SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF NEW YORK

--X

THE PEOPLE OF THE STATE OF NEW YORK,
by LETITIA JAMES, Attorney General of the
State of New York,

Plaintiff,

-against-

NATIONAL GENERAL HOLDINGS CORP.; INTEGON NATIONAL INSURANCE COMPANY; INTEGON CASUALTY INSURANCE COMPANY; INTEGON INDEMNITY CORPORATION; INTEGON GENERAL INSURANCE CORPORATION; INTEGON PREFERRED INSURANCE COMPANY; NATIONAL GENERAL ASSURANCE COMPANY; NATIONAL GENERAL INSURANCE COMPANY; NEW SOUTH INSURANCE COMPANY; ALLSTATE INSURANCE COMPANY,

Defendants.

--X

COMPLAINT

Index No.
IAS Part

Of Counsel:

CHRIS D'ANGELO
Chief Deputy for Economic Justice
KIM BERGER
Bureau Chief, Bureau of Internet and Technology
CLARK RUSSELL
Deputy Chief, Bureau of Internet and Technology
LAURA MUMM
ALEXANDRA HIATT
Assistant Attorneys General, Bureau of Internet and Technology
28 Liberty St.
New York, NY 10005
(212) 416-8433

TABLE OF CONTENTS

NATURE OF THE ACTION

1. Plaintiff, the People of the state of New York, by Attorney General Letitia James ("OAG"), brings this action pursuant to General Business Law ("GBL") §§ 899-aa and 899-bb, GBL §§ 349 and 350, and Executive Law § 63(12) to remedy unlawful, fraudulent, and/or deceptive conduct by National General Holdings Corp. ("NGHC"); Integon National Insurance Company, Integon Casualty Insurance Company, Integon Indemnity Corporation,[1] Integon General Insurance Corporation, Integon Preferred Insurance Company, National General Assurance Company, National General Insurance Company, and New South Insurance Company, which are affiliated insurance companies doing business under the umbrella of NGHC (together with NGHC, "National General"); and Allstate Insurance Company ("Allstate") (collectively, "Defendants").

2. In 2020 and 2021, National General—an insurer with millions of customers across the United States—suffered a pair of back-to-back data breaches in which the drivers' license numbers ("DLNs") of nearly 200,000 consumers, including more than 165,000 New Yorkers, were exposed to attackers.

3. In those breaches, bad actors targeted online auto insurance quoting tools that National General made available to consumers and independent agents who sold National General insurance. These tools were intended to provide consumers, either on their own or through an agent, with a fast quote for auto insurance. However, National General *intentionally* built these tools to automatically populate consumers' entire DLNs in plain text—in other words, *fully exposed* on the face of the quoting websites—during the quoting process. The quoting tools

[1] In the breach notification submitted to OAG on March 4, 2021, The Allstate Corporation referred to Integon Indemnity Corporation as Integon Indemnity Insurance Company.

would automatically populate the entire, unmasked DLNs of not just the consumer whose name and address were entered by the user, but of *all drivers* identified as living at that consumer's address.

4. Not surprisingly, attackers identified this vulnerability and targeted these quoting tools as an easy way to access the DLNs of many New Yorkers.

5. DLNs are valuable to bad actors because they can be used for many forms of fraud, including identity theft and government benefits fraud. Indeed, according to the New York State Department of Financial Services ("DFS"), the attacks on National General's websites appeared to have been part of a "systemic and aggressive campaign . . . to steal Nonpublic Information."[2] As DFS warned, attackers were stealing consumers' DLNs from the quoting websites of auto insurance companies to "submit fraudulent claims for pandemic and unemployment benefits."[3] "Notably, the concerted effort to steal [Nonpublic Information] from New Yorkers seem[ed] to have coincided with the implementation of enhanced identity requirements to obtain pandemic benefits in New York";[4] these enhanced requirements related to the verification of DLNs, which are not publicly available and are hard to change. According to DFS, as of March 2021, these attacks had "resulted in theft of sensitive data for hundreds of thousands of New Yorkers."[5]

6. The incidents at National General were remarkable in scale because the company made it easy for bad actors. The first attack was on a pair of consumer-facing websites that allowed users

---

[2] DFS Industry Letter, Cyber Fraud Alert (Feb. 16, 2021), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210216_cyber_fraud_alert.

[3] *Id.*

[4] *Id.*

[5] DFS Industry Letter, Cyber Fraud Alert (March 30, 2021), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210330_cyber_alert_followup.

to obtain auto insurance policy quotes, which National General had intentionally designed to expose consumers' private information with little prompting. Attackers discovered these weaknesses and used computer programs known as "bots" to harvest consumers' DLNs from the websites with significant speed. Because National General had not instituted tools to meaningfully block such automated attacks or sufficiently monitor for potentially malicious activity, National General did not detect these attacks for over two months, until November 2020. In that period, the DLNs of almost 12,000 consumers, including more than 9,100 New Yorkers, were compromised.

7. After it discovered the first breach, National General, in violation of state data breach notification laws, did not alert impacted New Yorkers or relevant New York state agencies. This lack of notification prevented New Yorkers from being able to take precautions to protect themselves from the potentially serious repercussions stemming from the attacks, and New York state agencies from quickly investigating the issue.

8. Worse yet, even after it remediated the first breach, National General left consumers' entire DLNs fully exposed on the online auto insurance quoting tool it made available to its network of independent agents. Attackers, predictably, targeted the agent quoting tool in a second, far larger breach that compromised an additional 187,000 consumers' DLNs, including the DLNs of approximately 155,000 New Yorkers.

9. Independent agents accessed the quoting tool through a website (the "agent portal"), which was nominally secured by a username and password. But these credentials offered little actual protection due to National General's poor access controls. Among other issues, National General did not require agents' passwords to be sufficiently long and complex to protect against theft or hacking; sent independent agencies their passwords in plain text using unencrypted

email; allowed passwords to be shared among entire agencies; and allowed agencies to use the same password indefinitely—all of which increased the likelihood a password could be stolen, guessed, or otherwise compromised. National General also did not require independent agents to enter a second form of authentication to access the agent portal or institute reasonable alternative controls, despite the fact that the agent portal allowed agents to access National General's internal network, and the sensitive information on it, from the internet.

10. While the specific source of the breaches was National General's design and release of several insecure websites, the broader cause of the incidents was National General's prioritization of profit over the implementation of reasonable data security safeguards. As National General's Chief Operating Officer put it in September 2019 when discussing whether certain data security expenses were necessary, National General's "internal risk appetite for a data breach [wa]s very high." And even after Allstate took control of National General's data security function after The Allstate Corporation acquired National General for $4 billion on January 4, 2021, National General's data security still fell below the standard required by New York state law.

11. Despite its lax approach to data security, National General nonetheless represented to consumers that it would protect their personal information. In the privacy notices it sent customers and provided to website visitors, National General expressly and by implication represented it would implement and maintain reasonable controls to safeguard their personal information. National General did not keep that promise.

12. As described above and further below, National General violated New York's breach notification law, GBL § 899-aa, by failing to report the first breach to impacted New Yorkers and relevant regulators. Defendants also violated New York's Stop Hacks and Improve

Electronic Data Security Act (the "SHIELD Act"), GBL § 899-bb, by failing to develop, implement, and maintain reasonable safeguards at National General to protect the security, confidentiality, and integrity of New Yorkers' private information. And Defendants' representations to consumers that National General used reasonable safeguards to protect their personal information were false and misleading and violated New York's consumer protection laws, Executive Law § 63(12) and GBL §§ 349 and 350.

PARTIES

13. Plaintiff is the People of the state of New York by their attorney, Letitia James.

14. National General Holdings Corp. ("NGHC") is a Delaware corporation and the ultimate parent company for numerous consolidated subsidiary insurance companies. Through at least 2020, NGHC was headquartered in New York City and NGHC's chief executive officers were based in New York, as were several functions that served NGHC and its subsidiaries, including the legal, finance, and escheatment teams. By and through its subsidiary companies and in the regular course of its business, NGHC owns and/or licenses computerized data which includes the private information of millions of consumers, including New York state residents. NGHC's subsidiary companies also conduct significant business in New York state, which, at least as of 2020, was one of NGHC's top three geographic regions in terms of property and casualty insurance gross written premium. On January 4, 2021, NGHC became a wholly-owned subsidiary of Allstate Insurance Holdings, LLC, a Delaware limited liability company that is, itself, a wholly-owned subsidiary of The Allstate Corporation, a Delaware corporation.

15. Integon National Insurance Company is an indirect subsidiary of NGHC that is based in North Carolina. It is licensed in New York state by DFS and has transacted business in New York state, including by selling and supplying insurance to consumers in New York state and/or

by licensing computerized data that includes the private information of New York state residents. It is one of the National General entities that employed the online quoting tools that were breached in 2020 and 2021.

16. Integon Casualty Insurance Company is an indirect subsidiary of NGHC that is based in North Carolina. It is licensed in New York state by DFS and has transacted business in New York state, including by selling and supplying insurance to consumers in New York state and/or by licensing computerized data that includes the private information of New York state residents. It is one of the National General entities that employed the online quoting tools that were breached in 2020 and 2021.

17. Integon Indemnity Corporation is an indirect subsidiary of NGHC that is based in North Carolina. It is licensed in New York state by DFS and has transacted business in New York state, including by selling and supplying insurance to consumers in New York state and/or by licensing computerized data that includes the private information of New York state residents. It is one of the National General entities that employed the online quoting tools that were breached in 2020 and 2021.

18. Integon General Insurance Corporation is an indirect subsidiary of NGHC that is based in North Carolina. It is licensed in New York state by DFS and has transacted business in New York state, including by selling and supplying insurance to consumers in New York state and/or by licensing computerized data that includes the private information of New York state residents. It is one of the National General entities that employed the online quoting tools that were breached in 2020 and 2021.

19. Integon Preferred Insurance Company is an indirect subsidiary of NGHC that is based in North Carolina. It is licensed in New York state by DFS and has transacted business in New

York state, including by selling and supplying insurance to consumers in New York state and/or by licensing computerized data that includes the private information of New York state residents. It is one of the National General entities that employed the online quoting tools that were breached in 2020 and 2021.

20. National General Assurance Company is a direct subsidiary of NGHC that is based in Missouri. It is licensed in New York state by DFS and has transacted business in New York, including by selling and supplying insurance to consumers in New York state and/or by licensing computerized data that includes the private information of New York state residents. It is one of the National General entities that employed the online quoting tools that were breached in 2020 and 2021.

