Danielle L. Perry (SBN 292120)
dperry@masonllp.com
Gary E. Mason (*pro hac vice forthcoming)*
gmason@wbmllp.com
MASON LIETZ & KLINGER LLP
5101 Wisconsin Ave. NW, Ste. 305
Washington, DC 20016
Tel: 202-429-2290
Fax: 202-429-2294

(other counsel listed on signature page)

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF CALIFORNIA

DOUGLAS DYRSSEN SR., individually and on behalf of all others similarly situated,

Plaintiff,

v.

NATIONAL WESTERN LIFE INSURANCE COMPANY and NATIONAL WESTERN LIFE GROUP, INC.,

Defendants.

CASE NO. 21-225

CLASS ACTION COMPLAINT

Filed: March 8, 2021

1. Plaintiff DOUGLAS DYRSSEN SR. ("Plaintiff"), individually and on behalf of all others similarly situated, brings this action against Defendants NATIONAL WESTERN LIFE INSUANCE COMPANY and NATIONAL WESTERN LIFE GROUP, INC. ("National Western" or "Defendants"), to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendants. Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of his counsel, and the facts that are a matter of public record:

NATURE OF THE ACTION

2. This class action arises out of the recent targeted cyber-attack against Defendants that allowed a third party to access Defendants' computer systems and data, resulting in the removal of at least 656 Gigabytes ("GB") of highly sensitive personal information belonging to thousands of customers from Defendants' computer networks (the "Cyber-Attack").

3. As a result of the Cyber-Attack, Plaintiff and Class Members suffered ascertainable losses in the form of loss of the value of their private and confidential information, loss of the benefit of their contractual bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

4. Plaintiff's and Class Members' sensitive personal information—which was entrusted to Defendants, their officials and agents—was compromised, unlawfully accessed, and stolen due to the Cyber-Attack. Information compromised in the Cyber-Attack includes names and the following: life insurance or annuity policy number, Social Security Number and financial account Information (collectively the "Private Information").

5. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendants' inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other

Class Members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

6. Defendants maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendants' computer network in a condition vulnerable to cyberattacks of this type.

7. Upon information and belief, the mechanism of the cyber-attack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known and foreseeable risk to Defendants, and Defendants were on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

8. In addition, Defendants and their employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendants properly monitored its property, it would have discovered the intrusion sooner.

9. Because of the Cyber-Attack, Plaintiff and Class members suffered injury and damages in the form of theft and misuse of their Private Information.

10. What's more, Plaintiff's and Class Members' identities are now at risk because of Defendants' negligent conduct since the Private Information that Defendants collected and maintained is now in the hands of known data thieves – the REvil ransomware operators.

11. Armed with the Private Information accessed in the Cyber-Attack, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in class members' names, taking out loans in class members' names, using class members' names to obtain medical services, using class members' health information to target other phishing and hacking intrusions based on their individual health needs, using class members' information to obtain government benefits, filing fraudulent tax returns using class members' information, obtaining driver's licenses in class

members' names but with another person's photograph, and giving false information to police during an arrest.

12. As a further result of the Cyber-Attack, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

13. Plaintiff and Class Members have and may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

14. As a direct and proximate result of the Cyber-Attack and subsequent data breach, Plaintiff and Class Members have suffered and will continue to suffer damages and economic losses in the form of: 1) the loss of time needed to: take appropriate measures to avoid unauthorized and fraudulent charges; change their usernames and passwords on their accounts; investigate, correct and resolve unauthorized debits, charges, and fees charged against their accounts; and deal with spam messages and e-mails received as a result of the Data Breach. Plaintiff and Class Members have likewise suffered and will continue to suffer an invasion of their property interest in their own personally identifying information ("PII") such that they are entitled to damages for unauthorized access to and misuse of their PII from Defendants. And, Plaintiff and Class Members will suffer from future damages associated with the unauthorized use and misuse of their PII as thieves will continue to use the stolen information to obtain money and credit in their name for several years.

15. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed and/or removed from the network during the Cyber-Attack.

16. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendants'

data security systems, future annual audits, and adequate credit monitoring services funded by Defendants.

17. Accordingly, Plaintiff brings this action against Defendants seeking redress for their unlawful conduct asserting claims for negligence, breach of implied contract, and breach of fiduciary duty.

PARTIES

18. Plaintiff Douglas Dyrssen Sr. is, and at all times mentioned herein was, an individual citizen of the State of California residing in Modesto, California. Plaintiff Dyrssen was and is a policyholder of Defendant National Western Life Insurance Company. Plaintiff Dyrssen received notice from Defendants that the Data Breach had occurred following an attack on Defendants' computer systems, and that his personal data was involved. A copy of the notice is attached hereto as Exhibit A.

19. Defendant National Western Life Insurance Company is a Colorado corporation with its principal place of business at 10801 N Mopac Expressway, Bldg. 3, Austin, Texas 78759, and is a wholly owned subsidiary of Defendant National Western Life Group, Inc.

