing in Granger, Indiana. On or about July 18, 2018, Plaintiff Bohannon received a letter from ComplyRight informing him that ComplyRight was subject to "a recent security incident involving some of [his] Personal Information that was maintained on [ComplyRight's] website." The letter stated further that his Personal Information "was accessed and/or viewed, and may have been downloaded or otherwise acquired, by an unauthorized user" including his "name, address, telephone number, email address, and Social Security number."

10. Although the letter was dated July 13, 2018, it indicated that ComplyRight "initially learned" of the Breach "on or about May 22, 2018."

11. Had Plaintiff Bohannon known that ComplyRight would not adequately protect the Personal Information and other sensitive information entrusted to it, he would not have allowed his Personal Information to be entrusted to ComplyRight.

12. As a result of ComplyRight's failure to adequately safeguard Plaintiff Bohannon's Personal Information, Plaintiff Bohannon has been injured.

**Plaintiff Holly Buckingham**

13. Plaintiff Holly Buckingham is an adult residing in Woodbine, Maryland. Sometime in July, Plaintiff Bohannon received a letter similar to, if not the same as, the letter sent to Plaintiff Bohannon, summarized above.

14. Since receiving the letter, Plaintiff Buckingham has spent at least two business days expending effort to ensure her Personal Information is not used by the hackers and that her identity is not stolen.

15. Had Plaintiff Buckingham known that ComplyRight would not adequately protect her Personal Information and other sensitive information entrusted to it, she would not have authorized her employer to transmit her Personal Information to ComplyRight and/or allowed ComplyRight to store her Personal Information.

16. As a result of ComplyRight's failure to adequately safeguard Plaintiff Bohannon's Personal Information, Plaintiff Bohannon has been injured.

**Defendant**

17. ComplyRight is a Minnesota corporation with a principal office located at 1725 Roe Crest Drive, North Mankato, MN 56003. ComplyRight lists its "main office" in Florida at 3300 Gateway Drive, Pompano Beach, FL 33069. ComplyRight's Registered Agent is C T Corporation System, located at 1200 South Pine Island Road, Plantation, FL 33324. ComplyRight offers a variety of legal compliance services for businesses to ensure that they comply with federal, state and local employment laws.

## JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds $5 million, exclusive of interest and costs, and is a class action in which some members of the Class are citizens of states different than Defendant. *See* 28 U.S.C. § 1332(d)(2)(A). This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

19. This Court has personal jurisdiction over ComplyRight because, *inter alia*, it maintains its "main office" in Pompano Beach, Florida, and has sufficient minimum contacts with the state of Florida and intentionally avails itself of the consumers and markets within the state through the promotion, marketing, and sale of its products.

20. Venue properly lies in this district pursuant to 28 U.S.C. § 1391(a)(2) because ComplyRight maintains an office and conducts substantial business in this district. A substantial part of the events and/or omissions giving rise to the claims occurred, in part, within this district.

## FACTUAL ALLEGATIONS

### Company Background

21. ComplyRight's website describes its mission as follows:

> At ComplyRight, our mission is to free employers from the burden of tracking and complying with the complex web of federal, state and local employment laws, so they can stay focused on managing and growing their businesses. How do we do this? We talk to employers every day. We listen to better understand their challenges. We track federal, state and local regulatory activity. And we consult with our in-house legal research team to understand how employment regulations affect employers day-to-day.
>
> We use these insights to create practical, affordable solutions that streamline essential tasks while staying 'within the lines' of those complex laws. We complement these solutions with educational content and actionable guidance to help employers act in their own best interest while still doing right by employees.

22. Its services are listed as: "hiring and training, to time tracking and recordkeeping, to labor law posting and tax information reporting, our innovative products and services address the real-world challenges employers face every day."

23. Ironically, on multiple pages on ComplyRight's website, it advertises that maintaining its customers' security is one of its top priorities, including but not limited to the following example:


24. Similarly, yet another page of ComplyRight's website further touts its purported focus on security and the security measures it has implemented and maintains?

## STATE OF THE ART ENCRYPTION

ComplyRight Tax Solutions uses advanced 256-bit data encryption technology to block the interception of sensitive data over the internet. Encryption alters the data before it is transmitted, making it unreadable until it is unlocked with a special cyber code after it is delivered to the authorized recipient. Data is password-protected and encrypted as soon as it's entered online and stays encrypted through the entire print, mail and e-file process.

- High-grade transport encryption protects electronic transmissions to the IRS and other government agencies
- Includes encryption at rest to safeguard information stored in our systems
- Effectively blocks interception of sensitive data

25. Indeed, ComplyRight assures its website viewers that its systems are protected against unauthorized access:

## SOC CERTIFICATION

ComplyRight Tax Solutions is SOC 2-certified. This means that every step of our process has undergone rigorous examination and approval by independent auditors.


SOC 2 (Service Organization Control) certification involves a detailed review of an organization's security policies, communications, procedures and monitoring. SOC 2 is considered the global standard for service organizations that handle sensitive personal and financial data, including data centers, printing facilities, online software providers and cloud-based services.

As a SOC 2-certified organization, we can promise:

- **Security –** Our system is protected against unauthorized access, use, or modification
- **Availability –** Our system is available for operation and use as committed or agreed upon
- **Processing integrity –** Our data processing is complete, valid, accurate, timely and authorized
- **Confidentiality –** Confidential information is protected as committed or agreed upon
- **Privacy –** Our processes for collecting, using, retaining, disclosing and disposing of personal information conform with the commitments in our privacy notice, and with criteria established by the AICPA

26. Despite the foregoing numerous assurances, ComplyRight failed to adequately protect Plaintiffs' and class members' (defined below) Personal Information.