21. National General Insurance Company is a direct subsidiary of NGHC that is based in Missouri. It is licensed in New York state by DFS and has transacted business in New York state, including by selling and supplying insurance to consumers in New York state and/or by licensing computerized data that includes the private information of New York state residents. It is one of the National General entities that employed the online quoting tools that were breached in 2020 and 2021.

22. New South Insurance Company is an indirect subsidiary of NGHC that is based in North Carolina. It is licensed in New York state by DFS and has transacted business in New York state, including by selling and supplying insurance to consumers in New York state and/or by licensing computerized data that includes the private information of New York state residents. It is one of the National General entities that employed the online quoting tools that were breached in 2020 and 2021.

23. From 2017 through 2020, NGHC and its consolidated subsidiaries did not have fewer than 50 employees, less than $3 million dollars in gross annual revenue in each of the prior three fiscal years, or less than $5 million in total year-end assets.

24. Upon information and belief, NGHC and its subsidiaries, including all of the above-named subsidiaries, have overlapping directors and officers, and share services, resources, infrastructure, office space, and staff for enterprise-wide functions, including the companies' enterprise-wide data security and information technology functions. Until the acquisition by The Allstate Corporation, NGHC exercised total control over those enterprise-wide functions, including by owning the policies that governed those functions, hiring personnel to staff the functions, providing shared office space for that personnel (most of the data security and information technology personnel, for example, operated out of NGHC's offices in or near Winston-Salem, North Carolina), and setting and managing the budgets for these enterprise-wide functions (including data security). In addition to sharing compliance and technology functions, NGHC and all its subsidiaries shared a legal team. And all of NGHC's auto insurance subsidiaries used the same technologies and systems to process their insurance policies and claims. In short, NGHC and its subsidiaries did not and do not operate at arm's length such that no real distinction exists among them and, before the acquisition by The Allstate Corporation, NGHC controlled the interrelated group of companies.

25. Allstate Insurance Company is an Illinois corporation that is a wholly-owned subsidiary of Allstate Insurance Holdings, LLC, a Delaware limited liability company. Allstate Insurance Holdings LLC is, in turn, a wholly-owned subsidiary of The Allstate Corporation, a Delaware corporation. Allstate Insurance Company is licensed in New York state by DFS and has transacted business in New York state, including by selling and supplying insurance to

consumers in New York state and/or by licensing computerized data that includes the private information of New York state residents. Upon information and belief, after the acquisition of National General by The Allstate Corporation in January 2021, personnel from Allstate Insurance Company took control of National General's data security and privacy functions, including the investigation and remediation of the breach of National General's agent portal, and the reporting to consumers and regulators of both National General breaches described herein.

26. OAG has provided Defendants with notice as specified in GBL §§ 349 and 350-c.

JURISDICTION

27. This Court has jurisdiction pursuant to: (i) GBL § 899-aa, which authorizes OAG to seek injunctive relief, damages, civil penalties, and other equitable relief when a person or business fails to disclose a security breach to New York state residents whose private information was, or is reasonably believed to have been, accessed or acquired without authorization; (ii) GBL § 899-bb, which authorizes OAG to seek injunctive relief, restitution, civil penalties, and other equitable relief when a person or business that owns or licenses computerized data that includes private information of New York state residents fails to develop, implement, and maintain reasonable safeguards to protect the security, confidentiality, and integrity of the private information; (iii) GBL § 349, which authorizes OAG to seek injunctive relief, restitution, civil penalties, and other equitable relief when a person or business engages in deceptive acts and practices in the conduct of any business, trade, or commerce in the state of New York; (iv) GBL § 350, which authorizes OAG to seek injunctive relief, restitution, civil penalties, and other equitable relief when a person or business engages in false advertising in the conduct of any business, trade, or commerce in the state of New York; and (v) Executive Law § 63(12), under which OAG is empowered to seek injunctive relief, restitution, damages, and other equitable

relief when a person or business engages in repeated fraudulent or illegal acts or persistent fraud or illegality in the carrying on, conducting, or transaction of business in the state of New York.

28. The parties entered into a series of tolling agreements that tolled the applicable statutes of limitations beginning April 21, 2022 and ending November 21, 2023.

FACTUAL ALLEGATIONS

I. National General's Business Relies on the Collection and Use of the Private Information It Is Legally Obligated to Protect

A. National General Collects, Uses, and Maintains Significant Amounts of Non-Public Consumer Information.

29. National General is one of the largest insurers in the United States. It provides personal and commercial auto insurance, homeowners and renters insurance, accident and health insurance, and several other insurance products, including flood, private collections, and umbrella insurance. As of 2020, National General had more than four million customers and total assets over $10 billion.

30. As an insurance company with millions of policyholders, National General necessarily collects, uses, and maintains its customers' private information in the normal course of business, including social security numbers ("SSNs"), DLNs, payment card information, and bank information.

31. Additionally, in order to provide quotes for insurance products, National General stores and uses the private information of *potential* customers, which consumers may provide to National General through its websites or through independent agents when considering purchasing an insurance policy. National General also has licensed consumer information—including DLNs, credit data, vehicle history data, and addresses—from third-party data providers.

32. Two of National General's primary systems that store, process, and/or use the private information of customers and potential customers are NPS and EPIC. NPS is National General's policy system that is used by employees, agents, and customers. It also is the engine behind the insurer's consumer-facing and agent-facing auto insurance quoting tools. NPS stores consumers' names, addresses, SSNs, DLNs, and payment information. EPIC is National General's claims system and it stores consumers' names, addresses, ages, genders, SSNs, DLNs, and dates of birth ("DOBs"). NPS and EPIC serve the vast majority of National General's business—as of 2020, they supported $5 billion in premiums, 1.7 million policies, 90,000 daily quotes, 42,000 agents, and 970,000 claims annually—and were deemed "enterprise critical" by the company.

B. National General Is Legally Obligated to Safeguard the Security, Confidentiality, and Integrity of Consumers' Private Information.

33. National General has for years been subject to various federal and state data security laws and regulations, as well as industry group standards, that require it to implement reasonable safeguards to protect consumers', including customers', private information.

34. Under those laws and regulations, an entity need not experience a security breach or incident—nor do any tangible damages need to follow from an incident—for a violation to occur. Rather, these laws recognize that, because no company can reliably predict *ex ante* how and when bad actors will exploit poorly protected data, companies must appropriately limit risks to consumers' private information, regardless of whether a breach has occurred.

35. The data security laws and regulations that National General has been subject to include, among others, New York's SHIELD Act, GBL § 899-bb; DFS's Cybersecurity Regulation (the "Cybersecurity Regulation" or "Part 500"), 23 NYCRR Part 500; the Health Insurance Portability and Accountability Act ("HIPAA"), Pub. L. No. 104-191, 110 Stat. 1936 (1996), as

amended by the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), Pub. L. No. 111-5, 123 Stat. 226 (2009), as well as the U.S. Department of Health and Human Services regulations at 45 C.F.R. § 164.302 *et seq*. (the "HIPAA Security Rule"); and the Gramm-Leach-Bliley Act (the "GLBA"), Pub. L. No. 106-102, 113 Stat. 1338 (1999), and its implementing regulations.

36. In addition, although not a law or regulation, payment card brands require entities involved in payment card processing to comply with the data security standards set forth in the Payment Card Industry Data Security Standard ("PCI DSS").

37. National General is also subject to state data breach notification laws that require the insurer to promptly notify individuals about security breaches involving their private information. *E.g.*, GBL § 899-aa(2).[6] New York state's notification law also requires that companies notify several New York state agencies, including OAG, of any breach notification sent to affected New York state residents. *Id.* § 899-aa(8)(a).

38. DLNs, when combined with personally identifying information such as names, are expressly protected under several laws and regulations, including New York's SHIELD Act, New York's Information Security Breach and Notification Act, and DFS's Cybersecurity Regulation. *See* GBL § 899-bb(1)(b); *id.* § 899-aa(1)(b); 23 NYCRR 500.1(k)(2).

---

[6] New York's Information Security Breach and Notification Act was enacted in 2005, requiring entities to expediently notify New York state residents whose private information—including DLNs, when combined with personally identifying information—was, or was reasonably believed to have been, "acquired" by a person without valid authorization. GBL § 899-aa(2) (2005). The requirement to also notify New York state residents if their private information was "accessed" was added by the SHIELD Act in 2019. GBL § 899-aa(2) (2019). The legislature has since amended the law further, but the 2019 version governed National General's conduct as alleged here.

II. National General Exposed to Attackers the Private Information of Nearly 200,000 Consumers, Including Approximately 165,000 New Yorkers

39. Despite its longstanding legal obligations to secure private information, National General exposed consumers' names and entire, unprotected DLNs through the auto insurance quoting tools it made available on several of its websites. National General did not sufficiently authenticate that the website visitors who accessed the DLNs through the quoting interfaces were entitled to view this sensitive information. Rather, National General *purposefully* designed these tools to expose DLNs to users with minimal prompting, and then—with insufficient testing for security or privacy issues—launched these websites for widespread use.

40. DLNs are a particularly valuable piece of personal information for bad actors because they are difficult to change and, therefore, are a nearly permanent identifier for individuals. DLNs can be used in several types of fraud, including but not limited to:

a. Applying for government benefits in the victim's name;
b. Opening bank accounts or lines of credit in the victim's name;
c. Creating fake identification using the victim's name; and
d. Using this fake identification to take myriad actions in the victim's name, including entering into rental agreements, taking out insurance contracts, or incurring a record of driving violations.

41. Here, the attacks on National General appear to have been part of a broader set of attacks against auto insurance companies' quoting tools in 2020 and 2021. As DFS warned insurers doing business in New York, attackers "were targeting [insurers'] websites that offer[ed] instant

online automobile insurance premium quotes . . . to steal unredacted driver's license numbers."[7] According to DFS, these attacks "appear[ed] to be part of a growing fraud campaign targeting pandemic and unemployment benefits" and that "the concerted effort to steal [non-public information] from New Yorkers seem[ed] to have coincided with the implementation of enhanced identity requirements" related to the need to provide an accurate DLN for the named applicant in order "to obtain pandemic benefits in New York."[8]

42. In this context, attackers identified National General's online auto insurance quoting tools as easy targets. In 2020 and 2021, attackers accessed the DLNs of nearly 200,000 consumers, including more than 165,000 New Yorkers, from National General's quoting tools as a result of the company's failure to adopt appropriate data security measures.