20. Defendant National Western Life Group, Inc. is a Delaware corporation with its principal place of business at 10801 N Mopac Expressway, Bldg. 3, Austin, Texas 78759, and is the parent corporation of Defendant National Western Life Insurance Company.

JURISDICTION AND VENUE

21. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). There are at least 100 putative Class Members, the aggregated claims of the individual Class Members exceed the sum or value of $5,000,000 exclusive of interest and costs, and Plaintiff Dyrssen and members of the proposed Class are citizens of states different from Defendants.

22. This Court has jurisdiction over Defendants through their business operations in this District, the specific nature of which (i.e. the sale of insurance policies and the gathering of personal information) occurs in this District. Defendants intentionally avail themselves of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

23. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District, and because Plaintiff Dyrssen resides in this judicial district.

FACTUAL ALLEGATIONS

Defendants' Business

24. Defendant National Western Life Group, Inc. is the parent holding company of National Western Life Insurance Company, Ozark National Life Insurance Company, and various non-insurance subsidiaries. It is headquartered in Austin, Texas, is incorporated in Delaware, and in 2019 had $12.6 billion in total consolidated assets.

25. National Western Life Group, Inc. was formed by and then acquired Defendant National Western Life Insurance Company on October 1, 2015.

26. Defendant National Western Life Insurance Company is a stock life insurance company offering a broad portfolio of individual universal life, whole life and term insurance plans, annuity products, and investment contracts meeting the financial needs of its customers in 49 states, the District of Columbia, and certain U.S. territories or possessions.

27. National Western Life Insurance Company was founded in 1956, and in 2019 it had 287 Home office employees, 120,000 annuity contracts, and $17.1 billion of life insurance in force.

28. There is a unity of identity between the Defendants, with National Western Life Insurance Company being a wholly owned subsidiary of National Western Life Group, Inc. The

two Defendants have common members of their boards of directors, with Ross R. Moody, David S. Boone, Stephen E. Glasgow, and E.J. Pederson serving on the boards of both entities.

29. The two entities also share common corporate officers, with Ross R. Moody serving as President and Chief Executive Officer of both entities, Rey Perez serving as Senior Vice President of the parent entity and President and Chief Operating Officer of the subsidiary, Brian M. Pribyl serving as Chief Financial Officer and Treasurer of both entities, and Gina Byrne Miller serving as Chief Legal Officer and Secretary of both entities.

30. The two entities operate out of the same headquarters location in Austin, Texas, where they share executive offices.

31. Defendants describe themselves as leading innovators in equity-indexed universal life products.

32. Defendants are in the business of selling annuities, life insurance, and "high quality insurance products that meet the financial security needs of well-defined market segments."

33. In the ordinary course of doing business with Defendants, customers are required to provide Defendants with sensitive, personal and private information such as:

- Names;
- Postal Addresses;
- Unique Personal Identifiers;
- Online Identifiers;
- Internet Protocol (IP) addresses;
- Email addresses;
- Dates of birth
- Social Security numbers;
- Driver's license numbers;

- Passport numbers;
- Financial account information (including credit and debit card numbers);
- Tax identification numbers;
- Information on liability;
- Information on assets;
- Employment history;
- Information on Income;
- Creditworthiness and credit history;
- Health history and status;
- Medical information;
- Marital status;
- Medical condition;
- Physical and mental disability;
- General reputation;
- Mode of living;
- Sexual orientation;
- Other information that may be deemed necessary to financial services.

34. As a condition of becoming a policyholder with Defendants, Plaintiff Dyrssen was required to disclose some or all of the Private Information listed above.

35. Defendants have promulgated, and place on their website, privacy policies for all of the jurisdictions in which they operate, including California.

36. All of Defendants' privacy policies prominently state "We Value Your Privacy," and go on to declare "National Western Life values its relationship with you. Protecting the privacy of information we have about you is of great importance to us. We want you to understand how we

protect the confidentiality and security of that information, as well as how and why we use and disclose it."[1]

37. In the course of collecting Private Information from consumers, including Plaintiff Dyrssen, Defendants promise to provide confidentiality and security for customer data.

38. Because of the highly sensitive and personal nature of the Private Information Defendants acquire and store with respect to its consumers, Defendants further promise to "restrict access to personal information about you to those employees and agents who need to know that information to provide products or services to you. We maintain physical, electronic, and procedural safeguards that comply with state and federal regulations to guard your personal information."[2]

The Cyber-Attack and Data Breach

39. On August 15, 2020, Defendants discovered a malware incident impacting certain company computer systems.

40. Beginning on August 7, 2020 and possibly earlier, known cybercriminals gained unauthorized access to Defendants' computer systems and networks and acquired copies of Private Information held on Defendants' systems.

41. Defendants did not discover that unauthorized persons had gained access to their computer systems for over a week (from at least August 7, 2020 to August 15, 2020), and only became aware of the unauthorized access when the cyberthieves infected Defendants' IT systems with malicious software (aka malware).