**The ComplyRight Data Breach**

27. In late May 2018, ComplyRight publicized that it suffered from a criminal cyberattack, in which the Personal Information of employees of its various business customers was accessed and/or obtained by unauthorized persons, including but not limited to their names, addresses, phone numbers, email addresses and Social Security numbers. Multiple news outlets reported that the breach took place from roughly April 20, 2018 and lasting until May 22, 2018.[1]

28. It was not until nearly three months after the initial breach that ComplyRight notified individuals affected by the Data Breach.

29. Specifically, ComplyRight published the following "ComplyRight Data Security Incident Notice" on its website, which states in pertinent part as follows:

> ComplyRight was the victim of a criminal cyberattack. In late May 2018, ComplyRight was alerted to a potential issue affecting the tax form preparation websites using our platform. Upon learning of the potential issue, we disabled the platform and remediated the issue on the website. In consultation with third-party forensic cybersecurity experts, we took swift action to secure the data of our partners, business customers and the individuals potentially impacted.
>
> The forensic investigators concluded that there was unauthorized access to our website resulting in compromise of Personal Information for some individual recipients of tax forms such as 1099 or W-2 forms. Although the forensic investigation determined the information was accessed and/or viewed, the investigators were unable to confirm whether the information was downloaded or otherwise acquired by the unauthorized user.

30. ComplyRight described the facts of the breach as follows:

> **What happened?**
>
> On May 22, 2018, ComplyRight initially learned of a potential issue involving our tax reporting web platform. After investigation, we concluded that a criminal cyberattack had targeted some of the Personal Information maintained on the websites using our platform.

[1] *See, e.g.*, https://www.securityweek.com/hr-services-firm-complyright-suffers-data-breach (last visited Jul. 26, 18).

**How did this happen?**

The investigation determined there was unauthorized access to the ComplyRight web platform that is used by various websites to prepare tax-related forms for individuals (for example, 1099 and W-2 forms). Upon learning of the issue, we disabled the platform, remediated the issue on the website, and commenced a prompt and thorough investigation using external cybersecurity professionals to determine who was potentially affected and what information was accessed or viewed. Although the investigation determined the information was accessed and/or viewed, it could not confirm if the information was downloaded or otherwise acquired by an unauthorized user.

**Who is affected?**

A portion (less than 10%) of individuals with tax forms prepared on the ComplyRight web platform were impacted by this incident. All affected individuals have been sent notifications via U.S. Mail to their last known addresses. This letter included information to help safeguard them against identity fraud, including 12 months of free credit monitoring and identity theft protection services through TransUnion.

**What information was involved?**

The investigation confirmed that the portion of the website that was accessed contained names, addresses, phone numbers, email addresses, and Social Security numbers of individual tax form recipients.

**Why did I receive a letter from ComplyRight?**

ComplyRight provides a web platform used by a number of different tax form preparation websites. On behalf of those organizations and our clients, we executed the communication plan to advise those affected as promptly as possible. This is not a scam, and we apologize for any confusion that may have arisen due to your lack of familiarity with our company.

**Why did ComplyRight have my information?**

Tax reporting forms (such as 1099s or W-2s) sent to you were prepared on a site using the ComplyRight web platform.

**How am I affected if I am a site user or employer (payer)?**

The investigation found no evidence that any user or payer information was compromised. No credit card or bank account information of users or payers was involved.

31. On July 19, 2018, Plaintiff Bohannon received a letter dated July 13, 2018, from ComplyRight, stating in pertinent part:

> We are writing with important information about a recent security incident involving some of your Personal Information that was maintained on our website. Your Personal Information was entered onto our website by, or on behalf of, your employer or payer to prepare tax related forms, for example, Forms 1099 and W-2. We wanted to provide you with information regarding the incident, share the steps we have undertaken since discovering the incident, and provide guidance on what you can do to protect yourself.
>
> *What Happened?*
>
> On or about May 22, 2018 we initially learned of a potential issue involving our website. Upon learning of the potential issue, we disabled the platform and remediated the issue on the website.
>
> *What We Are Doing*
>
> In addition, we commenced a prompt and thorough investigation using external cybersecurity professionals. The forensic investigation concluded that there was unauthorized access to our website, which occurred between April 20, 2018 and May 22, 2018. After the extensive forensic investigation, a sophisticated review of our website, and analysis of potentially impacted individuals, on June 14, 2018 we discovered that some of your Personal Information was accessed and/or viewed. Although the forensic investigation determined that your information was accessed and/or viewed on the website, it could not confirm if your information was downloaded or otherwise acquired by an unauthorized user. We are not aware of any report of identity fraud as a direct result of this incident. Nevertheless, out of an abundance of caution we wanted to make you aware of the incident.
>
> *What Information Was Involved?*
>
> Your Personal Information that was accessed and/or viewed, and may have been downloaded or otherwise acquired, by an unauthorized user included your name, address, telephone number, email address, and Social Security number

32. Based on the foregoing—and information and belief—Plaintiff and the Class' Personal Information was stolen, acquired, accessed, downloaded, and/or viewed by unauthorized persons from ComplyRight's website.

33. Furthermore, as stated in its letter, ComplyRight withheld disclosure of the Breach from Plaintiffs and the Class for nearly two months.

34. Neither the letter, the statement on Defendant's website, nor the contemporaneous statements by ComplyRight to media outlets gave any indication as to the magnitude of the Data Breach or the number of customers affected. However, upon information and belief, the ComplyRight Data Breach affected the large majority of individuals whose employers are customers/clients of ComplyRight's various business services.

35. Although ComplyRight is offering impacted individuals complimentary 12-month credit monitoring and identity protection services, that does not sufficiently protect those individuals from the prodigious number of threats that data breaches impose and is not long to eliminate all potential damage from the breach.

36. ComplyRight's own public statements confirm that the Breach will subject Plaintiffs and the Class to continued, future risk of identity theft and other damages. For instance, ComplyRight instructed consumers to "remain vigilant in reviewing … financial account statements and credit reports for fraudulent or irregular activity."

