

1 Russell S. Thompson, IV (029098)
2 Thompson Consumer Law Group, PC
3 5235 E. Southern Ave., D106-618
4 Mesa, AZ 85206
5 602-388-8898
6 866-317-2674 facsimile
7 rthompson@consumerlawinfo.com
8 Attorney for Plaintiffs

9 UNITED STATES DISTRICT COURT
10 FOR THE DISTRICT OF ARIZONA

11 Mary Birdoes and Jeff Bowlin, on behalf) Case No. _____
12 of themselves and all others similarly)
13 situated,

14) **CLASS ACTION COMPLAINT AND**
15) **TRIAL BY JURY DEMAND**

16 Plaintiffs,

17 vs.

18 Drizly LLC and The Drizly Group, Inc.,

19 Defendants.

20 Plaintiffs Mary Birdoes and Jeff Bowlin (collectively “Plaintiffs”), individually
21 and on behalf of all others similarly situated, assert the following claims against
22 Defendants Drizly LLC and The Drizly Group, Inc. (collectively “Defendants” or
23 “Drizly”), based upon personal knowledge, public reporting, information and belief, and
24 the investigation of counsel.

25 **NATURE OF ACTION**

26 1. Plaintiffs bring this Class Action Complaint on behalf of consumers who
27 used the Drizly service and subsequently had their highly sensitive personal information
28 exposed in a data breach. Drizly’s failure to protect its customers’ sensitive personal
information allowed hackers to sell this information on the Dark Web – an underground

1 black market with rampant illegal activity. The Data Breach occurred sometime prior to
2 February 13, 2020, yet Drizly did not alert its customers that their information was
3 exposed until July 28, 2020, stating “that an unauthorized party appears to have obtained
4 some of our customers’ personal information” (the “Data Breach”).
5

6 2. Drizly is an online alcohol delivery service. As part of that service, Drizly
7 collects highly sensitive customer information such as delivery addresses, billing
8 addresses, dates of birth, email addresses, passwords, phone numbers, IP addresses,
9 geolocation data, and credit card information. While Drizly acknowledged that some of
10 this information such as email and delivery addresses was breached, startup and
11 technology news site www.TechCrunch.com (“TechCrunch”) reported that nearly all of
12 this information was available for approximately 2.5 million Drizly accounts.¹
13
14

15 3. TechCrunch was able to obtain a portion of the Data Breach information
16 and was able to verify the data against public records. The portion of the data that
17 TechCrunch obtained contained highly sensitive customer information. TechCrunch
18 identified the source of the data as a February 13, 2020 Dark Web post. That Dark Web
19 listing additionally contains Drizly users’ credit card numbers and order histories, placing
20 customers at high risk for fraud, identity theft, and other financial crimes.
21
22

23 4. Drizly not only failed to protect its customers highly sensitive information,
24 it also failed to discover and disclose the full scope of the Data Breach. Drizly failed to
25 disclose the Data Breach for over five months – from February 13, 2020 to July 28, 2020.
26
27

28

¹ Zack Whittaker, *Alcohol Delivery Service Drizly Confirms Data Breach*, TechCrunch (July 28, 2020),
<https://techcrunch.com/2020/07/28/drizly-data-breach/>.

1 Drizly failed to maintain reasonable security measures, and as a result, Plaintiffs and
2 Class Members were not afforded adequate notice that their customer information was
3 compromised for five months and were unable to take proactive measures to mitigate the
4 harm caused by the Data Breach.
5

6 5. Plaintiffs' and Class Members' sensitive customer information is still
7 available for purchase by cyber criminals on the Dark Web and may circulate for years in
8 illicit forums. Therefore, Plaintiffs and Class Members have sustained an immediate,
9 tangible injury as a direct result of the Data Breach. Plaintiffs and Class Members
10 extended time and effort in reviewing bank and credit card statements in order to mitigate
11 the effects of the Data Breach.
12

13 6. Plaintiffs seek to remedy the harms caused by Drizly on behalf of
14 themselves and all similarly situated individuals whose sensitive customer data was stolen
15 in the Data Breach. Plaintiffs and Class Members seek reimbursement of losses due to
16 fraud, identity theft, and other financial losses, compensation for time spent in response
17 to the Data Breach, credit monitoring and identity theft insurance, and injunctive relief
18 requiring Drizly to improve its data security practices.
19
20
21