42. The malware deployed "ground to a halt," Defendants' computer systems "with at least one employee reporting that there were "no systems up."[3]

[1] https://nwlstaticassets.azureedge.net/nwlwebsitedocumentstore/nwl-com/SP-8280-CA.pdf (last accessed March 2, 2021)
[2] *Id.*
[3] https://cybleinc.com/2020/08/24/national-western-life-insurance-company-nightmare-continues/ (last accessed March 1, 2021)

43. The malware – a form of ransomware deployed by known cybercriminals (the REvil ransomware operators) also encrypted and locked out employee access to files.

44. On August 18, 2020, an independent data security research team identified a leak disclosure post on the internet, in which the REvil ransomware operators claimed to have breached Defendants computer systems, and claimed to have stolen 656 gigabytes of confidential data, consisting of 25110 folders containing 453695 files.

45. In that same leak disclosure post, the REvil ransomware operators posted screenshots on the internet, including a snapshot of Defendants' database files, passport copies of family members of Defendants' CEO, corporate contract agreements, information about Defendants' clients, and other information.

46. On August 23, 2020, the REvil ransomware operators published another leak disclosure post online in which they claim to have access to Defendants' company emails.

47. The REvil ransomware operators also placed online and released a data archive containing approximately 1% of the total amount of data stolen.

48. Analysis of the stolen files posted by the cyberthieves in the online archive showed that the data stolen included the Private Information of Defendants' customers, including customer Social Security numbers, dates of birth, full names, dates of death, state of residence, policy numbers, and policy termination dates.

49. The cybercriminals also posted online internal Defendant company emails, showing that as late as August 23, 2020, Defendants had not managed to unencrypt their encrypted files.

50. Forensic investigation later confirmed that between August 7, 2020 and August 10, 2020, the data that the cyberthieves claimed to have stolen had in fact been taken ("exfiltrated") from Defendants' computer systems.

51. The cyber-attack was specifically targeted at Defendants, as the REvil ransomware operators posted public messages online indicating that they were contacted by a representative of a competitor company to compromise Defendants' networks, and that the competitor "offered us a good amount to satisfy our work in the National Western Life Infrastructure."[4]

52. The cyber-attack was also expressly designed and targeted to gain access to private and confidential data, including (among other things) the PII of Defendants' customers and clients. Evidence of this specific targeting of Private Information is the compromise and theft of the passports of the company CEO's family members. The REvil ransomware operators also sought payment directly from Defendants' clients whose Private Information was compromised and stolen, which is further evidence of the specific targeting.

53. Despite learning of the Cyber-Attack on or about August 15, 2020, Defendants failed to make a timely and adequate response to the Cyber-Attack. Based upon the public postings from the REvil ransomware operators, files were still encrypted as late as August 23, 2020, and possibly later.

54. Moreover, letters written on Defendants' behalf indicate that while Defendants alleged employed third-party investigators "immediately" "to determine the nature and scope" of the Cyber-Attack, it was not until on or about September 29, 2020 that "a third-party firm was engaged to programmatically and manually review the files at issue to identify all impacted individuals and the types of data associated with those individuals."[5]

55. Even worse, despite learning of the Cyber-Attack on August 15, 2020, and despite the facts that A) the REvil ransomware operators were publicly posting customer data online in

[4] https://healthitsecurity.com/news/ransomware-hacking-groups-post-data-from-5-healthcare-entities (last accessed March 2, 2021)

[5] https://www.doj.nh.gov/consumer/security-breaches/documents/national-western-life-insurance-20210120.pdf (last accessed March 2, 2021)

August 2020, and also B) were contacting Defendants' affected customers directly in August 2020 seeking ransoms for stolen data, Defendants only began providing notice of the data breach to its customers beginning on or about January 14, 2021, in derogation of multiple state data breach notification statutes that requires notice as soon as possible, without unreasonable delay, or within a certain amount of time (typically 30 to 60 days after discovery of the data breach).

56. Compounding the problem, Defendants' initial notice of data breach letters contained no information about the types of personal information impacted by the Cyber-Attack, and Defendants had to issue supplemental notices indicating that the stolen information contained Social Security numbers, life insurance or annuity policy numbers, and financial account information.

57. Outside experts have criticized companies that allowed their data to be breached, and who then delayed in notifying customers, downplaying the risk. Kate Borten, president of the privacy and security consulting firm The Marblehead Group, has stated (in the context of a healthcare related data breach:

"Notification delay raises the risk of harm to patients . . . If patients are unaware that their information has been compromised, they cannot take protective steps."[6]

58. Based on the Notice of Data Breach letters he received (Exhibits A to this Complaint), which informed Plaintiff that his Private Information was removed from Defendants' network and computer systems, Plaintiff believes his Private Information was stolen from Defendants' networks (and subsequently sold) in the Cyber-Attack.

59. Further, the removal of the Private Information from Defendants' system – information that included full names, dates of birth, and Social Security numbers (which are the keys to identity theft and fraud) -- demonstrates that this cyberattack was targeted.

[6] https://www.healthcareinfosecurity.com/notification-breach-affecting-219000-delayed-a-15986 (last accessed 2/22/2021)

60. Defendants had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

61. Plaintiff and Class Members provided their Private Information to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

62. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches in the banking/credit/financial services industry preceding the date of the breach.