37. Because Social Security numbers do not expire and are almost impossible to change, thieves will be able to do so for years to come. This risk that will continue so long as Social Security numbers have such a critical role in consumers' financial lives.

38. The unauthorized disclosure of Social Security Numbers can be particularly damaging because Social Security Numbers cannot easily be replaced. In order to obtain a new number, a person must prove, among other things, he or she continues to be disadvantaged by the misuse. Thus, under current rules, no new number can be obtained until the damage has been done. Furthermore, as the Social Security Administration warns:

> A new number probably will not solve all your problems. This is because other governmental agencies (such as the Internal Revenue Service and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Also, because credit reporting companies use the number, along with other Personal Information, to identify your credit record, using a new number will not guarantee you a fresh start. This is especially true if your other Personal Information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you will not be able to use the old number anymore. For some victims of identity theft, a new number actually creates new problems. If the old credit card information is not associated with the new number, the absence of any credit history under the new number may make it more difficult for you to get credit. [2]

**Industry Standards and the Protection of Customer Personal Information**

39. It is well known that customer Personal Information (particularly Social Security numbers) is valuable and frequently targeted by hackers. Despite the risk of a data breach and the widespread publicity and industry alerts regarding the other notable data breaches, ComplyRight failed to take reasonable steps to adequately protect its computer systems from being breached.

40. ComplyRight is, and at all relevant times has been, aware that the Personal Information it maintains is highly sensitive and could be used for nefarious purposes by third parties, such as perpetrating identity theft and making fraudulent purchases.

41. As reflected in the screenshots above from its website, ComplyRight's various website pages acknowledges that its customers/clients expect it to adequately safeguard their employees' Personal Information.

42. ComplyRight is, or reasonably should have been, aware of the importance of safeguarding its customers' Personal Information and of the foreseeable consequences that would occur if its data security systems were breached.

---

[2] *Identity Theft and Your Social Security Number* (June 2017) at 6, http://www.ssa.gov/pubs/10064.html (last accessed Jul. 26, 2018).

43. Legitimate organizations and the criminal underground alike recognize the value in sensitive consumer personal information. Otherwise, they wouldn't pay for it or aggressively seek it. For example, in "one of 2013's largest breaches . . . not only did hackers compromise the [data] of three million customers, they also took registration data from 38 million users."[3] Similarly, in the Target data breach, in addition to card information data pertaining to 40,000 credit and debit cards, hackers stole personal information pertaining to 70,000 customers.

44. As one report has noted, "[m]any hospitality and retail sector organizations also have poor information security practices, according to Verizon's 2017 Data Breach Investigations Report."[4]

45. "Increasingly, criminals are using biographical data gained from multiple sources to perpetrate more and larger thefts."[5]

46. Fraudsters will turn to the Dark Web or other criminal resources to purchase stolen financial and personal information to perpetrate financial frauds.[6]

47. Based on the recent data breaches across the United States, Defendant knew or should have known that it was at high risk for a similar data breach.

---

[3] Verizon 2014 PCI Compliance Report, available at <http://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci2014.pdf> (hereafter "2014 Verizon Report"), at 54 (last visited March 19, 2018).

[4] https://www.bankinfosecurity.com/172-applebees-restaurants-hit-payment-card-malware-a-10699 (last visited March 20, 2018).

[5] Verizon 2014 PCI Compliance Report, available at <http://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci2014.pdf> (hereafter "2014 Verizon Report"), at 54 (last visited March 19, 2018).

[6] *See, e.g.,* "Inside The Dark Net Markets For Stolen Credit Cards", available at http://www.vocativ.com/311187/dark-net-credit-card/ (last visited March 19, 2018) (discussing the sale of hacked credit card data on online criminal black markets).

48. Indeed, Julie Conroy – research director at the research and advisory firm Aite Group – has identified that "[i]f your data was stolen through a data breach that means you were somewhere out of compliance."[7]

49. According to the Federal Trade Commission ("FTC"), the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act of 1914 ("FTC Act"), 15 U.S.C. § 45.

50. In 2007, the FTC published guidelines that establish reasonable data security practices for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of Personal Information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

51. The FTC has also published a document, entitled "Protecting Personal Information: A Guide for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[8]

---

[7] http://www.reuters.com/article/us-chipotle-cyber-idUSKBN18M2BY (last visited March 19, 2018).

[8] FTC, *Protecting Personal Information: A Guide for Business* (Nov. 2011), www.stopfraudcolorado.gov/sites/default/files/bus69-protecting-personalinformation-guide-business_0.pdf.

52. As noted above, and in light of the multitude of recent high-profile data breaches across the United States, Defendant should have been aware of the need to have adequate data security systems in place.

53. Despite this, ComplyRight failed to upgrade and maintain its data security systems in a meaningful way so as to prevent data breaches. Had ComplyRight maintained its information technology ("IT") systems and adequately protected them, it could have prevented the Data Breach.

54. As a result of industry warnings, industry practice, and multiple well-documented data breaches, Defendant was alerted to the risk associated with failing to ensure that its IT systems were adequately secured.

55. Defendant was indisputably aware of the threat of data breaches. Numerous large data breaches have targeted large companies including Target, Sally Beauty, Neiman Marcus, Michaels Stores, and Supervalu. As a result, Defendant was aware that data security inadequacies creates a real threat for infiltration by hackers. Despite the fact that Defendant was on notice of the very real possibility of consumer data theft associated with its security practices and that Defendant knew or should have known about the elementary infirmities associated with ComplyRight's security systems, it still failed to make necessary changes to its security practices and protocols.

56. Defendant, at all times relevant to this action, had a duty to Plaintiffs and members of the Class to: (a) properly secure Personal Information submitted to or collected on Defendant's website and on Defendant's internal networks; (b) encrypt Personal Information using industry standard methods; (c) use available technology to defend its systems from well-known methods of invasion; (d) act reasonably to prevent the foreseeable harms to Plaintiffs and

the Class, which would naturally result from Personal Information theft; and (e) promptly notify customers when Defendant became aware of the potential that customers' Personal Information may have been compromised.