22 **JURISDICTION AND VENUE**

23 7. This Court has subject matter jurisdiction under the Class Action Fairness
24 Act, 28 U.S.C. § 1332(d) because this is a class action involving more than 100 class
25 members, the amount in controversy exceeds \$5 million, and members of the class are
26 citizens of states different from Drizly.
27
28

1 21. It is important to note that Drizly has not yet indicated when the hack
2 occurred, how long the Data Breach lasted and its users' sensitive customer data was
3 exposed, when Drizly detected and became aware of the Data Breach, or how many
4 accounts were affected. But, Drizly advised users to change their passwords.
5

6 22. However, an anonymous spokesperson for Drizly stated to TechCrunch
7 that: "In terms of scale, up to 2.5 million accounts have been affected. Delivery address
8 was included in under 2% of the records. And as mentioned in our email to affected
9 consumers, no financial information was compromised." Drizly's notification to its
10 customers similarly stated, "it's important to note that no financial information -- i.e.
11 neither credit card nor debit card information -- was compromised."
12

13 23. Drizly's account of the Data Breach appears to be an intentional
14 understatement of its scope and magnitude. For example, while Drizly claimed that no
15 "financial information" was taken in the Data Breach, a screen capture (Figure 1)
16 obtained by TechCrunch shows the exact opposite. Figure 1 below is a dark web posting
17 from February 13, 2020 by a well-known seller of stolen credit card data. The listing
18 offers to sell "Fresh Hacked drizly.com Account [sic] with Valid CC attached and Order
19 History" for \$14.
20
21
22
23
24
25
26
27
28

Figure 1

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

The screenshot shows a marketplace listing for a 'Fresh Hacked drizly.com Account with Valid CC attached and Order History'. The listing includes a product image with a red bull logo and text 'ALCOHOL DELIVERY FROM OUR APP TO YOUR DOOR DRIZLY'. The product details are as follows:

Features		Features	
Product Class	Digital	Origin Country	United States
Quantity Left	Unlimited	Ships to	World Wide
Ends In	Never	Payment	Escrow

Additional details include: '- 0 sold since February 13, 2020', 'Vendor Level 5', 'Trust level 5', and 'D 310 (4.58)'. The purchase price is 'USD 14.00'. There are three 'Buy Now' buttons (Bitcoin, Litecoin, XMR) and a 'Queue' button. The listing also includes a description, feedback, and refund policy section.

24. The Drizly “Fresh Hacked” post in Figure 1 demonstrates that hackers successfully obtained Drizly users’ sensitive customer data, including credit card numbers, resulting in the harm already sustained by Plaintiffs and Class members.

25. Additionally, the “Fresh Hacked” post confirms that Plaintiffs and Class members are at a significant and imminent risk of future harm of identity theft and fraud, including fraudulent charges that may be placed on customers’ cards, as cybercriminals on the dark web are able to purchase their financial information and use it to commit identity theft and fraud.

26. Drizly failed to properly safeguard Plaintiffs’ and Class members’ information or timely notify them that sensitive customer data was stolen, allowing cybercriminals to access its users’ sensitive customer data since at least February 13,

1 2020, when the “Fresh Hacked” dump of sensitive customer data was posted on the dark
2 web. Drizly also failed to properly monitor its systems. Had it done so, it would have
3 discovered the Data Breach much sooner.
4

5 27. Drizly had a continuing duty pursuant to statute, regulations, the common
6 law, and industry standards to safeguard customers’ sensitive customer data through
7 reasonable and necessary data security measures and practices.
8

9 28. Drizly was—and at all relevant times has been—aware that the sensitive
10 customer data that it obtains and processes is highly sensitive and could be used for
11 nefarious purposes by third parties, such as perpetrating identity theft and making
12 fraudulent purchases.
13

14 29. Drizly also was—and at all relevant times has been—aware of the
15 importance of safeguarding its customers’ sensitive customer data and of the foreseeable
16 consequences that would occur if its data security systems were breached, including the
17 fraud losses and theft that would be imposed on consumers.
18

19 30. Drizly’s data security obligations were particularly important and well-
20 known given the numerous recent malware-based payment card data breaches throughout
21 the retail and food service industry preceding the Data Breach, including breaches at
22 Neiman Marcus, Michaels, Sally Beauty Supply, P.F. Chang’s China Bistro, Eddie
23 Bauer, Goodwill, SuperValu Grocery, UPS, Home Depot, Jimmy John’s, Dairy Queen
24 Restaurants, Staples, Kmart, Noodles & Co., GameStop, Wendy’s, Chipotle, Arby’s,
25 Wawa, and Rutter’s, which have all been widely reported by the media over the last
26
27
28

1 several years. The increase in data breaches, and the risk of future breaches, is widely
2 known throughout the retail and food service industry, including to Drizly.