63. Data breaches, including those perpetrated against the banking/credit/financial sector of the economy, have become widespread.

64. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[7]

65. Of the 1,473 recorded data breaches, 108 of them were in the banking/credit/financial industry, with the number of sensitive records being exposed exceeding 100 million. In fact, over 62% of the 164 million sensitive records exposed in data breaches in 2019 were exposed in those 108 breaches in the banking/credit/financial sector.[8]

66. The 108 reported financial sector data breaches reported in 2019 exposed 100,621,770 sensitive records, compared to 2018 in which only 1,778,658 sensitive records were exposed in financial sector breaches.[9]

[7] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last accessed December 10, 2020)
[8] Id.
[9] Id at p15.

67. Indeed, cyber- attacks, such as the one experienced by Defendants, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendants' industry, including Defendants.

Defendants Fail to Comply with FTC Guidelines

68. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

69. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines 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 to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting 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.

70. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

71. The FTC has brought enforcement actions against businesses for failing to protect customer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

72. Defendants failed to properly implement basic data security practices, and their failure to employ reasonable and appropriate measures to protect against unauthorized access to customer PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

73. Defendants were at all times fully aware of their obligation to protect the PII of customers. Defendants were also aware of the significant repercussions that would result from its failure to do so.

Defendants Fail to Comply with Industry Standards

74. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendants' cybersecurity practices.

75. Best cybersecurity practices that are standard in the financial services industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

76. Upon information and belief, Defendants failed to meet the minimum standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including

without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness.

77. These foregoing frameworks are existing and applicable industry standards in Defendants' industry, and Defendants failed to comply with these accepted standards, thereby opening the door to the Cyber-Attack and causing the data breach.

Defendants' Breach

78. Defendants breached their obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems, networks, and data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions, brute-force attempts, and clearing of event logs;

d. Failing to apply all available security updates;

e. Failing to install the latest software patches, update its firewalls, check user account privileges, or ensure proper security practices;

f. Failing to practice the principle of least-privilege and maintain credential hygiene;

g. Failing to avoid the use of domain-wide, admin-level service accounts;

h. Failing to employ or enforce the use of strong randomized, just-in-time local administrator passwords, and;

i. Failing to properly train and supervise employees in the proper handling of inbound emails.

79. As the result of computer systems in dire need of security upgrading and inadequate procedures for handling cybersecurity threats, Defendants negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft

80. Defendants were well aware that the Private Information they collect is highly sensitive, and of significant value to those who would use it for wrongful purposes, like the REvil ransomware operators who perpetrated this Cyber-Attack.

81. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[10]

82. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[11]

83. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

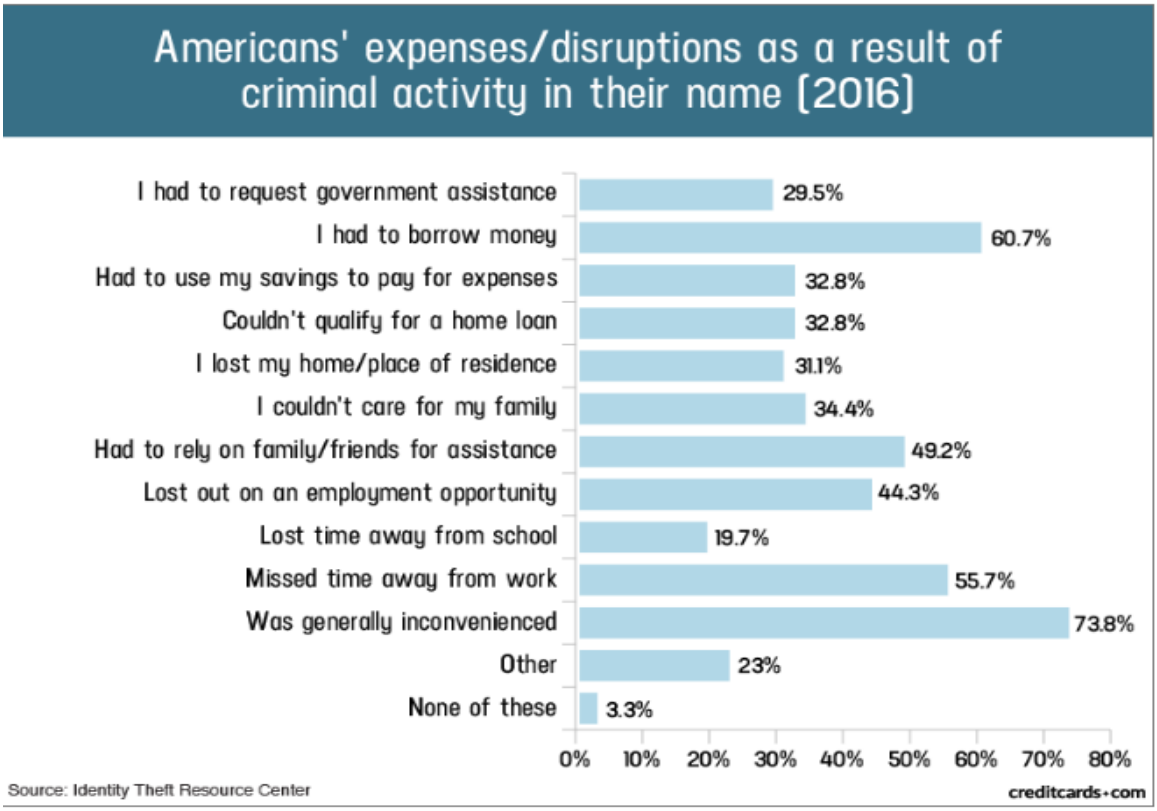
[10] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Apr. 12, 2019) ("GAO Report").