57. Defendant negligently allowed Personal Information to be compromised by failing to take reasonable steps against an obvious threat.

58. In addition, leading up to the ComplyRight Data Breach, and during the course of the breach itself and the investigation that followed, ComplyRight failed to follow the guidelines set forth by the FTC and other data security standards.

59. As a result of the events detailed herein, Plaintiff and other members of the Class have suffered injury and damages, including, but not limited to: (i) an increased risk of identity theft and identity fraud; (ii) improper disclosure of their Personal Information; (iii) the value of their time spent mitigating the increased risk of identity theft and identity fraud; (iv) the value of their time and expenses associated with mitigation, remediation, and sorting out the risk of fraud and actual instances of fraud; and (v) deprivation of the value of their Personal Information, for which there is a well-established national and international market.

60. Plaintiff and the other Class members have suffered the foregoing damages, and will continue to suffer additional damages including but not limited to the opportunity cost and value of time that Plaintiffs and the other Class members have been already forced to expend and will continue to expend in the future to monitor their financial accounts and credit files as a result of the Data Breach.

## CLASS ALLEGATIONS

61. Plaintiffs bring this action on their own behalf, and on behalf of the following Class pursuant to FED. R. CIV. P. 23:

> All persons whose Personal Information was compromised in the ComplyRight Data Breach that occurred from at least April 20, 2018 through May 22, 2018.

62. Excluded from the Class are Defendant, its affiliates, officers, directors, assigns, successors, and the Judge(s) assigned to this case. Plaintiffs reserve the right to modify, change, or expand the definitions of the Class based on discovery and further investigation.

63. **Numerosity**: While the precise number of Class members has not yet been determined, members of the Class are so numerous that their individual joinder is impracticable, as the proposed Class appears to include many thousands of members who are geographically dispersed. Upon information and belief, the Data Breach affected people across the United States.

64. **Typicality**: Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all members of the Class were injured through ComplyRight's uniform misconduct. The same event and conduct that gave rise to Plaintiffs' claims are identical to those that give rise to the claims of every other Class member because Plaintiffs and each member of the Class had their data and Personal Information compromised in the same way by the same conduct by ComplyRight.

65. **Adequacy**: Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the Class that they seek to represent; Plaintiffs have retained counsel competent and highly experienced in class action litigation (including data breach cases); and Plaintiffs and their counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

66. **Superiority**: A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of

individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for members of the Class individually to effectively redress Defendant's wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class-action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

67. **Existence and Predominance of Common Questions of Fact and Law**: Common questions of law and fact exist as to plaintiffs and all members of the Class. These questions predominate over the questions affecting individual Class members. These common legal and factual questions include, but are not limited to, the following:

- whether ComplyRight engaged in the wrongful conduct alleged herein;
- whether ComplyRight owed a duty to Plaintiffs and members of the Class to adequately protect their Personal Information and to provide timely and accurate notice of the breach to Plaintiffs and the Class, and whether it breached these duties;
- whether ComplyRight violated federal and state laws—including but not limited to state consumer protection laws and data privacy laws (e.g., Section 5 of the FTC Act, 15 U.S.C. § 45; Indiana's data breach statute, IND. CODE § 24-4.9-3.5; the Maryland Personal Information Protection Act, MD. CODE COM. LAW §§ 14-3591, *et seq.*) thereby breaching its duties to Plaintiffs and the Class;
- whether ComplyRight knew or should have known that its computer and network systems were vulnerable to attack from hackers;
- whether ComplyRight's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its computer and network systems resulting in the loss of consumers' Personal Information;
- whether ComplyRight wrongfully failed to inform Plaintiffs and members of the Class that it did not maintain computer software and other security procedures sufficient to reasonably safeguard highly-sensitive personal data;

- whether ComplyRight failed to inform Plaintiffs and the Class of the data breach in a timely and accurate manner;
- whether ComplyRight wrongfully waited to inform Plaintiffs and Class members that their sensitive Personal Information was exposed in the security breach;
- whether ComplyRight continues to breach duties to Plaintiffs and Class;
- whether ComplyRight has sufficiently addressed, remedied, or protected Plaintiffs and Class members following the data breach and has taken adequate preventive and precautionary measures to ensure the Plaintiffs and Class members will not experience further harm;
- whether Plaintiffs and members of the Class suffered injury as a proximate result of ComplyRight's conduct or failure to act; and
- whether Plaintiffs and the Class are entitled to recover damages, equitable relief, and other relief, and the extent of the remedies that should be afforded to Plaintiffs and the Class.

68. Defendant has acted or refused to act on grounds generally applicable to Plaintiffs and the other members of the Class, thereby making appropriate final injunctive relief and declaratory relief with respect to the Class as a whole.

69. Given that Defendant has engaged in a common course of conduct as to Plaintiffs and the Class, similar or identical injuries and common law and statutory violations are involved and common questions far outweigh any potential individual questions.

70. The Class is defined in terms of objective characteristics and common transactional facts; namely, the exposure of sensitive Personal Information to cyber criminals due to Defendant's failure to protect this information and adequately warn the Class that it was breached. Class membership will be readily ascertainable from Defendant's business records.

71. Plaintiffs reserve the right to revise the above Class definitions based on facts adduced in discovery.

**COUNT I**
**Negligence**
**(On Behalf of Plaintiffs and the Class)**

72. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

73. ComplyRight obtained sensitive Personal Information from Plaintiffs and Class members in its provision of human resources services.

74. ComplyRight owed a duty to Plaintiffs and the Class to maintain confidentiality and to exercise reasonable care in safeguarding and protecting their Personal Information in ComplyRight's possession from being compromised by unauthorized persons. This duty included, *inter alia*, designing, maintaining, and testing ComplyRight's security systems to ensure that Plaintiffs' and Class members' Personal Information was adequately protected both in the process of collection and after collection.