A. National General's Insecure Consumer Quoting Tool Purposefully Exposed Consumers' DLNs to Unauthenticated Users.

43. The first of the attacks on National General occurred between approximately August and November 2020 and targeted two publicly accessible National General websites—https://nationalgeneral.com and https://www.directauto.com—where consumers could receive an instant auto insurance quote via an application that could be accessed from both sites (the "consumer quoting tool"). National General had operated a consumer quoting tool for many years, but redesigned it in or around 2019. All of the National General entities that were impacted by the breaches, *see supra* ¶¶ 15-22, used this quoting tool.

[7] DFS Industry Letter, Cyber Fraud Alert (Feb. 16, 2021), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210216_cyber_fraud_alert.

[8] *Id.*

44. In the version of the consumer quoting tool available online beginning in or around 2019, a user would begin the quoting process by entering the zip code of an area where National General offered instant auto insurance quotes.[9] The user would then be taken to a webpage where they could enter the name and address—information that is available in a phone book and online—of *any* consumer to begin the quoting process. Upon information and belief, at various times the consumer quoting tool may also have prompted users to provide a DOB, but that DOB did not need to be accurate for the user to proceed through the quoting process.

45. The name and address provided by the user would be used to automatically populate information on the "Driver Details" pages within the consumer quoting tool using a process referred to as "prefill." With prefill, the consumer quoting tool queries National General's third-party data provider, LexisNexis Risk Solutions ("Lexis"), for driver and vehicle information associated with the entered name and address. The tool then automatically displays, or prefills, the results it receives from Lexis, including (i) the name of the consumer whose information had been entered by the user, (ii) the entire DLN of that consumer, (iii) the names of any other drivers identified as potentially living at that consumer's address, and (iv) the entire DLNs of those other drivers. National General designed the consumer quoting tool so that all of this information would appear in plain text—*i.e.*, fully exposed—to the user of the tool. In effect, if a user of the consumer quoting tool entered a consumer's name and address, the tool would automatically populate the quoting screens with the fully visible names and DLNs of *all drivers*

[9] At various points, the consumer quoting tool may have prompted the user to enter the make, year, and model of the vehicle the user sought to insure before asking for the user's name and address. However, this information was not verified before the user could proceed. In other words, the user could enter the information for *any* vehicle and continue with the quoting process.

identified as living at the consumer's address without any sort of authentication that the user was entitled to view the information.

46. Specifically, a user that entered a consumer's name and address (and potentially any DOB), would make it to the consumer quoting tool's "Driver Details" page, as depicted in Figure A, below. That page would prompt the user to confirm the consumer's DLN, which would have been prefilled by the tool. At the time of the breach, National General had designed the tool so that the consumer's entire, prefilled DLN was displayed in plain text (although, in Figure A, which was captured after the incident, National General had masked the DLN as part of the breach remediation).[10]

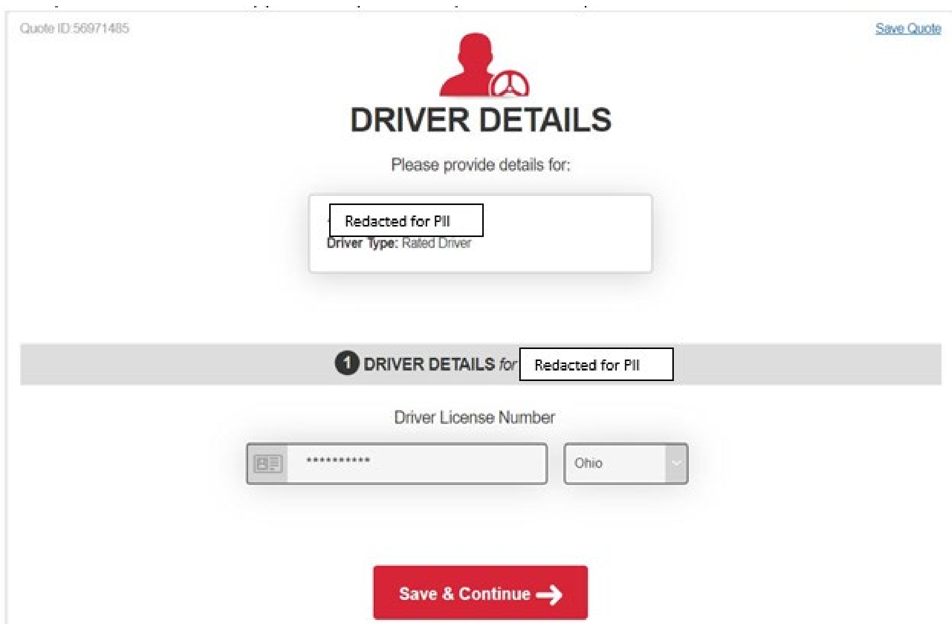

Figure A –
The "Driver Details" page for the directauto.com consumer quoting tool around March 2021

[10] Personally identifying information in Figures A - D has been redacted by counsel for privacy reasons.

47. The quoting tool would then prompt the user to "Add" to their auto insurance quote other household drivers whose names were automatically populated by the tool, as depicted in Figure B.

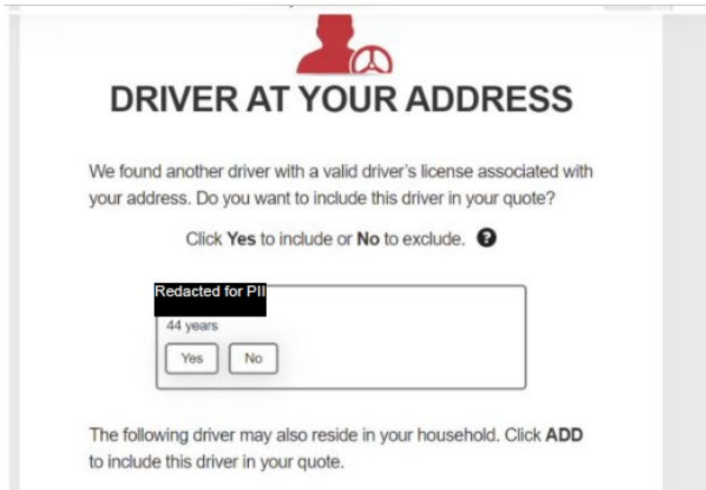

Figure B –
The "Driver At Your Address" page for the directauto.com consumer quoting tool around June 2021

48. After the user added the household members, the quoting tool would automatically display household members' DLNs to the user, as depicted in Figure C. At the time of the breach, National General had designed the quoting tool so that these other drivers' entire DLNs were displayed in plain text (although the DLN is masked in Figure C, which was captured after the incident).

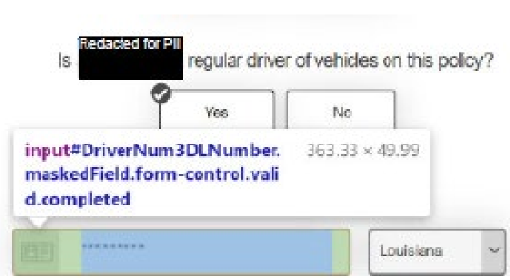

Figure C –
Household driver DLN prefill page for the directauto.com consumer quoting tool around June 2021

49. National General licensed consumers' personal information—including New Yorkers' information—from Lexis to prefill these fields in the consumer quoting tool. Lexis would transmit the consumer personal information needed for prefill to National General's policy system, NPS, through an application programming interface, or an "API" (which allows applications to communicate with one another). The information, including DLNs, would then be transmitted to the quoting tool from NPS through another API.

50. This prefill functionality was provided because National General could sell more policies and faster if users did not need to manually enter their DLNs.

51. But DLNs should not have been exposed to unauthenticated users in full and in plain text for the sake of consumer convenience and National General's bottom line. First, National General was legally obligated to protect DLNs from unauthorized access. *See supra* ¶¶ 35-38. Second, National General's Data Classification Policy at the time classified DLNs as "Confidential" information that needed to be "protected to a higher standard than Internal Use Only," and "Internal Use Only" data could "never be posted to public sites." Third, there were simple and widely-used alternatives to providing unauthenticated users with full, unprotected DLNs that would not have diminished the consumer experience. For example, National General could have masked DLNs—*i.e.*, replaced digits with artificial data or symbols, like an asterisk (*)—as it did after the incidents. *See supra* Figures A & C.

52. In addition, National General's contract with Lexis required National General to adhere to Lexis's Data Display Requirements, which in turn prohibited National General from displaying DLNs on consumer-facing websites like the consumer quoting tool. National General also was required to immediately alert Lexis if National General "learn[ed] or ha[d] reason to

believe" that the consumer information Lexis provided to National General had been compromised as part of a security event.

53. National General, however, failed to ensure that the consumer quoting tool's design and testing teams were aware that DLNs needed to be protected. In fact, the teams building and reviewing the version of the consumer quoting tool that incorporated prefill *purposefully* designed the tool so that entire DLNs would be displayed in plain text. As Allstate later determined, "DLN was not classified as [non-public information]" by the relevant National General teams "and as such the plain text display was by design."

54. The attackers used bots—computer programs that can be used to rapidly perform an action on a webpage—to repeatedly query National General's consumer quoting tool to harvest consumers' DLNs. And the attackers were able to do so for months without National General noticing because the insurer did not have sufficient protections in place to mitigate or slow down bot attacks, such as appropriately calibrated rate limiting (a technique that limits the frequency of requests that can be made to a server within a specified time frame), bot detection tools like a CAPTCHA system (a security tool used to differentiate between humans and bots on websites), or a web application firewall (a security tool that can monitor and filter out suspicious web traffic to an online application like the consumer quoting tool). In other words, National General had not deployed widely available tools that could have been used to stymie these well-known and common types of attacks.

55. National General also did not sufficiently monitor its websites for easily detectable indications of suspicious activity. Monitoring for behaviors typical of bot attacks was particularly important because some National General websites—like the consumer quoting

tool—used and displayed consumers' private information. Without sufficient monitoring, National General failed to detect the attacks on the consumer quoting tool for over two months.

56. Ultimately, it was National General's product and marketing teams—and not the insurer's cybersecurity team—that detected the attack as part of their efforts to identify the potential purchase of fraudulent policies. And those teams identified the suspicious activity using a tool that, by chance, National General had been piloting for about a month.

B. Attackers Were Able to Access Nearly 12,000 DLNs, Including More Than 9,000 New Yorkers' DLNs, via National General's Consumer Quoting Tool.