[11] *See* https://www.identitytheft.gov/Steps (last visited Dec. 8, 2020).

84. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

85. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

86. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[12]



[12] *See* Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 23, 2020) https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last accessed December 10, 2020).

87. What's more, theft of Private Information is also gravely serious. PII is a valuable property right.[13]

88. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

89. It must also be noted there may be a substantial time lag – measured in years – between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

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

See GAO Report, at p. 29.

90. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

91. Indeed, a robust "cyber black market" exists in which criminals openly post stolen Private Information on multiple underground Internet websites, just as the REvil ransomware operators did here.

92. Where the most private information belonging to Plaintiff and Class Members was accessed and removed from Defendants' network, and entire batches of that stolen information

[13] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

already dumped by the REvil ransomware operators on the cyber black market, there is a strong probability that additional batches of stolen information are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

93. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

94. While credit card information can sell for as little as $1-$2 on the black market, other more sensitive information can sell for as much as $363 according to the Infosec Institute. PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

95. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200.

96. Social Security numbers 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. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud.

97. For example, 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. 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.

98. Moreover, it is not an 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. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[14]

99. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[15]

100. At all relevant times, Defendants knew or reasonably should have known these risks, the importance of safeguarding Private Information, and the foreseeable consequences if its data security systems were breached, and strengthened their data systems accordingly. Defendants were put on notice of the substantial and foreseeable risk of harm from a data breach, yet they failed to properly prepare for that risk.

Plaintiff's and Class Members' Damages

101. To date, Defendants have done absolutely nothing to provide Plaintiff and Class Members with relief for the damages they have suffered as a result of the Cyber-Attack and data

[14] *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015, http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited October 28, 2020).

[15] *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, Feb. 6, 2015, http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited October 28, 2020).

breach, including, but not limited to, the costs and loss of time they incurred because of the Cyber-Attack. Defendants have only offered 12 months of inadequate identity monitoring services, and it is unclear whether that credit monitoring was only offered to certain affected individuals (based upon the type of data stolen), or to all persons whose data was compromised in the Cyber-Attack.

102. Moreover, the 12 months of credit monitoring offered to persons whose private information was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud.

103. Defendants entirely fail to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

104. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Cyber-Attack.

105. Plaintiff Dyrssen has been placed at the imminent, immediate, and continuing risk of harm through the theft of his name, date of birth, and Social Security number, which are the keys to financial fraud, as well as through the theft of his insurance or annuity policy number. *See* Exhibit A. He has also experienced a noticeable increase in spam phone calls, which he attributes to the theft of his Private Information.

106. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

107. Plaintiff and Class Members have been, and face substantial risk of being targeted in the future, subjected to phishing, data intrusion, and other illegal based on their Private Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and Class Members.

108. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the cyber-attack.

109. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Cyber-Attack. Numerous courts have recognized the propriety of loss of value damages in related cases.

110. Class Members were also damaged via benefit-of-the-bargain damages, in that they overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Class Members paid to Defendants was intended to be used by Defendants to fund adequate security of Defendants' computer property and Plaintiff's and Class Members' Private Information. Thus, Plaintiff and the Class Members did not get what they paid for.

111. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts and records for misuse.

112. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Cyber-Attack. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Cyber-Attack relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

113. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendants, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

114. Further, as a result of Defendants' conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

115. Plaintiff and Class members were also injured and damaged by the delayed notice of this data breach, as it exacerbated the imminent risk of harm by leaving Plaintiff and Class Members without the knowledge that would have enabled them to take proactive steps to protect themselves.

116. As a direct and proximate result of Defendants' actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

CLASS ACTION ALLEGATIONS

117. Plaintiff incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

118. Plaintiff brings this action individually and on behalf of all other persons similarly situated ("the Class") pursuant to Federal Rule of Civil Procedure 23.

119. Plaintiff proposes the following Class definition(s), subject to amendment based on information obtained through discovery. Notwithstanding, at this time, Plaintiff bring this action and seeks certification of the following Classes:

> National Class: All persons whose PII was compromised as a result of the Cyber-Attack that National Western Life Insurance Company discovered on or about August 15, 2020, and who were sent notice of the Data Breach.
>
> California Subclass: All persons residing in the State of California whose PII was compromised as a result of the Cyber-Attack that National Western Life Insurance Company discovered on or about August 15, 2020, and who were sent notice of the Data Breach.