75. ComplyRight further owed a duty to Plaintiffs and Class members to implement processes that would detect a breach of its security system in a timely manner and to timely act upon warnings and alerts.

76. ComplyRight owed a duty to Plaintiffs and Class members to provide security consistent with industry standards and requirements and to ensure that its computer systems and networks—and the personnel responsible for them—adequately protected the Personal Information of Plaintiffs and Class members whose confidential data ComplyRight obtained and maintained.

77. ComplyRight holds itself out as an expert in legal compliance, and thus knew, or should have known, of the risks inherent in collecting and storing the Personal Information of

Plaintiffs and Class members and of the critical importance of providing adequate security for that information.

78. ComplyRight's conduct created a foreseeable risk of harm to Plaintiffs and members of the Class. This conduct included but was not limited to ComplyRight's failure to take the steps and opportunities to prevent and stop the breach as described above. ComplyRight's conduct also included its decision not to comply with industry standards for the safekeeping and maintenance of Plaintiffs' and Class members' Personal Information.

79. ComplyRight knew or should have known that it had inadequate computer systems and data security practices to safeguard such information, and ComplyRight knew or should have known that hackers were attempting to access the Personal Information in databases such as ComplyRight's.

80. ComplyRight breached the duties it owed to Plaintiffs and members of the Class by failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the Personal Information of Plaintiffs and members of the Class, as identified above. This breach was a proximate cause of injuries and damages suffered by Plaintiffs and Class members.

81. As a direct and proximate result of ComplyRight's negligent conduct, Plaintiffs and Class members have suffered injury and are entitled to damages in an amount to be proven at trial. ComplyRight's violations of its duties of care were conducted with reckless indifference toward the rights of others, such that an award of punitive damages is appropriate.

**COUNT II**
**Negligence *Per Se***
**(On Behalf of Plaintiffs and the Class)**

82. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

83. Pursuant to Section 5 of the FTC Act, 15 U.S.C. § 45 (among the other state consumer data privacy laws), ComplyRight had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' Personal Information.

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

85. ComplyRight violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Personal Information and not complying with applicable industry standards as described in detail herein. ComplyRight's conduct was particularly unreasonable given the nature and amount of Personal Information it collected and stored—which included highly sensitive Social Security numbers—and the foreseeable consequences of a breach, including, specifically, the immense damages that would result to consumers.

86. The harm that has occurred is the type of harm the FTC Act (and similar state statutes) is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, as a result of their failure to employ reasonable data security

measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

87. ComplyRight had a duty to Plaintiffs and Class members to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and Class members' Personal Information.

88. ComplyRight breached its duties to Plaintiffs and Class members under the FTC Act (and similar state statutes), by failing to provide fair, reasonable, or adequate data security practices to safeguard Plaintiffs' and Class members' Personal Information.

89. ComplyRight's violation of Section 5 of the FTC Act (and similar state statutes) and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

90. But for ComplyRight's wrongful and negligent breach of its duties owed to Plaintiffs and Class members, Plaintiffs and Class members would not have been injured.

91. The injury and harm suffered by Plaintiffs and Class members was the reasonably foreseeable result of ComplyRight's breach of its duties. ComplyRight knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiffs and Class members to suffer the foreseeable harm associated with the exposure of their sensitive Personal Information.

92. As a direct and proximate result of ComplyRight's negligence *per se*, Plaintiffs and Class members have suffered harm, including but not limited to improper disclosure of their Personal Information; loss of time and money resolving fraudulent charges; loss of time and money incurred to mitigate the effects of the breach; lost control over the value of Personal Information; unreimbursed losses relating to fraudulent charges; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of

unauthorized use of stolen Personal Information, entitling them to damages in an amount to be proven at trial.

**COUNT III**
**Breach of Implied Contract**
**(On Behalf of Plaintiffs and the Class)**

93. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

94. Plaintiffs and Class members whose Personal Information is obtained by ComplyRight in connection with its provision of human resources services have valid, binding, and enforceable implied contracts or with ComplyRight.

95. Specifically, Plaintiffs and Class members agreed to the release of their sensitive Personal Information to ComplyRight to be used in connection with its provision of third-party human resources services. In exchange, ComplyRight agreed, among other things: (1) to provide third-party human resources services to Plaintiffs and Class members; (2) to take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class members' Personal Information; and (3) to protect Plaintiffs' and Class members' Personal Information in compliance with federal and state laws and regulations and industry standards.

96. Protection of Personal Information is a material term of the implied contracts between Plaintiffs and Class members, on the one hand, and ComplyRight, on the other hand. Plaintiffs and Class members consented—implicitly or explicitly—to the release of their sensitive Personal Information to ComplyRight. Had Plaintiffs and Class members known that ComplyRight would not adequately protect their Personal Information, they would not have consented to or protested their Personal Information being provided ComplyRight.

97. ComplyRight did not satisfy its promises and obligations to Plaintiffs and Class members under the implied contracts because it did not take reasonable measures to keep Plaintiffs' and Class members' Personal Information secure and confidential and did not comply with the applicable laws, regulations, and industry standards.

98. ComplyRight materially breached its implied contracts with Plaintiffs and Class members by failing to implement adequate data security measures.

99. Plaintiffs and Class members fully performed their obligations under their implied contracts with ComplyRight.

100. ComplyRight's failure to satisfy its obligations led directly to the successful intrusion of ComplyRight's computer servers and stored Personal Information and led directly to unauthorized parties access and exfiltration of Plaintiffs' and Class members' sensitive Personal Information.

101. ComplyRight breached these implied contracts as a result of its failure to implement adequate data security measures.

102. Also, as a result of ComplyRight's failure to implement the security measures, Plaintiffs and Class members have suffered actual damages resulting from the theft of their Personal Information and remain at imminent risk of suffering additional damages in the future.