57. On November 18, 2020, an analyst on National General's product team detected a larger than normal volume of requests on the consumer quoting tool. These quotes were unusual because they did not result in the binding (*i.e.*, purchase) of auto insurance policies; instead, users of the quoting tool were abandoning quotes after reaching the "Drivers Details" page, where consumers' names and DLNs were displayed in plain text, *see supra* ¶¶ 45-49.

58. Despite the indications of fraudulent activity, the product and marketing teams did not contact National General's cybersecurity team until November 23, 2020—five days after the unusual activity had been detected—because they were unaware of or unfamiliar with the procedures they were supposed to follow in the event of a data security incident (which required the cybersecurity and compliance teams to be promptly notified).

59. Even when the cybersecurity team was engaged, the business teams continued to drive the investigation and remediation of the incident. They did so despite having no expertise in cybersecurity and even though the National General employee whose team first noticed the suspicious activity suspected attackers were "using [National General's] system to mine people's personal data and likely use it against them for something like identity theft." And, on November

23, 2020, when the cybersecurity team elevated the issue to management, the decision was made to just continue monitoring the activity—despite the likely exposure of private information.

60. The next day, on November 24, 2020, National General decided to mask the DLNs appearing on the consumer quoting tool's user interface, *i.e.*, on the face of the websites, so that visitors to the sites would not see the DLNs in plain text.

61. Even as this change was made, though, National General personnel noted that full DLNs were *still visible* through a web browser's developer tools. Developer tools are accessible to any website visitor with a few clicks of a mouse or by pressing the F12 key, and they allow the visitor to see data elements (including unmasked data elements) in the website's code. In the highlighted section next to the red arrow, Figure D shows where users would have seen unmasked DLNs if they opened the consumer quoting tool's developer tools (although they are masked in Figure D, which was captured after the incidents).

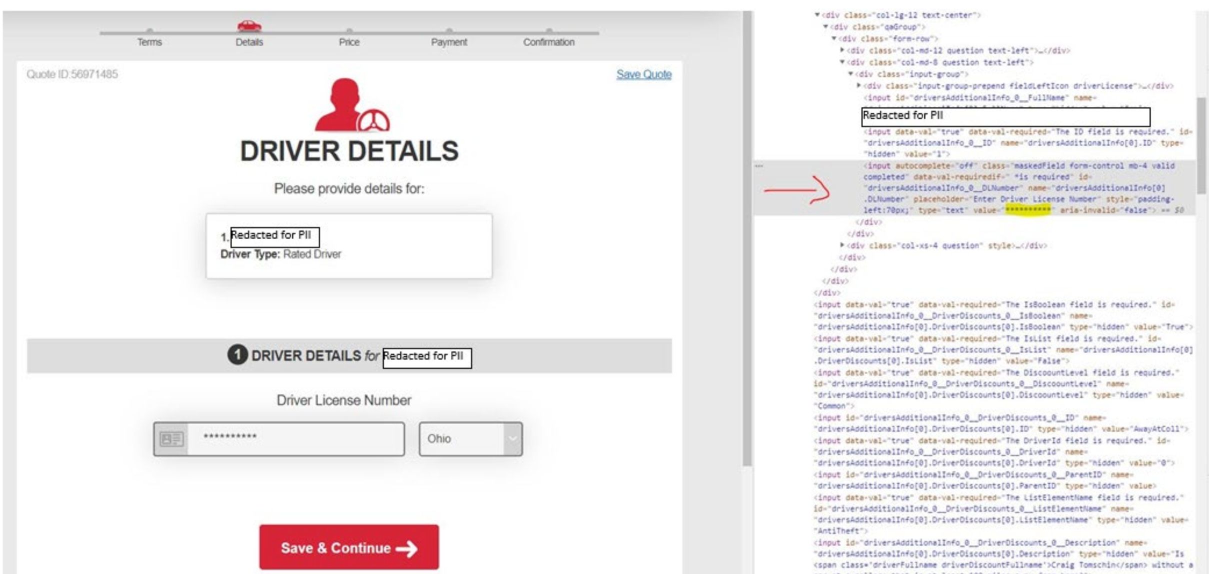

Figure D – Using the developer tools to view the code

62. In other words, even after the company had masked DLNs on the face of the websites, National General continued to operate the consumer quoting tool with *full, unprotected DLNs*

visible to any website visitors who knew how to access developer tools in their browsers—as online bad actors would. And it did so for a full week after it first identified the suspicious activity. During that seven-day period, National General's management discussed the possibility of taking the consumer quoting tool offline completely but decided not to, prioritizing profitability over consumer privacy. Consequently, malicious activity continued until National General finally turned off the prefill function entirely on November 30, 2020.

63. In all, it took nearly two weeks from when National General first detected the suspicious activity on its consumer quoting tool for the company to take the steps necessary to stop it. As a result, attackers were able to harvest the DLNs of 11,885 consumers, including more than 9,100 New Yorkers.

64. After remediating the breach, National General failed to identify whether DLNs or other private information were exposed in other parts of National General's environment. Had it done so, it should have recognized that the quoting tool it made available to independent agents on the agent portal used *the exact same Lexis prefill functionality* and also displayed DLNs in plain text. That recognition could have allowed National General to prevent the second breach, which targeted the agent portal, and therefore could have prevented the theft of many additional consumers' private information.

C. <u>National General Failed to Alert Impacted New Yorkers or Relevant New York State Agencies of the Consumer Quoting Tool Breach.</u>

65. Under GBL § 899-aa, companies are required to promptly disclose a security breach to New York state residents whose private information was, or is reasonably believed to have been, accessed or acquired without authorization, and to notify several New York state agencies,

including OAG, of the breach. GBL § 899-aa(2), (8). Most other states have similar data breach notification laws.

66. Despite these requirements, National General did not report the incident to any impacted consumers or relevant regulators after the breach was discovered. Upon information and belief, National General did not identify which consumers were impacted by the breach at that time. One National General employee testified that the company's Chief Information Security Officer ("CISO") told the employee that National General did not report the incident because it had been "resolved."

67. Ultimately, it was Allstate that reported the first incident to consumers and regulators—after the acquisition closed and the second breach had been detected. Allstate reported the incident to DFS in February 2021, OAG in March 2021, and New York state residents by April 2, 2021.

68. National General also did not inform Lexis of the consumer quoting tool incident at the time of the breach, despite the contractual requirement that it do so promptly. Lexis only learned of the breach after Allstate's acquisition.

D. Attackers Subsequently Breached National General's Agent Portal, Exploiting the DLNs of Almost 190,000 Consumers, Including Approximately 155,000 New Yorkers.

69. The second attack began in or around October 2020 but was not detected by National General until late January 2021. This attack targeted the agent portal, a website National General made available to independent agents who sold National General insurance and which provided a quoting tool that agents could use to run auto insurance quotes for customers and potential customers.

70. As with the consumer quoting tool, the agent portal was connected to NPS and had access to private information—including New Yorkers' private information—that was stored on or flowed through NPS. And as with the consumer quoting tool, the agent portal quoting tool had a prefill functionality that was powered by Lexis. If an agent input a consumer's name and address (and potentially a DOB), the names and DLNs for that consumer and members of the consumer's household were automatically populated into the quoting tool from Lexis's database. As with the consumer quoting tool, these DLNs were fully displayed in plain text on the face and in the code of the agent portal.

71. Unlike the publicly accessible consumer quoting tool, an agent needed to provide a valid username and password to access the agent portal. However, National General's insecure access controls meant that these credentials offered little protection. As described below, (i) agents' passwords were not sufficiently complex (specifically, they did not contain enough characters to make it harder for a stranger to guess it); (ii) agent portal logins had no password expiration (in other words, agents could use the same password indefinitely); (iii) the agent portal had no password lockout policy (so users could try any number of passwords to log on to the agent portal and would not be locked out); (iv) agents could use prior passwords after password resets (thus increasing the likelihood that an already compromised password would be re-used); (v) passwords could be and were shared by all the agents in an agency (which made them more vulnerable to theft or compromise, and made it harder to detect anomalous activity); and (vi) National General manually offboarded users to the agent portal, and apparently did not actually terminate system access to many users when they no longer sold National General insurance (making it possible for former agents to retain agent portal credentials and to continue their access to sensitive information without authorization). *See infra* ¶ 114. All of these factors made

the agent portal vulnerable to an attack, as they increased the likelihood that bad actors could guess, steal, or crack a user's password and then get access to sensitive information through the agent portal.

72. In addition, National General did not require agents to use a second authentication step—such as a code sent to a personal device or a prompt from a dedicated application—or reasonable alternative controls to log in to the agent portal. Multi-factor authentication ("MFA") is an additional layer of security that helps prevent unauthorized access to accounts that store or process sensitive information, especially when the accounts are internet-facing. National General had implemented MFA on certain systems but not the agent portal, even though it gave agents access to consumers' private information on National General's internal systems.

73. Moreover, National General had been on notice that its websites might be targets of attacks but had not taken action. For instance, in September 2019, National General personnel discussed an attack on State Farm Insurance where compromised user credentials were used to access policyholders' accounts. At that time, National General's information security leadership team considered which of the company's websites might be the target of similar attacks and identified measures that could mitigate a "credential stuffing" attack (in which attackers attempt to use stolen username-password pairs to access other sites). Upon information and belief, this discussion did not lead to strengthened access controls and the agent portal remained weakly protected.

74. In addition, as with the consumer quoting tool, *see supra* ¶¶ 54-55, the agent portal lacked protections that would reduce the risk of bot attacks, including tools to adequately mitigate bot activity and tools to sufficiently monitor for and detect anomalous activity. Thus, the

agent portal was similarly vulnerable to attacks in which consumers' personal information could be serially and rapidly queried without detection.

75. Attackers exploited these weaknesses to gain access to the agent portal quoting tool. As part of the incident postmortem, Allstate determined that attackers used independent agent credentials that had been leaked and/or shared to gain access to the tool as early as October 22, 2020.

76. But National General did not detect the attack until January 28, 2021 and, again, a National General product analyst, rather than a member of the cybersecurity team, noticed the unusual activity.

77. The acquisition of National General by The Allstate Corporation had closed several weeks before, on January 4, 2021. Accordingly, National General informed Allstate of the suspicious quoting activity on the agent portal after it was detected. Around this time, National General also informed Allstate of the prior attack on the consumer quoting tool. Allstate assembled an incident response team that included both Allstate and National General personnel and took the agent portal quoting tool offline to halt the suspicious activity.