Excluded from the Classes are Defendants' officers, directors, and employees; any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Excluded also from the Classes are members of the judiciary to whom this case is assigned, their families and members of their staff.

120. Plaintiff reserves the right to amend the definitions of the Classes or add a Class if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

121. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

122. Numerosity. The members of the Classes are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time,

based on information and belief, the Classes consists of thousands of Defendants' customers and policyholders whose data was compromised in the Cyber-Attack and data breach.

123. Commonality. There are questions of law and fact common to the Classes, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a) Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b) Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Cyber-Attack;

c) Whether Defendants' data security systems prior to and during the Cyber-Attack complied with applicable data security laws and regulations;

d) Whether Defendants' data security systems prior to and during the Cyber-Attack were consistent with industry standards;

e) Whether Defendants owed a duty to Class Members to safeguard their Private Information;

f) Whether Defendants breached their duty to Class Members to safeguard their Private Information;

g) Whether computer hackers obtained Class Members' Private Information in the Cyber-Attack;

h) Whether Defendants knew or should have known that its data security systems and monitoring processes were deficient;

i) Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;

j) Whether Defendants owed a duty to provide Plaintiff and Class Members notice of this data breach, and whether Defendants breached that duty;

k) Whether Defendants' conduct was negligent;

l) Whether Defendants' acts, inactions, and practices complained of herein amount to an invasion of privacy;

m) Whether Defendants' actions violated federal law;

n) Whether Defendant's acts violated California law, and;

o) Whether Plaintiff and Class Members are entitled to damages, civil penalties, and/or injunctive relief.

124. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Cyber-Attack.

125. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the members of the Classes. Plaintiff's Counsel are competent and experienced in litigating class actions.

126. Predominance. Defendants have engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

127. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most class

members would likely find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications with respect to individual class members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each class member.

128. Defendants have acted on grounds that apply generally to the Classes as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and All Class Members)

129. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 128 above as if fully set forth herein.

130. Defendants required Plaintiff and Class Members to submit non-public personal information in order to obtain services or purchase life insurance products.

131. By collecting and storing this data in its computer property, and sharing it and using it for commercial gain, Defendants had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendants' duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

132. Defendants owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

133. Defendants' duty of care to use reasonable security measures arose Defendants were in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

134. In addition, Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

135. Defendants breached their duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failure to periodically ensure that their network system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

f. Failing to timely notify Class Members about the Cyber-Attack so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

g. Failing to have mitigation and back-up plans in place in the event of a cyber-attack and data breach.

136. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the financial services industry.

137. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

138. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Cyber-Attack and data breach.

139. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and All Class Members)

140. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 128 above as if fully set forth herein.

141. Through their course of conduct, Defendants, Plaintiff, and Class Members entered into implied contracts for the Defendants to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

142. When Plaintiff and Class Members provided their Private Information to Defendants in exchange for Defendants' financial services, they entered into implied contracts with Defendants pursuant to which Defendants agreed to reasonably protect such information.

143. Defendants solicited and invited Class Members to provide their Private Information as part of Defendants' regular business practices. Plaintiff and Class Members accepted Defendants' offers and provided their Private Information to Defendants.

144. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations, including the Gramm Leach Bliley Act, and were consistent with industry standards.

145. Class Members who paid money to Defendants reasonably believed and expected that Defendants would use part of those funds to obtain adequate data security. Defendants failed to do so.

146. The protection of Plaintiff's and Class Members' Private Information was a material aspect of the implied contracts between Defendants' and its policyholders.

147. The implied contracts – contracts that include the contractual obligations to maintain the privacy of Plaintiff's and Class Members' Private Information—are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendants' Privacy Notice.

148. Defendants' express representations, including, but not limited to the express representations found in its Privacy Notice, memorializes and embodies the implied contractual obligation requiring Defendants to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

149. Consumers of life insurance products value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining high quality life insurance products private. To customers such as Plaintiff and Class Members, financial services that do not adhere to industry standard data security protocols to protect Private Information is

fundamentally less useful and less valuable than financial services that adheres to industry-standard data security.

150. Plaintiff and Class Members would not have entrusted their Private Information to Defendants and entered into these implied contracts with Defendants without an understanding that their Private Information would be safeguarded and protected, or entrusted their Private Information to Defendants in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

151. A meeting of the minds occurred, as Plaintiff and Members of the Class agreed to and did provide their Private Information to Defendants and paid for the provided financial services in exchange for, amongst other things, the protection of their Private Information.

152. Plaintiff and Class Members performed their obligations under the contract when they paid for their financial services and provided their valuable Private Information.

153. Defendants materially breached their contractual obligation to protect the nonpublic Private Information Defendants gathered when the information was accessed and exfiltrated by unauthorized personnel as part of the Cyber-Attack.

154. Defendants materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the relevant Privacy Notice. Defendants did not maintain the privacy of Plaintiff's and Class Members' Private Information as evidenced by its notifications of the Cyber-Attack to Plaintiff and thousands of Class Members. Specifically, Defendants did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA, or otherwise protect Plaintiff's and the Class Members' Private Information, as set forth above.