103. Alternatively, Plaintiffs and each of the members of the Class are intended third-party beneficiaries of any contracts between ComplyRight, on the one hand, and the employers or entities that utilized ComplyRight's human resources services and provided Plaintiffs' and Class members Personal Information to ComplyRight, on the other hand.

104. Accordingly, Plaintiffs and Class members have been injured as a proximate result of ComplyRight's breaches of implied contracts and are entitled to damages and/or restitution in an amount to be proven at trial.

**COUNT IV**
**Breach of Contracts to Which Plaintiffs and Class Members Were Third Party Beneficiaries**
**(On Behalf of Plaintiffs and the Class)**

105. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

106. Upon information and belief, Plaintiffs and Class members are intended third party beneficiaries of contracts entered into between Defendant and third parties, such as the employers for which Plaintiffs and the Class work that retained ComplyRight for its third party human resources services.

107. Upon information and belief, these contracts between ComplyRight and third parties require, *inter alia*, that ComplyRight takes appropriate steps to safeguard the Personal Information of Plaintiffs and the Class.

108. Upon information and belief, ComplyRight has saved (or avoided spending) a substantial sum of money by not complying with its contractual obligations. Instead, many of these costs have been incurred by Plaintiffs and Class members.

109. Defendant breached these agreements by, *inter alia*, failing to adequately safeguard their sensitive Personal Information. This has directly caused injuries to Plaintiffs and the Class.

**COUNT V**
**Violations of the Indiana Deceptive Consumer Sales Act**
**IND. CODE §§ 24-5-0.5-1, *et seq.* ("IDCSA")**
**(On Behalf of Plaintiff Bohannon and the Class)**

110. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

111. ComplyRight is a "person" as defined by IND. CODE § 24-5-0.5-2(a)(2).

112. ComplyRight is a "supplier" as defined by § 24-5-0.5-2(a)(1), because it regularly engages in or solicits "consumer transactions," within the meaning of § 24-5-0.5-2(a)(3)(A).

113. Plaintiff and other members of the Class were subjected to ComplyRight's unfair, deceptive, and abusive acts or practices in violation of the IDCSA, in failing to properly implement adequate, reasonable security measures to protect their Personal Information and in failing to provide adequate, reasonable, and timely notification of the breach.

114. ComplyRight willfully ignored the clear and present risk of a security breach of its systems and failed to implement and maintain reasonable security measures to prevent, detect, and mitigate the breach.

115. ComplyRight's representations and omissions include both implicit and explicit representations. For example, ComplyRight made misrepresentations on its website regarding the strength and adequacy of its security measures when in fact its systems were vulnerable to unauthorized access.

116. ComplyRight benefitted from not taking preventative measures and implementing adequate security measures that would have prevented, detected, and mitigated the data breach.

117. ComplyRight's conduct alleged herein offends public policy and is immoral, unethical, oppressive, and unscrupulous, and causes substantial injury to consumers. Defendant specifically violated the IDCSA, by engaging in (but not limited to) the following conduct:

- Failing to maintain sufficient security to keep Plaintiff's and The Class members' sensitive Personal Information from being breached and stolen;

- Misrepresenting and fraudulently advertising (or omitting) material facts by representing and advertising that it would (or omitting that it would not) maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's and The Class members' Personal Information from unauthorized disclosure, release, data breaches, and theft;

- Misrepresenting (or omitting) material facts to Plaintiff and the Class by representing and advertising that it did and would (or omitting that it would not) comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff's and The Class members' sensitive Personal Information;

- Omitting, suppressing, and concealing the material fact of the inadequacy of the data privacy and security protections for Plaintiff's and The Class members' Personal Information;

- Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Plaintiff's and The Class members' sensitive Personal Information in violation of duties imposed by and public policies reflected in applicable federal and state laws resulting in the data breach. These unfair acts and practices violated duties imposed by laws including the FTC Act (15 U.S.C. § 45) and Indiana's data breach statute (IND. CODE § 24-4.9-3.5); and

- Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the data breach to Plaintiff and The Class members in a timely and accurate manner, contrary to the duties imposed by IND. CODE § 24-4.9-3.3.

118. ComplyRight's acts and practices were "unfair" because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

119. The injury to consumers from ComplyRight's conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury and an unwarranted risk to the safety of their Personal Information or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant

number of consumers, but also because it inflicted a significant amount of harm on each consumer.

120. Plaintiff Bohannon and the other The Class members had no reasonable alternatives or chance to avoid the harm. Plaintiff Bohannon and the other The Class members largely had no idea that ComplyRight maintained their information at all, let alone had the negotiating power individually to demand adequate data security. By withholding important information from consumers about the inadequacy of its data security, ComplyRight created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

121. ComplyRight's acts and practices were "abusive" for numerous reasons, including:

(a) Because they took unreasonable advantage of consumers' inability to protect their own interests. Consumers could not protect their interests due to the asymmetry in information between them and ComplyRight concerning the state of its security (indeed, most Class members did not even know ComplyRight was handling their Personal Information); and

(b) Because ComplyRight took unreasonable advantage of consumers' reasonable reliance that it would acting in their interests to secure their data.

122. ComplyRight also engaged in "deceptive" acts and practices in violation of Indiana Code § 24-5-0.5-3(a) and § 24-5-0.5-3(b), including:

(a) Misrepresenting that the subject of a consumer transaction has sponsorship, approval, performance, characteristics, accessories, uses, or

benefits it does not have which the supplier knows or should reasonably know it does not have;

(b) Misrepresenting that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not and if the supplier knows or should reasonably know that it is not; and

(c) Misrepresenting that the subject of a consumer transaction will be supplied to the public in greater quantity (i.e., more data security) than the supplier intends or reasonably expects.

123. ComplyRight's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of its data security and ability to protect the confidentiality of consumers' Personal Information.