78. At Allstate's direction, several system modifications were made to the agent portal before its quoting tool was brought back online, including:

a. Masking DLNs on both the face of the agent portal and in its code;

b. Strengthening the agent portal's password requirements;

c. Enacting automatic password expiration after 90 days;

d. Preventing re-use of old passwords;

e. Disabling approximately 17,000 accounts belonging to inactive independent agencies; and

f. Resetting passwords for all independent agency accounts.

79. With these changes in place, the attacks on the agent portal stopped by February 5, 2021.

80. MFA was eventually instituted for the agent portal, but not until November 2023.

81. More than 187,000 consumers' DLNs, including those of approximately 155,000 New Yorkers, were compromised in the second attack on the agent portal quoting tool.

82. In total, 199,106 consumers' DLNs were compromised during the two attacks on National General's quoting tools, including the DLNs of 165,472 New Yorkers. At least some of the consumers who were impacted were existing National General customers.

83. As noted above, Allstate notified New York state residents impacted by the breaches by April 2, 2021. DFS was notified in February 2021 and OAG in March 2021.

E. <u>The Attackers Who Exploited National General's Quoting Tools Could Use the Stolen DLNs to Harm New York Residents.</u>

84. As noted above, DLNs can be used to commit various forms of identity theft and fraud. *See supra* ¶¶ 40-41. Indeed, the attacks against National General and other auto insurers were "part of a growing fraud campaign targeting pandemic and unemployment benefits."[11]

85. Thus, the individual New Yorkers who received notice that their DLNs may have been compromised during the National General breaches needed to take precautions to prevent fraud, if they could, including by enrolling in credit monitoring services, monitoring credit reports, running background checks to identify if someone fraudulently used their identity, requesting driving records, filing police reports regarding the stolen information, and/or contacting OAG or other government agencies.

[11] DFS Industry Letter, Cyber Fraud Alert (Feb. 16, 2021), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210216_cyber_fraud_alert.

86. And those New Yorkers whose DLNs were used for fraud may have faced and may still face other concrete harms, including shouldering the burden and expense of unwinding any transactions made in their name or repairing damaged credit scores, disputing tax bills for government benefits they never received, facing higher barriers to applying for government benefits in the future, and dealing with delays in receiving future government benefits if their accounts have been flagged as likely fraudulent.

87. National General's failure to notify impacted consumers of the consumer quoting tool breach it detected in November 2020 prevented those consumers from being able to take precautions to guard against fraud and, for those consumers whose DLNs were in fact used for fraud, from being able to promptly address the repercussions of that fraud. In addition, the lack of regulator notification prevented New York state agencies from quickly investigating the issue.

III. The Breaches Were Caused by National General's Failure to Implement Reasonable Data Security Safeguards

88. These breaches were a reflection of, and caused by, National General's failure to implement a data security program that could reasonably safeguard the private data the insurer handled. This failure led to a series of data security gaps that, as detailed in this complaint, left National General open to several forms of attack, including the specific breaches that occurred.

89. Indeed, in its subsequent analysis of the breaches, Allstate personnel placed the blame for the breaches squarely on National General's inadequate data security program. One senior Allstate cybersecurity expert observed:

> "[T]he immature state of infrastructure and application security at National General create[s] a wide aperture for various vectors of compromise, any one of which could result in the outcomes that initially launched this response effort. Additionally, although they are willing and active partners, our [National General] counterparts are not well-positioned to follow-through on the sorts of changes that would bring confidence that this incident is contained."

In other words, National General was highly vulnerable to attacks and its staff was incapable of properly responding to them, even when Allstate provided direction.

90. The same Allstate cybersecurity expert further observed that NPS, National General's policy system to which the quoting tools connected, "[wa]s . . . not built with security in mind, leaving limited options for monitoring and controls." Stated otherwise, NPS, which stored immense amounts of consumers' private information, was not developed in a way that allowed National General to implement key security controls.

91. Thus, prior to the breaches, National General was wide open to potential attacks—the actual breaches that occurred took advantage of only a few of National General's significant data security weaknesses. As detailed below, National General's failure to develop, implement, and maintain reasonable safeguards to protect the security, confidentiality, and integrity of the private information it owned and licensed violated New York's SHIELD Act.

A. <u>National General Did Not Have Reasonable Administrative Safeguards to Protect Private Information.</u>

92. National General failed to implement reasonable administrative safeguards, which are organizational controls used to safeguard sensitive data, resulting in issues that contributed to the breaches. Those control gaps included, but were not limited to, the following failures.

93. ***National General failed to effectively communicate and tailor its data security policies***: By 2019, National General had a data security program on paper, but it had not effectively communicated these written information security policies to employees or ensured staff understood their obligations under them. As a result, the teams in charge of developing and testing the version of the consumer quoting tool that National General launched in or around 2019 were not aware that DLNs were categorized as "Confidential" under National General's

policies—and therefore should not have been shared or viewable publicly—instead creating a tool that *purposefully* exposed entire DLNs in plain text. Moreover, the business personnel who identified the breach of the consumer quoting tool in November 2020 were not even aware that National General *had* an incident response policy, much less how to follow it, leading to a delay in involving the appropriate cybersecurity personnel.

94. In certain instances, moreover, National General employees could not have known how to follow the insurer's data security policies because those policies were not tailored to National General's actual operations. For example, while National General's Data Classification Policy made clear that DLNs could not be posted publicly, *see supra* ¶ 51, the "Confidential Data Transmission" section of its Confidential Data Policy only addressed the security controls associated with the transmission of information via physical mail and faxes, rather than through electronic transmission. Accordingly, even if employees had been aware they needed to protect DLNs—and they were not—National General did not provide them with guidance on how to do so in many common scenarios.

95. ***National General failed to train employees on incident response, including incident reporting***: National General also failed to train its employees on what constitutes a data security incident, how to identify such incidents, or what to do if confronted with a suspected breach. As Allstate's CISO put it, "it [did not] appear that the broader [National General] technology organization understood when it was appropriate to engage cybersecurity or privacy or the law department in the event of an incident."

96. National General's information security leadership was aware of this issue:

a. In February 2018, an external security assessor recommended that National General "[e]stablish and implement a more complete information security activity review (monitoring) policy and procedures," noting it was "unclear how cybersecurity personnel [were] provided with cybersecurity updates and training sufficient to address relevant cybersecurity risks."

b. In September 2020, National General acknowledged that it had an incident response policy "but lack[ed] a true forensic investigation, root cause analysis, communication strategy and [senior] level bre[a]ch exercises," all of which would have made its incident response efforts significantly more effective.

97. These gaps, again, directly impacted National General's inadequate response to the consumer quoting tool breach, as the teams who discovered the breach in November 2020 were slow to involve the cybersecurity team and address the exposure of consumers' private information.

98. Additionally, National General's failure to report the consumer quoting tool breach to consumers and regulators likely reflected the poor understanding its staff, and even its leadership, had of proper procedures related to data security incidents. In its acquisition due diligence, Allstate found that National General "identified an extremely low number of incidents that are reported and investigated." Allstate surmised that "[t]his could be due to a lack of formal reporting process for suspected incidents"; "[g]iven our own experience, it would appear that [National General's] reporting process is not catching all suspected incidents and it's unlikely that there has never been unauthorized access to electronic data." National General's claim that it had experienced few data security incidents was even more suspect given that Allstate's due diligence indicated that National General account credentials were part of publicly disclosed leaks, and dark web forums were selling access to compromised National General user login data.

99. ***Roles within National General's data security program were ill-defined, allowing important functions to fall through the cracks***: National General failed to define roles and responsibilities for data security personnel, resulting in communication problems and gaps that risked the security of consumers' private information. For instance, the cybersecurity team that was responsible for detecting and responding to cyber attacks disavowed responsibility for the security of the data used by National General's web applications, including the consumer quoting tool. As a result, the teams that developed the consumer quoting tool—which allowed outsiders to access sensitive data within National General's internal systems—were in charge of ensuring that the data used or transmitted by the applications was secure, despite having no specialized or experienced cybersecurity personnel. Moreover, this division of responsibility was not documented anywhere, creating additional opportunities for confusion.

100. ***National General failed to conduct necessary risk assessments***: Risk assessments help organizations identify and prioritize potential risks to the security, confidentiality, or integrity of sensitive data. Without them, entities do not know where their vulnerabilities lie and what controls are reasonable for ensuring their data remains secure. Accordingly, risk assessments are required under several data security laws and regimes.

101. As of 2019, National General had a team that was responsible for conducting risk assessments, but that team was under-resourced and did not have the ability to conduct risk assessments regularly or holistically.

102. As a result, as of 2020, National General had not conducted risk assessments of NPS or EPIC, which contained millions of records containing consumers' private information and which National General considered to be "enterprise critical" systems. And National General did not conduct the risk assessment required by HIPAA until 2022 or 2023. Instead, National General

knowingly prioritized risk assessments that were needed to meet certain certifications that would result in "[a]dditional customers" or "additional revenue"—*i.e.*, business priorities drove the risk assessment process. This meant that, for years, there were many parts of National General's technology ecosystem—including those that contained massive amounts of consumers' private data—that the company had not assessed for risks. Because National General did not even know what risks it faced, the company could not implement safeguards or controls to address those risks, and consumers' private data remained vulnerable to attack.

103. ***National General did not have an effective data management program***: A data management program is used to identify what data an entity stores or transmits, ascribe a level of confidentiality to the data, and then ensure the data is appropriately protected based on its confidentiality or criticality. Data management is vital to information security—entities need to know what sensitive data they use and where that data is located in order to safeguard it.

104. Before 2021, National General acknowledged that it was unable "to identify and locate sensitive data in and across [its] systems," despite recognizing that it was "required to [do so to] support a number of regulatory requirements." While National General nominally undertook an effort to locate its sensitive data in 2018, this project was far from complete when Allstate took over National General's data security function in 2021.

105. This lack of data management directly impaired National General's ability to effectively respond to the breaches. During its investigation of the second breach, Allstate found that there were a "considerable number of APIs"—protocols that allow software applications to exchange data—"designed not to require authentication [and] [i]t is currently unclear what they have access to, and they are not hooked into Dynatrace"—a technology used to monitor data flows—"for monitoring." In other words, National General had a considerable number of data apertures

for which the company (i) did not authenticate the user accessing the data, (ii) did not know what data was being exchanged, and (iii) was not monitoring for abuse. As a result, investigators remediating the second breach needed to take time to determine whether these APIs exposed sensitive data and were themselves vulnerable to attack.