155. The Cyber-Attack was a reasonably foreseeable consequence of Defendants' actions in breach of these contracts.

156. As a result of Defendants' failure to fulfill the data security protections promised in these contracts, Plaintiff and Members of the Class did not receive the full benefit of the bargain, and instead received financial services that were of a diminished value to that described in the contracts. Plaintiff and Class Members therefore were damaged in an amount at least equal to the difference in the value of the financial services with data security protection they paid for and the financial services they received.

157. Had Defendants disclosed that their security was inadequate or that they did not adhere to industry-standard security measures, neither the Plaintiff, the Class Members, nor any reasonable person would have purchased financial services from Defendants.

158. As a direct and proximate result of the Cyber-Attack/data breach, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendants.

159. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Cyber-Attack/data breach.

160. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT III
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and All Class Members)

161. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 128 above as if fully set forth herein.

162. Insurance companies, as providers of a public service with vast power over the public and control over vast financial assets, are recognized as fiduciaries.

163. In providing their Private Information to Defendants, Plaintiff and Class Members justifiably placed special confidence in Defendants to act in good faith and with due regard to interests of Plaintiff and Class Members to safeguard and keep confidential that Private Information.

164. Defendants accepted the special confidence placed in it by Plaintiff and Class Members, as evidenced by the promulgation of and language in the Privacy Notices. There was an understanding between the parties that Defendants would act for the benefit of Plaintiff and Class Members in preserving the confidentiality of the Private Information.

165. In light of the special relationship between Defendants and Plaintiff and Class Members, whereby Defendants became guardians of Plaintiff's and Class Members' Private Information, Defendants became fiduciaries by their undertaking and guardianship of the Private Information, to act primarily for the benefit of its policyholders, including Plaintiff and Class Members, for the safeguarding of Plaintiff's and Class Members' Private Information.

166. Defendants breached their fiduciary duties to Plaintiff and Class Members by failing to diligently discover, investigate, and give notice of the Cyber-Attack and data breach in a reasonable and practicable period of time.

167. Defendants breached their fiduciary duties to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' Private Information.

168. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Cyber-Attack and data breach.

169. Defendants breached their fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

170. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (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 Cyber-Attack and data breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Cyber-Attack and data breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendants' services they received.

171. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT IV
Negligence *Per Se*
(On Behalf of Plaintiff and All Class Members)

172. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 128 above as if fully set forth herein.

173. Pursuant to Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

174. Plaintiff and Class Members are within the class of persons that the FTCA was intended to protect.

175. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, 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 Plaintiff and the Class.

176. Defendants breached their duties to Plaintiff and Class Members under the Federal Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

177. Defendants' failure to comply with applicable laws and regulations constitutes negligence *per se.*

178. But for Defendants' wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

179. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendants' breach of its duties. Defendants knew or should have known that they were failing to meet their duties, and that Defendants' breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

180. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiff and All Class Members)

181. Plaintiff restates and realleges paragraphs 1 through 128 above as if fully set forth herein, and plead this count in the alternative to the breach of contract count above.

182. Upon information and belief, Defendants funds their data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and the Class Members.

183. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendants.

184. Plaintiff and Class Members conferred a monetary benefit on Defendants. Specifically, Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the Cyber-Attack, Defendants instead calculated to increase their own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' decision to prioritize their own profits over the requisite security.

185. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendants failed to implement appropriate data management and security measures that are mandated by industry standards.

186. Defendants acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

187. If Plaintiff and Class Members knew that Defendants had not secured their PII, they would not have agreed to provide their PII to Defendants.

188. Plaintiff and Class Members have no adequate remedy at law.

189. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PIII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (v) 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 Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect PII in their 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 Breach for the remainder of the lives of Plaintiff and Class Members.

190. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

191. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendants' services.

COUNT VI
VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW
CAL. BUS. & PROF. CODE § 17200, et seq.
(ON BEHALF OF PLAINTIFF AND THE CALIFORNIA SUBCLASS)

192. Plaintiff realleges, as if fully set forth, the allegations of the preceding paragraphs 1 to 128.

193. Plaintiff and members of the California Subclass are consumers who purchased products or services (life insurance and financial services from Defendants primarily for personal, family, or household purposes.

194. Defendants' acts, practices, and omissions were done in the course of its business of marketing, offering for sale, and selling goods and services throughout the United States, including sales in the State of California.

195. Defendants violated Cal. Bus. and Prof. Code §17200, *et seq.*, by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200 with respect to the good and services provided to the California Subclass.

196. Defendants engaged in unfair acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiff's and Subclass members' PII with knowledge that the information would not be adequately protected; and by storing Plaintiff's and Subclass members' PII in an unsecure electronic environment.

197. Defendants' conduct constitutes unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and/or unlawful acts or practices, including, among other things:

a. Failure to maintain adequate computer payment card processing systems and data security practices to safeguard customers' personal information;
b. Failure to disclose that its computer systems and data security practices were inadequate to safeguard customers' personal information from theft;
c. Failure to timely and accurately disclose the data breach to Plaintiff and the Class members.