124. As a direct and proximate result of Defendant's deceptive trade practices, Plaintiff Bohannon and the Class members suffered injuries, including the loss of their legally protected interest in the confidentiality and privacy of their Personal Information and damages.

125. The above unfair and deceptive practices and acts by Defendant were done as part of a scheme, artifice, or device with intent to defraud or mislead and constitute incurable deceptive acts under the IDCSA.

126. ComplyRight's conduct and acts are incurable for the reasons set forth herein, including but not limited to because Plaintiff's and the Class members' sensitive Personal Information—including their Social Security numbers—have been indefinitely exposed to the risk that this information will be used for nefarious purposes by fraudsters. Nothing that ComplyRight can or may do will cure this harm.

127. Indeed, as a self-touted expert in compliance, ComplyRight knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff's and the Class members' Personal Information and that risk of a data breach and data theft was highly likely. Given this knowledge, an intent to defraud was clearly present on the part of ComplyRight or it can be inferred from the circumstances.

128. ComplyRight acted intentionally, knowingly, and maliciously to violate the IDCSA, and recklessly disregarded Plaintiff and The Class members' rights. ComplyRight was on notice that its security and privacy protections were inadequate given the multitude of recent high-profile data breaches. ComplyRight's actions were not the result of a mistake of fact or law, honest error or judgment, overzealousness, or other human failing.

129. Plaintiff Cook and the Class members seek relief under IND. CODE § 24-5-0.5-4, including, not limited to damages, restitution, penalties, injunctive relief, reasonable attorneys' fees and costs, and punitive damages. Senior members of the Class injured by Defendant's unfair and deceptive trade practices also seek treble damages pursuant to IND. CODE §24-5-0.5-4(i).

**COUNT VI**
**Violations of the Maryland Personal Information Protection Act**
**MD. CODE COM. LAW §§ 14-3591, *et seq.* ("MPIPA")**
**(On Behalf of Plaintiff Buckingham and the Class)**

130. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

131. Under the MPIPA, "[t]o protect Personal Information from unauthorized access, use, modification, or disclosure, a business that owns or licenses Personal Information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of Personal Information owned or licensed and the nature and size of the business and its operations." MD. COMM. CODE § 14-3503(a).

132. ComplyRight is a business that owns or licenses computerized data that includes Personal Information as defined by MD. COMM. CODE §§ 14-3501(b)(1) and (2).

133. Plaintiff Buckingham and The Class members are "individuals" and "customers" as defined and covered by MD. COMM. CODE §§ 14-3502(a) and 14-3503.

134. Plaintiff's and The Class members' Personal Information includes Personal Information as covered under MD. COMM. CODE § 14-3501(d).

135. ComplyRight did not maintain reasonable security procedures and practices appropriate to the nature of the Personal Information owned or licensed and the nature and size of its business and operations in violation of MD. COMM. CODE § 14-3503.

136. The data breach was a "breach of the security of a system" as defined by MD. COMM. CODE § 14-3504(1).

137. Under MD. COMM. CODE § 14-3504(b)(1), "[a] business that owns or licenses computerized data that includes Personal Information of an individual residing in the State, when it discovers or is notified of a breach of the security system, shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that Personal Information of the individual has been or will be misused as a result of the breach."

138. Under MD. COMM. CODE §§ 14-3504(b)(2) and 14-3504(c)(2), "[i]f, after the investigation is concluded, the business determines that misuse of the individual's Personal Information has occurred or is reasonably likely to occur as a result of a breach of the security system, the business shall notify the individual of the breach" and that notification "shall be given as soon as reasonably practical after the business discovers or is notified of the breach of a security system."

139. Because ComplyRight discovered a security breach and had notice of a security breach, it had an obligation to disclose the breach in a timely and accurate fashion as mandated by MD. COMM. CODE §§ 14-3504(b)(2) and 14-3504(c)(2). It did not do this, waiting multiple months to disclose and inform consumers of the breach.

140. By failing to disclose the breach in a timely and accurate manner, ComplyRight violated MD. COMM. CODE §§ 14-3504(b)(2) and 14-3504(c)(2).

141. As a direct and proximate result of ComplyRight's violations of the MPIPA, Plaintiff and The Class members suffered damages, as described herein.

142. Pursuant to MD. COMM. CODE § 14-3508, ComplyRight's violations of MD. COMM. CODE §§ 14-3504(b)(2) and 14-3504(c)(2) are unfair or deceptive trade practices within the meaning of the MCPA, MD. COMM. CODE §§ 13-101, *et seq*. and subject to the enforcement and penalty provisions contained within the MCPA.

143. Plaintiff and The Class members seek relief under MD. COMM. CODE §13-408, including actual damages and attorney's fees.

**COUNT VII**
**Violations of the Maryland Social Security Number Privacy Act**
**MD. COMM. CODE §§ 14-3401, et seq. ("MSSNPA")**
**(On Behalf of Plaintiff Buckingham and the Class)**

144. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

145. ComplyRight is a "person" as covered by MD. COMM. CODE § 14-3402.

146. Plaintiff and The Class members are "individual[s]" covered by MD. COMM. CODE § 14-3402.

147. MD. COMM. CODE § 14-3402 prohibits a person from requiring an individual to transmit his/her Social Security number over the Internet unless the connection is secure or the

individual's Social Security number is encrypted, and from initiating the transmission of an individual's Social Security number over the Internet unless the connection is secure or the Social Security number is encrypted.

148. As described above, ComplyRight transmitted Plaintiff's and The Class members' Social Security numbers over the Internet on unsecure connections and/or without encrypting the Social Security Numbers in violation of MD. COMM. CODE § 14-3402.

149. As a direct and proximate result of ComplyRight's violations of MD. COMM. CODE § 14-3402, Plaintiff and The Class members suffered damages, as described above.

150. Plaintiff and The Class members seek relief under MD. COMM. CODE § 14-3402, including actual damages and attorneys' fees.