106. Without knowing where its data was located, where it was flowing from or to, or who could access it, National General could not properly assign levels of confidentiality to the data or ensure its systems that contained private data had sufficient controls in place.

107. ***National General failed to assess and monitor the third parties, including independent agents, that accessed its systems***: National General lacked an effective third-party risk management program, including with regard to independent agents. Third-party risk management programs include assessing whether a third party—like a vendor, service provider, or agent—has systems in place to protect the entity's data such that the entity is comfortable allowing the third party to access the entity's information. National General, however, failed to conduct these risk assessments for thousands of entities that had access to its data and/or systems, including through the agent portal.

a. *National General did not conduct data security due diligence on independent agents*: The independent agencies that National General contracted with to sell its insurance had access—via the agent portal—to National General's policy platform, NPS, and the private information that NPS stored or used. As National General itself recognized in 2019, third parties that do business with National General "may hold significant amounts of sensitive Company and customer data." And "[i]n the absence of proper procedures, controls and oversight, data that is shared with third parties and vendors"—which would include independent agents—"could be unprotected and improperly handled, increasing the risk of leakage and misuse." At some point in or around 2018, National General began assessing *new* vendors and independent agencies for their data security risks. But, at this time, approximately 4,000 "legacy" New York-based independent agencies—and many more nationwide—had *never* been assessed, even though many had long accessed National General's private information. Even though it was aware of the risks, National General took years to get through the backlog of legacy independent agencies that needed to be assessed for data security. In January 2021, National General was still conducting due diligence on those agencies.

b. *National General failed to address high-risk independent agents*: Even after it began assessing the data security of the New York-based independent agencies with which it did business, National General did not impose any requirements on those independent agents it deemed to be "high risk." As of January 2021, National General considered almost 300 New York-based agencies to be high risk. National General discussed options for addressing the high-risk agents with whom it did business and who had access to National General's private information, but never took action. In other words, high-risk agencies continued to operate as they always had, notwithstanding that National General knew they posed risks to National General's private information. As of fall 2024, National General still had not placed any restrictions on high-risk independent agencies.

B. National General Did Not Have Reasonable Technical Safeguards to Protect Private Information.

108. National General also did not implement reasonable technical safeguards to secure private information. Technical safeguards are the processes used to protect an entity's technology assets, including its systems and data. National General's web applications—like the quoting tools, which transmitted consumers' private data outside of the company via web interfaces—were not protected by reasonable technical safeguards and were not sufficiently monitored by National General.

109. ***National General did not have a secure software development lifecycle***: A software development lifecycle ("SDLC") is a structured process entities adopt to help teams of software developers work in a systematic way. As relevant here, a well-designed SDLC is a process to design, develop, and test high-quality and secure software and, in particular, to ensure an application's code has no unknown vulnerabilities that could be leveraged by attackers.

110. By the time of the breaches in 2020 and 2021, National General's data security leadership had long been aware that the company did not have a comprehensive and secure enterprise-wide SDLC, as an external security assessor had advised National General of this gap years prior. *See infra* ¶ 143. However, the company had continued to develop and release software, including the consumer quoting tool, without a secure SDLC in place, leading to security flaws.

111. After the acquisition in 2021, Allstate reviewed National General's software development standards and found them to be problematic, observing that they did not include "detailed guidance for the protection of sensitive information like DLN throughout the data lifecycle," did not consider the privacy impact of software code changes, and did not provide for "non-functional test cases specific to security [or] privacy." The lack of a secure software development

process, Allstate concluded, meant "application developers and key stakeholders did not identify DLN as a high-risk data element requiring additional security controls." Moreover, Allstate found that National General's privacy and security training for its software developers was inadequate.

112. ***National General did not conduct comprehensive penetration tests of its web applications***: Penetration tests are simulated attacks on a system to identify vulnerabilities and evaluate the system's security, and are required by multiple regulations and industry standards. They often are conducted on specific web applications and systems to detect vulnerabilities. Prior to 2021, National General did not regularly conduct penetration tests on all of its internet-facing websites and, specifically, had not conducted comprehensive penetration tests against many of the web applications connected to NPS. And while a vendor had conducted at least one penetration test of one of the auto insurance quoting sites in April 2020, Allstate later found that the test "did [not do] much more than automated testing with common testing tools." In other words, the penetration test was designed to identify technical issues, such as potential vulnerabilities in the code of the site, but not to identify glaring privacy issues—like the plain text exposure of DLNs—purposefully coded into the quoting interface itself.

113. ***National General did not implement tools to protect its websites***: National General failed to invest in technological tools that would protect its websites from attack. These included:

a. <u>*Bot protections*</u>: There are several technologies companies can use to slow down bot attacks. These mechanisms include behavioral analysis tools (which can prevent users that appear to be bots from continuing to query websites), limitations on the number of quotes a user can request in each session on the website (*i.e.*, within a certain timeframe without leaving the site and returning), and interactive features that slow down bots, like a CAPTCHA. National General did not have mechanisms in place on its quoting tools to sufficiently mitigate bot attacks.

b. *Monitoring tools*: Monitoring tools help organizations detect and respond to potential threats to their systems. National General did not sufficiently monitor activity on its quoting websites, despite the fact that these applications provided access from the internet to consumers' private data on NPS. In 2018, one of National General's information security leaders suggested that National General was not willing to invest in appropriate monitoring tools because the company had "angst . . . with spending money appropriate to [its] size and complexity." This lack of investment resulted in National General being slow to detect the attacks on its quoting tools, which were ultimately identified by the product team as they monitored for the purchase of fraudulent policies.

c. *Web application firewall*: A web application firewall ("WAF") is another type of security tool that monitors incoming web traffic and can be configured to detect and/or block malicious traffic. National General's cybersecurity team had requested funding for a WAF "a few times" before 2021, but "it had been removed from the budget each year," notwithstanding that, in the words of National General's head of IT infrastructure, "[b]est practice would have on[e] for all publicly accessible apps."

114. ***The access controls for the agent portal were weak***: Once logged in to National General's agent portal, a user could access (1) consumer information through the quoting tool and (2) information about the independent agent's or agency's entire book of business, including

customer policy information. National General's weak access controls (*i.e.*, measures that limit who can access certain data) for the agent portal meant this sensitive information was not sufficiently secured. These weak access controls, which can comprise both technical and administrative safeguards, included:

a. National General manually onboarded and offboarded users to its systems, including the agent portal, and apparently did not actually terminate system access to many users after they no longer sold National General insurance. As a result, after the second breach, approximately 17,000 accounts belonging to inactive agencies needed to be disabled. And, prior to the breaches, National General could not permanently disable independent agent accounts *at all*.

b. National General's process for providing independent agencies with credentials for the agent portal was insecure and created the potential for data leakage. Specifically, National General generated two agent portal user IDs for each independent agency: one was an "admin" ID, and the other was meant to be shared (and was, in fact, shared) among all agents for that independent agency writing and maintaining National General business. These passwords were auto-generated by NPS and sent in plain text, *i.e.*, not protected or masked, in an unencrypted email to the agency.

c. National General did not have the ability to automatically reset passwords for the agent portal.

d. National General's password policy did not require passwords for the agent portal to be sufficiently long and complex such that they would be difficult to crack or guess.

e. National General allowed agents to use prior passwords after password resets, thus increasing the likelihood an already compromised password would be re-used.

f. Agent portal passwords did not expire (in other words, independent agents could use the same password indefinitely) and the agent portal had no password lockout policy (so independent agents could try an infinite number of passwords to log on to the agent portal and would not be locked out).

g. National General did not require independent agents to use MFA (which requires users to enter more than just a username and password when logging in to an application or system), or reasonable alternative controls, to access the agent portal. The agent portal was an external method for accessing sensitive data on National General's internal network. Thus, compromised credentials could be used to directly access consumers' private data, without any backstop.

IV. The Data Security Issues That Led to the Breaches Were Representative of National General's Broader Information Security Failings

115. The lapses in National General's data security that led to the breaches were representative of National General's broader data security failings.

116. Prior to the incidents, Allstate had known from the due diligence process that National General had not implemented "several foundational cybersecurity controls" and that the company's "privacy and security program and related compliance processes [we]re immature for an organization of [its] size." But it turned out that National General's problems were, in the words of Allstate's CISO, more "pervasive or more deeply rooted" than Allstate had anticipated.

117. After National General alerted Allstate to the second breach, Allstate launched an investigation into the quoting tool incidents that led to a deeper dive into the state of National General's data security program. What Allstate discovered was sufficiently alarming that it paused its planned migration of data from Allstate's independent agent business to NPS and EPIC because the systems were too insecure and, therefore, the risks to Allstate of the migration were too high. This issue was reflective of the significant problems with National General's data security program, and its non-compliance with several other data security laws and standards in addition to the SHIELD Act.

A. National General Was Not Compliant with HIPAA's Security Rule.

118. The HIPAA Security Rule requires regulated entities (*i.e.*, entities subject to HIPAA) to use reasonable and appropriate security measures to protect any electronic protected health information ("ePHI") that they create, receive, maintain, or transmit. 45 C.F.R. § 164.306(a)(1), (b)(1). For example, regulated entities are required to conduct risk assessments, 45 C.F.R. § 164.308(a)(1)(ii)(A); implement security measures sufficient to reduce security risks and vulnerabilities to a reasonable and appropriate level consistent with the standards of the HIPAA Security Rule, *id.* §§ 164.306(a), 164.308(a)(1)(ii)(B); implement policies and procedures to address security incidents, *id.* § 164.308(a)(6)(i); and implement measures to guard against unauthorized access to ePHI, *id.* §§ 164.312(d), 164.312(e)(1).

119. Upon information and belief, National General launched its Accident & Health business line in or around 2012. The entities in that business line—which create, receive, maintain, and/or transmit ePHI—are subject to the HIPAA Security Rule. But, as described above, National General failed to implement reasonable safeguards to protect consumers' sensitive data—whether that data was DLNs or ePHI. *See supra* ¶ 102 (no HIPAA risk assessment); ¶¶ 108-113

(inadequate application security); ¶¶ 93-98 (failure to effectively communicate and train on incident response policies); ¶ 114 (inadequate access controls); ¶ 107 (lack of diligence and monitoring of third parties with access to consumer data).

120. Indeed, National General only truly launched its HIPAA compliance efforts in 2020, when it began to assess its HIPAA Security Rule compliance gaps, started to identify the location and scope of its ePHI, and launched an effort to institute the HIPAA-required role-based access controls. And although National General was "targeting March of 2021 to be 'reasonably and appropriately' compliant with the HIPAA . . . Security Rule[]," it did not complete its first HIPAA risk assessment until 2022 or 2023.