198. The foregoing failures, acts and/or omissions were done in derogation of standards set forth by the California Consumer Protection Act ("CCPA"), including but not limited to Cal. Civ. Code § 1798.81.5, which requires Defendants to take reasonable methods of safeguarding the PII of Plaintiff and the Subclass members; Federal Trade Commission ("FTC") Guidelines; and other readily available industry-wide resources that provide clear rules for the safeguarding of customers' PII in the State of California.

199. Defendants knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff and the Subclass members' PII, and that the risk of a data breach or theft was highly likely. Defendants' actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and members of the Subclass.

200. Defendants' unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and the Class members. They were likely to conceal the truth and deceive the public into believing their PII was securely stored, when it was not. The harm these practices caused to Plaintiff and the Subclass members outweighed their utility, if any.

201. Defendants also engaged in unfair acts and practices with respect to the provision of services by failing to take proper action following the disclosure of the data breach to enact adequate privacy and security measures and protect Subclass members' PII from further unauthorized disclosure, release, data breaches, and theft. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and the Subclass members. The harm these practices caused to Plaintiff and the Subclass members outweighed their utility, if any.

202. As a direct and proximate result of Defendants' unfair acts and practices, Plaintiff and the Subclass members were injured and lost money or property, including but not limited to the costs of credit monitoring, the price received by Defendants for the goods and services provided to Plaintiff in breach of their duties to protect PII, the loss of Plaintiff's and the Subclass members' legally protected interest in the confidentiality and privacy of their PII, statutory and actual damages, and additional losses as further described herein, including but not limited to:

a. Actual theft of their personal information by criminals;

b. Actual or potential fraudulent charges on their payment card accounts, some of which were not reimbursed;

c. Costs associated with the detection and prevention of identity theft;

d. Costs associated with the theft or fraudulent use of their financial accounts;

e. Loss of use of and access to some or all of their account funds and costs incurred as a result of being unable to access those funds;

f. Costs and lost time associated with handling the administrative consequences of the data breach, including identifying, disputing, and seeking reimbursement for fraudulent charges, canceling and activating payment cards;

g. Purchasing products and services from Defendants that they would not have purchased had they known of Defendants' unfair practices;

h. Impairment to their credit scores and ability to borrow and/or obtain credit, and;

i. The continued risk to their personal information, which remains on Defendants' insufficiently secured computer systems.

203. Plaintiff and the Subclass members seek relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including, but not limited to, actual damages, statutory damages, restitution to Plaintiff and the Subclass members of money or property that the Defendants may have acquired by means of its unfair business practices, restitutionary disgorgement of all profits accruing to Defendants because of its unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

204. As a result of Defendants' violations, Plaintiff and members of the Class are entitled to injunctive relief, including, but not limited to:

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

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

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

d. Ordering that Defendants segment customer data by, among other things, creating firewalls and access controls so that if one area of Defendants is compromised, hackers cannot gain access to other portions of Defendants systems;

e. Ordering that Defendants purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;

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

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

h. Ordering Defendants to meaningfully educate its customers about the threats they face as a result of the loss of personal information to third parties, as well as the steps its customers must take to protect themselves.

205. Plaintiff and the Class members reserve the right to amend this Complaint as of right to seek damages and relief under Cal. Civ. Code § 1798.100, *et seq*.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a class action and appointing Plaintiff and his counsel to represent the Class;

b) For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c) For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

e) Ordering Defendants to pay for not less than three years of credit monitoring services for Plaintiff and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i) Pre- and post-judgment interest on any amounts awarded; and

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

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues. Dated:

March 8, 2021 Respectfully submitted,

/s/ *Danielle L. Perry*
Danielle L. Perry (SBN 292120)
Gary E. Mason*
MASON LIETZ & KLINGER LLP
5301 Wisconsin Avenue, NW Suite 305
Washington, DC 20016
Tel: (202) 429-2290
dperry@masonllp.com
gmason@masonllp.com

Gary M. Klinger*
MASON LIETZ & KLINGER LLP
227 W. Monroe Street, Suite 2100
Chicago, IL 60630
Tel.: (202) 429-2290
gklinger@masonllp.com

Attorneys for Plaintiff

*Will seek admission *pro hac vice*

JS 44 (Rev. 10/20)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

Douglas Dyrssen Sr., individually and on behalf of all others similarly situated,

(b) County of Residence of First Listed Plaintiff Stanislaus
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Mason Lietz & Klinger, LLP. 5101 Wisconsin Ave. NW. Ste. 305
Washington, DC 20016. 202-429-2290

DEFENDANTS

National Western Life Insurance Company and National Western Life Group, Inc.

County of Residence of First Listed Defendant Austin, TX
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☒ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☒ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☒ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332; 15 U.S.C. § 45

Brief description of cause:
Class Action; Data Breach

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $ over $5,000,000

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE 3/8/2021

SIGNATURE OF ATTORNEY OF RECORD /s/ Danielle L. Perry

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____