**COUNT VIII**
**Violations of the Maryland Consumer Protection Act**
**MD. CODE COM. LAW §§ 13-101, *et seq.* ("MCPA")**
**(On Behalf of Plaintiff Buckingham and the Class)**

151. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

152. ComplyRight is a person as defined by MD. COMM. CODE § 13-101(h).

153. ComplyRight's conduct as alleged herein related to "sales," "offers for sale," or "bailment" as defined by MD. COMM. CODE § 13-101(i) and § 13-303.

154. The Class members are "consumers" as defined by MD. COMM. CODE § 13-101(c).

155. ComplyRight advertises, offers, or sell "consumer goods" or "consumer services" as defined by MD. COMM. CODE § 13-101(d).

156. ComplyRight advertised, offered, or sold goods or services in Maryland and engaged in trade or commerce directly or indirectly affecting the people of Maryland.

157. ComplyRight engaged in unfair and deceptive trade practices, in violation of MD. COMM. CODE § 13-301, including:

(a) False or misleading oral or written representations that have the capacity, tendency, or effect of deceiving or misleading consumers;

(b) Representing that consumer goods or services have a characteristic that they do not have;

(c) Representing that consumer goods or services are of a particular standard, quality, or grade that they are not;

(d) Failing to state a material fact where the failure deceives or tends to deceive;

(e) Advertising or offering consumer goods or services without intent to sell, lease, or rent them as advertised or offered;

(f) Deception, fraud, false pretense, false premise, misrepresentation, or knowing concealment, suppression, or omission of any material fact with the intent that a consumer rely on the same in connection with the promotion or sale of consumer goods or services or the subsequent performance with respect to an agreement, sale lease or rental.

158. ComplyRight engaged in these unfair and deceptive trade practices in connection with offering for sale or selling consumer goods or services or with respect to the provision of human resources services, in violation of MD. COMM. CODE § 13-303, including:

(a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and The Class members' Personal

Information, which was a direct and proximate cause of the ComplyRight data breach;

(b) Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the ComplyRight data breach;

(c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and The Class members' Personal Information, including duties imposed by, *inter alia*, the FTC Act, 15 U.S.C. § 45, and the MPIPA, which was a direct and proximate cause of the ComplyRight data breach;

(d) Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and The Class members' Personal Information, including by implementing and maintaining reasonable security measures;

(e) Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and The Class members' Personal Information, including duties imposed by, *inter alia*, the FTC Act, 15 U.S.C. § 45, and the MPIPA;

(f) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and The Class members' Personal Information; and

(g) Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security

and privacy of Plaintiff and The Class members' Personal Information, including duties imposed by, *inter alia*, the FTC Act, 15 U.S.C. § 45, and the MPIPA.

159. ComplyRight's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of ComplyRight's data security and ability to protect the confidentiality of consumers' Personal Information.

160. Had ComplyRight disclosed that its data systems were not secure and, thus, vulnerable to attack, Plaintiff and the Class members would have been able to protect themselves against ComplyRight's vulnerable systems (i.e., by avoiding their services) and ComplyRight would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, ComplyRight held itself out as a company that has expertise in legal compliance, and ComplyRight was trusted with sensitive and valuable Personal Information regarding thousands of consumers, including Plaintiff and the Class. ComplyRight accepted the responsibility of being a bailee of sensitive data while keeping the inadequate state of its security controls secret from the public.

161. ComplyRight acted intentionally, knowingly, and maliciously to violate the MCPA, and recklessly disregarded Plaintiff and The Class members' rights. Given the large number of recent high-profile data breaches, ComplyRight was on notice that its security and privacy protections were inadequate.

162. As a direct and proximate result of ComplyRight's unfair and deceptive acts and practices, Plaintiff and The Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for

fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

163. Plaintiff and The Class members seek all monetary and nonmonetary relief allowed by law, including damages, disgorgement, injunctive relief, and attorneys' fees and costs.

**PRAYER FOR RELIEF**

Plaintiffs, on behalf of themselves and the Class, respectfully request that the Court grant the following relief:

A. Certify this case as a class action pursuant to FED. R. CIV. P. 23(a) and (b)(3), and, pursuant to FED. R. CIV. P. 23(g), appoint Plaintiffs as Class representatives and their counsel as Class counsel.

B. Award Plaintiffs and the Class appropriate monetary relief, including actual damages, restitution, disgorgement, and punitive damages.

C. Award Plaintiffs and the Class equitable, injunctive and declaratory relief as may be appropriate. Plaintiffs, on behalf of the Class, seek appropriate injunctive relief designed to ensure against the recurrence of a data breach by adopting and implementing best security data practices to safeguard customers' Personal Information, extend long-term credit monitoring services and similar services to protect against all types of identity theft, and to provide elevated credit monitoring services to minor and elderly Class members who are more susceptible to fraud and identity theft.

D. Award Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowable.

E. Award Plaintiffs and the Class reasonable attorneys' fees and costs as allowable.

F. Award Plaintiffs and the Class such other favorable relief as allowable under law or at equity.

Dated: July 26, 2018

Respectfully submitted,

*/s/ Seth M. Lehrman*
Seth M. Lehrman (Fla. Bar No. 132896)
E-mail: seth@epllc.com
EDWARDS POTTINGER LLC
425 North Andrews Avenue, Suite 2
Fort Lauderdale, FL 33301
Telephone: 954-524-2820
Facsimile: 954-524-2822

Benjamin F. Johns (*Pro Hac Vice to be filed*)
E-mail: bfj@chimicles.com
Andrew W. Ferich (*Pro Hac Vice to be filed*)
E-mail: awf@chimicles.com
Mark B. DeSanto (Fla. Bar No. 107688)
E-mail: mbd@chimicles.com
CHIMICLES & TIKELLIS LLP
One Haverford Centre
361 W. Lancaster Avenue
Haverford, PA 19041
Telephone: 610-642-8500

*Counsel for Plaintiffs and the Putative Class*