B. National General Was Not Compliant with DFS's Cybersecurity Regulation.

121. DFS's 2017 Cybersecurity Regulation (often referred to as Part 500) requires DFS licensees—including the National General entities that experienced the online quoting tool breaches—to "design a [cybersecurity] program that addresses [their] risks in a robust fashion" by implementing a series of risk-based protections or, where the specific protection identified cannot be implemented, reasonable alternative controls. *See generally* 23 NYCRR Part 500 (2017). Licensees must annually certify that they are in compliance with Part 500 and report any cybersecurity events to DFS's superintendent within 72 hours. *Id.* § 500.17.

122. For each year from at least 2018 through 2020, the National General entities that are DFS licensees certified that they were compliant with the Cybersecurity Regulation. But National General was in violation of many provisions of Part 500 during that time.

123. Indeed, in early 2021, the "[l]ack of [National General]'s NYDFS cyber compliance" was "of 'high' concern" to Allstate. Allstate believed that "should a [National General] entity be

subject to a [DFS] regulatory exam" there was a "significant risk" that "it would not be able to adequately substantiate its compliance."

124. As a general matter, National General was not in compliance with Part 500's overarching requirement that licensees maintain a cybersecurity program that, among other things, is based on the licensee's risk assessment; protects nonpublic information on the licensee's information systems; and detects, responds to, and recovers from cybersecurity events. *See* 23 NYCRR § 500.02; *see also supra* ¶¶ 100-102 (insufficient risk assessments); ¶¶ 92, 99, 103-114 (lack of reasonable safeguards and controls); ¶¶ 93-98 (failure to effectively communicate and train on incident response policies).

125. In its 2021 review of National General's compliance with DFS's Cybersecurity Regulation, Allstate found that, among many other compliance issues, National General had not even defined the scope of its DFS cybersecurity program properly, as National General had not included all systems storing, transmitting, or processing nonpublic information within its prior Part 500 compliance efforts.

126. National General also failed to comply with specific provisions of Part 500, including Section 500.08's requirement to implement policies and procedures designed to ensure application security, *see supra* ¶¶ 108-113; Section 500.09's requirement to conduct periodic risk assessments of the licensee's information systems, *see supra* ¶¶ 100-102; Section 500.11's requirement to implement policies and procedures designed to ensure the security of information systems and nonpublic information accessible to third-party service providers, *see supra* ¶ 107; Section 500.12(b)'s requirement to use MFA or reasonably equivalent or more secure access controls for any individuals accessing the licensee's internal network from an external network

(like the agent portal), *see supra* ¶ 114(f); and Section 500.17(a)'s requirement to timely notify DFS of cybersecurity events, *see supra* ¶ 83.

C. National General Was Not Compliant with the GLBA and Its Implementing Regulations.

127. The GLBA, which was enacted in 1999, requires financial institutions, including insurance companies, to safeguard nonpublic customer information. 15 U.S.C. § 6801. It authorizes federal and state regulatory entities to issue regulations enforcing this requirement. *Id.* § 6805(a); *see also* N.C. Gen. Stat. Ann. § 58-39-130 *et seq.*; Mo. Ann. Stat. § 362.422; Mo. Code Regs. Ann. tit. 20, § 100-6.110.

128. As of May 2021, National General had not even assessed its compliance with the GLBA (or, presumably, the GLBA's implementing regulations). Had it conducted such an assessment, though, it would have identified several areas of noncompliance. As alleged above, National General failed to implement appropriate or reasonable safeguards to protect nonpublic consumer, including customer, data. *See supra* ¶¶ 100-102 (insufficient risk assessments); ¶¶ 103-106 (lack of data management); ¶¶ 108-113 (insufficient application security); ¶ 113(b) (inadequate monitoring); ¶ 107 (lack of third-party due diligence); ¶¶ 93-98 (failure to effectively communicate and train on incident response policies). National General did not even know where sensitive customer information was stored or used, *see supra* ¶¶ 103-106, and thus could not ensure reasonable safeguards were in place to protect it.

D. National General Was Not Compliant with PCI DSS.

129. National General has long been subject to PCI DSS, which sets minimum data security standards for entities that store, process, or transmit payment cardholder data and/or

authentication information (in other words, consumers' credit, debit, and/or cash card information).

130. From approximately 2017 through 2020, National General struggled to comply with the payment card regime and fell out of compliance on multiple occasions, despite only monitoring a subset of its systems for PCI DSS compliance.

131. A primary challenge National General faced in complying with PCI DSS related to the company's vulnerability management and patching program. PCI DSS requires companies to regularly scan their in-scope systems for vulnerabilities and to patch those vulnerabilities; covered companies must produce a "clean" scan (*i.e.*, a scan with no unpatched critical or high vulnerabilities) on a quarterly basis in order to be compliant with PCI DSS. But National General often struggled, and sometimes failed, to get a clean scan. For instance, in Q2 2020, National General was unable to provide a clean scan after identifying 12,000 vulnerabilities that could not be timely remediated.

132. These issues were deeply entrenched. In 2020, National General "self-identified" to Allstate "numerous deficiencies with its [PCI] compliance" and, even in 2022, Allstate found that National General was not meeting all PCI DSS requirements.

V. National General Misrepresented Its Data Security to Consumers

133. National General falsely led customers, and consumers more broadly, to believe that it had reasonable safeguards in place to protect personal information.

134. For example, National General sent policyholders a privacy notice that represented the company would comply with data security laws and regulations, which as a general matter required National General to develop, implement, and maintain reasonable or appropriate data security safeguards. *E.g.*, GBL § 899-bb(2); N.C. Gen. Stat. Ann. § 58-39-145 (requiring North

Carolina-based insurance companies to implement appropriate information security safeguards); Mo. Code Regs. Ann. tit. 20, § 100-6.110 (same for Missouri-based insurance companies). Specifically, beginning in 2017, the notice stated:

> **<u>How Do We Protect The Information That We Collect About You and Your Accounts?</u>**
>
> To protect the privacy and security of nonpublic personal information we collect about you, we restrict access to the information to our employees, agents and subcontractors who need this information to provide products and services to you. **We maintain physical, electronic, and procedural safeguards that comply with applicable federal and state laws and regulations to guard your non-public personal information.** We strive to keep our information about you accurate. We require those individuals to whom we permit access to your customer information to protect it and keep it confidential . . . . (Emphasis added.)

135. This notice was sent to policyholders of, among others, Integon National Insurance Company, Integon Casualty Insurance Company, Integon Indemnity Corporation, Integon General Insurance Corporation, Integon Preferred Insurance Company, National General Assurance Company, National General Insurance Company, and New South Insurance Company—*i.e.*, all of the National General entities that were breached.

136. National General's online privacy policy—which also was issued on behalf of and explicitly applied to all of the National General entities that were breached—promised that the company would protect personal information consumers provided to National General when visiting its websites. That policy provided:

> **What Steps Do You Take to Protect Personal Information About Me?**
>
> We restrict access to the information obtained from our web sites and web pages to our employees, agents and contractors. We maintain physical, electronic and procedural safeguards designed to protect your personal information.

137. The personal information referenced depended on the website the consumer visited, but the policy explained it "may include" name, address, SSN, telephone number, National General

policy or account number, financial information, email address, email referral information, and DOB.

138. National General acknowledged the importance consumers place on data security generally and on National General's representations regarding its data security practices in particular. For example, the first paragraph of National General's online privacy policy stated:

> You take online privacy seriously and so does National General Insurance. We are a group of companies committed to protecting the personal information of visitors to our web sites and web pages. **This policy is one way of sustaining your trust in our companies, our products and our services**. (Emphasis added.)

139. National General's online privacy policy was the same between 2010 and at least May 2021.

140. After the acquisition, Allstate's privacy and compliance function began overseeing National General's equivalent function. Allstate also hired an external vendor to assess and recommend enhancements to National General's privacy program, including regarding updates to and the distribution of National General's privacy policies.

141. National General's representations—both before and after the acquisition—were misleading and deceptive. As described above, in numerous instances continuing through at least 2021, National General failed to use reasonable or appropriate safeguards to protect personal information, or to implement safeguards that it was otherwise legally required to maintain.

VI. National General and Allstate Knew National General's Data Security Was Inadequate

142. National General knew for years that its data security was not only inadequate, but that it failed to comply with applicable laws and regulations. Allstate, likewise, knowingly took over and managed a noncompliant National General program after the acquisition.

143. In February 2018, National General hired an external cybersecurity assessor to identify gaps in its compliance with the HIPAA Security Rule, Part 500, and PCI DSS. The assessor identified many issues, including that:

a. National General did not have a documented policy or process regarding risk assessments;

b. National General's SDLC process lacked basic security controls, application security requirements were not documented, no security experts were involved in the SDLC, and "[n]ew threats and vulnerabilities for external-facing applications needed to be addressed";

c. National General's access controls were weak, including because the insurer provided users access to systems to which the users did not require access, did not ensure accounts were deactivated after termination, and allowed users to share IDs and passwords;

d. National General's monitoring program had many gaps;

e. National General had not instituted critical elements of a vendor management program;

f. National General had not conducted a risk-based analysis regarding MFA, and several avenues of external access to National General's internal network did not require MFA; and

g. National General had not formalized roles and responsibilities for security incident response duties, and the security incident response procedures were missing important elements and "d[id] not cover notifications."

144. The next year, in 2019, National General's internal audit team drafted a report on National General's cybersecurity program. It identified several structural issues with the program, concluding that the "[l]ack of a clearly defined and centralized Cybersecurity program creates the potential for threats to go undetected and unmitigated, and the organization to be exposed and vulnerable." The report also identified several specific issues, including ones that the external assessor had flagged the year before. For example, the internal auditors raised that National General was not assessing and monitoring all third-party vendors, notwithstanding that they "may hold significant amounts of sensitive Company and customer data" and that, without proper oversight, there was an increased "risk for leakage and misuse" of data. The 2019 audit report also highlighted application security issues, including that there were "no procedures in place to properly vet and onboard new applications" or to "track the maintenance of existing applications within the organization," and that without such processes, "new applications containing security gaps and other exploitable flaws could expose critical and sensitive data to loss and misuse."

145. Most, if not all, of these gaps had yet to be addressed by the time of the breaches and the acquisition. And Allstate was fully aware that National General was missing "several foundational cybersecurity controls" and had an "immature" privacy and security program, *see supra* ¶ 116, when it decided to move forward with the acquisition.

146. The second breach occurred shortly after the acquisition, at which point Allstate (specifically, upon information and belief, teams at and employees of Allstate Insurance Company) took control of National General's privacy and data security functions.

147. Allstate's control of National General's privacy and data security functions included analyzing and responding to privacy and cybersecurity incidents, conducting risk assessments of

National General's technology systems and applications, reviewing the testing and monitoring of National General's technology systems and applications, directing the remediation of gaps within National General's data security program, and managing National General's efforts to come into compliance with DFS's Part 500 regulations. Allstate's takeover of National General's data security program also included the replacement of National General's data security leadership team. Specifically, Allstate replaced National General's CISO, whom Allstate's own CISO observed had limited cybersecurity experience and lacked the technical understanding necessary to be effective.

148. Allstate initially estimated that it would take as many as two to three years to implement the changes to National General's data security program that were needed to mitigate the risks identified during due diligence. However, as of late 2024 (more than three years after the breaches and acquisition), Allstate's CISO believed more work still needed to be done to remediate National General's data security program.

149. Upon information and belief, National General remained non-compliant with New York's SHIELD Act (and other data security laws and regulations) for a significant period of time after the breaches were remediated.

CAUSES OF ACTION

FIRST CAUSE OF ACTION
(GBL § 899-aa: Notification)
AGAINST NATIONAL GENERAL

150. OAG repeats and realleges paragraphs 1 through 149 as if fully set forth herein.

151. In 2020 and 2021, GBL § 899-aa required that any person or business that owns or licenses computerized data disclose, in the most expedient time possible and without unreasonable delay, a breach of security to all New York state residents whose private

information was, or is reasonably believed to have been, accessed or acquired without valid authorization.

152. Furthermore, in 2020 and 2021, GBL § 899-aa required that, in the event New York state residents were required to be notified of a breach, the person or business also notify OAG, the New York Department of State, and the New York Division of State Police.

153. As set forth above, National General owns and licenses computerized data which includes private information.

154. As set forth above, National General knowingly or recklessly violated GBL § 899-aa by failing to disclose a breach of security to New York state residents whose private information was, or is reasonably believed to have been, accessed or acquired without valid authorization in or around 2020, and by failing to notify the appropriate New York state agencies of the breach.

SECOND CAUSE OF ACTION
(GBL § 899-bb: Data Security Protections)
AGAINST ALL DEFENDANTS

155. OAG repeats and realleges paragraphs 1 through 149 as if fully set forth herein.

156. GBL § 899-bb requires that any person or business that owns or licenses computerized data which includes private information of New York state residents develop, implement, and maintain reasonable safeguards to protect the security, confidentiality, and integrity of the private information.

157. Any person or business that fails to comply with GBL § 899-bb shall be deemed to have violated GBL § 349, and OAG may bring an action to enjoin such violations and obtain civil penalties.

158. As set forth above, National General owns and licenses computerized data which includes private information of New York state residents.

159. As set forth above, National General failed to implement reasonable safeguards to protect the security, confidentiality, and integrity of private information of New York state residents. And, after Allstate took over National General's data security function in or around January 2021, National General continued to lack reasonable safeguards to protect the security, confidentiality, and integrity of private information of New York state residents.

160. For the same reasons, both before and after Allstate took over National General's data security function in or around January 2021, National General also failed to comply with the GLBA and its regulations, regulations implementing HIPAA and the HITECH Act, DFS's Cybersecurity Regulation, or any other data security rules and regulations of, and statutes administered by, the federal or New York state government.

THIRD CAUSE OF ACTION
(GBL § 349: Deceptive Business Practices)
AGAINST ALL DEFENDANTS

161. OAG repeats and realleges paragraphs 1 through 149 as if fully set forth herein.

162. GBL § 349 prohibits deceptive acts or practices in the conduct of any business, trade, or commerce or in the furnishing of any service in the state of New York.

163. Defendants have engaged in repeated and persistent deceptive acts and practices in violation of GBL § 349, including but not limited to misrepresenting—both before and after Allstate took over National General's data security function in or around January 2021—to consumers and customers, expressly and by implication, that National General provided reasonable safeguards to protect consumers' and customers' personal information.

FOURTH CAUSE OF ACTION
(GBL § 350: False Advertising)
AGAINST ALL DEFENDANTS

164. OAG repeats and realleges paragraphs 1 through 149 as if fully set forth herein.

165. GBL § 350 prohibits false advertising in the conduct of any business, trade, or commerce or in the furnishing of any service in the state of New York.

166. Defendants have engaged in repeated and persistent false advertising in violation of GBL § 350, including but not limited to misrepresenting—both before and after Allstate took over National General's data security function in or around January 2021—to consumers and customers, expressly and by implication, that National General provided reasonable safeguards to protect consumers' and customers' personal information.

FIFTH CAUSE OF ACTION
Executive Law § 63(12) (Illegality)
(GBL § 899-bb: Data Security Protections)
AGAINST ALL DEFENDANTS

167. OAG repeats and realleges paragraphs 1 through 149 as if fully set forth herein.

168. Executive Law § 63(12) authorizes OAG to seek injunctive and other equitable relief when any individual or business engages in repeated and persistent illegal conduct in the carrying on, conducting, or transaction of business in the state of New York.

169. GBL § 899-bb requires that any person or business that owns or licenses computerized data which includes private information of New York state residents develop, implement, and maintain reasonable safeguards to protect the security, confidentiality, and integrity of the private information.

170. As set forth above, National General owns and licenses computerized data which includes private information of New York state residents.

171. As set forth above, National General failed to implement reasonable data security safeguards to protect the security, confidentiality, and integrity of private information of New York state residents. And, after Allstate took over National General's data security function in or

around January 2021, National General continued to lack reasonable safeguards to protect the security, confidentiality, and integrity of private information of New York state residents.

172. For the same reasons, both before and after Allstate took over National General's data security function in or around January 2021, National General also failed to comply with the GLBA and its regulations, regulations implementing HIPAA and the HITECH Act, DFS's Cybersecurity Regulation, or any other data security rules and regulations of, and statutes administered by, the federal or New York state government.

173. By these actions in violation of GBL § 899-bb, Defendants have engaged in repeated and persistent illegality in violation of Executive Law § 63(12).

SIXTH CAUSE OF ACTION
Executive Law § 63(12) (Illegality)
(GBL § 349: Deceptive Business Practices)
AGAINST ALL DEFENDANTS

174. OAG repeats and realleges paragraphs 1 through 149 as if fully set forth herein.

175. Executive Law § 63(12) authorizes OAG to seek injunctive and other equitable relief when any individual or business engages in repeated and persistent illegal conduct in the carrying on, conducting, or transaction of business in the state of New York.

176. GBL § 349 prohibits deceptive acts or practices in the conduct of any business, trade, or commerce or in the furnishing of any service in the state of New York.

177. Defendants have engaged in repeated and persistent deceptive acts and practices in violation of GBL § 349, including but not limited to misrepresenting—both before and after Allstate took over National General's data security function in or around January 2021—to consumers and customers, expressly and by implication, that National General provided reasonable safeguards to protect consumers' and customers' personal information.

178. By these actions in violation of GBL § 349, Defendants have engaged in repeated and persistent illegality in violation of Executive Law § 63(12).

SEVENTH CAUSE OF ACTION
Executive Law § 63(12) (Illegality)
(GBL § 350: False Advertising)
AGAINST ALL DEFENDANTS

179. OAG repeats and realleges paragraphs 1 through 149 as if fully set forth herein.

180. Executive Law § 63(12) authorizes OAG to seek injunctive and other equitable relief when any individual or business engages in repeated and persistent illegal conduct in the carrying on, conducting, or transaction of business in the state of New York.

181. GBL § 350 prohibits false advertising in the conduct of any business, trade, or commerce or in the furnishing of any service in the state of New York.

182. Defendants have engaged in repeated and persistent false advertising in violation of GBL § 350, including but not limited to misrepresenting—both before and after Allstate took over National General's data security function in or around January 2021—to consumers and customers, expressly and by implication, that National General provided reasonable safeguards to protect consumers' and customers' personal information.

183. By these actions in violation of GBL § 350, Defendants have engaged in repeated and persistent illegality in violation of Executive Law § 63(12).

EIGHTH CAUSE OF ACTION
Executive Law § 63(12) (Fraud)
AGAINST ALL DEFENDANTS

184. OAG repeats and realleges paragraphs 1 through 149 as if fully set forth herein.

185. Executive Law § 63(12) authorizes OAG to seek injunctive and other equitable relief when any individual or business engages in repeated and persistent fraud in the carrying on, conducting, or transaction of business in the state of New York.

186. As set forth above, Defendants have engaged in repeated and persistent fraudulent acts, including but not limited to misrepresenting—both before and after Allstate took over National General's data security function in or around January 2021—to consumers and customers, expressly and by implication, that National General provided reasonable safeguards to protect consumers' and customers' personal information.

187. By these actions, Defendants have engaged in repeated and persistent fraudulent conduct in violation of Executive Law § 63(12).

PRAYER FOR RELIEF

WHEREFORE, OAG requests an order and judgment:

a. Permanently enjoining Defendants from violating the laws of the state of New York, including GBL §§ 899-aa, 899-bb, 349, and 350, and Executive Law § 63(12);
b. Directing National General to pay a civil penalty of $20 for each knowing or reckless violation of GBL § 899-aa, pursuant to GBL § 899-aa(6);
c. Directing Defendants to properly notify each New York state resident whose private information was acquired without authorization;
d. Directing Defendants to pay a civil penalty of $5,000 for each violation of GBL Article 22-A, pursuant to GBL § 350-d;
e. Directing such other equitable relief as may be necessary to redress Defendants' violations of New York law;

f. Awarding Plaintiff costs of $2,000 per Defendant pursuant to CPLR § 8303(a)(6); and

g. Granting such other and further relief as the Court deems just and proper.

New York, NY
March 10, 2025

Respectfully submitted,

Letitia James
Attorney General of New York

By: /s Laura Mumm
CHRIS D'ANGELO
Chief Deputy for Economic Justice
KIM BERGER
Bureau Chief, Bureau of Internet and Technology
CLARK RUSSELL
Deputy Chief, Bureau of Internet and Technology
LAURA MUMM
ALEXANDRA HIATT
Assistant Attorneys General, Bureau of Internet and Technology
28 Liberty St.
New York, NY 10005
(212) 416-8433