3
4 31. These warnings, among others, put Drizly on notice that it may be
5 susceptible to a data breach and of the importance of prioritizing data security to prevent
6 a breach. Despite Drizly's knowledge of the likelihood that its customers' payment
7 sensitive customer data would be stolen without reasonable security measures, Drizly
8 failed to implement adequate data security measures that would have prevented hackers
9 from penetrating its systems to steal sensitive customer data.
10

11 **Drizly Violated Industry Standards**

12
13 32. Drizly failed to comply with industry standards for data security and
14 actively mishandled the data entrusted to it by its customers, including Plaintiffs and
15 Class members.
16

17 33. The Payment Card Industry Security Standards Council promulgates
18 minimum standards, which apply to all organizations that store, process, or transmit
19 sensitive customer data. These standards are known as the Payment Card Industry Data
20 Security Standard ("PCI DSS"). PCI DSS is the industry standard governing the security
21 of sensitive customer data, although it sets the minimum level of what must be done, not
22 the maximum.
23
24
25
26
27
28

1 a transaction; to timely upgrade its payment system software; implement proper network
2 segmentation; encrypt sensitive customer data at the POS; restrict access to sensitive
3 customer data to those with a need to know; establish a process to identify; and timely fix
4 security vulnerabilities. Upon information and belief, Drizly failed to comply with some
5 or all of these requirements.

6
7
8 37. As noted in the chart, PCI DSS required Drizly to “protect all systems
9 against malware.” Drizly failed to do so. Drizly specified that it had “identified some
10 suspicious activity involving customer data” and that “an unauthorized party appears to
11 have obtained some of our customers’ personal information...”

12
13 38. PCI DSS also required Drizly to “[t]rack and monitor all access to network
14 resources.” Drizly failed to do so. The hacker(s) had access to Drizly’s system for an
15 unspecified period of time, illustrating that Drizly had materially deficient tracking and
16 monitoring systems in place.

17
18 39. Upon information and belief, Drizly violated numerous other provisions of
19 the PCI DSS, including subsections underlying the chart above. Those deficiencies will
20 be revealed during discovery with the assistance of expert witnesses.

21
22 40. PCI DSS sets the minimum level of what must be done, not the maximum.
23 While PCI compliance is an important first step in securing cardholder data, it is not
24 sufficient on its own to protect against all breaches, nor does it provide a safe harbor
25 against civil liability for a data breach.

26
27 41. At all relevant times, Drizly was well-aware of its PCI DSS obligations to
28 protect cardholder data. Drizly was an active participant in the payment card networks as

1 it collected and likely transmitted thousands (or more) of sets of payment card data per
2 day across 180 geographic market across 26 states.

3
4 42. Industry experts acknowledge that a data breach is indicative of data
5 security failures. For example, research and advisory firm Aite Group has stated: “‘If
6 your data was stolen through a data breach that means you were somewhere out of
7 compliance’ with payment industry data security standards.”³

9 **Drizly Violated the FTC Act**

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

14
15 44. In 2007, the FTC published guidelines that establish reasonable data
16 security practices for businesses. The guidelines note that businesses should protect the
17 personal customer information that they keep; properly dispose of personal information
18 that is no longer needed; encrypt information stored on computer networks; understand
19 their network’s vulnerabilities; and implement policies for installing vendor-approved
20 patches to correct security problems. The guidelines also recommend that businesses
21 consider using an intrusion detection system to expose a breach as soon as it occurs;
22 monitor all incoming traffic for activity indicating someone may be trying to hack the
23
24
25
26

27
28 ³ Lisa Baertlein, *Chipotle Says Hackers Hit Most Restaurants in Data Breach*, REUTERS (May
26, 2017) (accessible at: <https://www.reuters.com/article/us-chipotle-cyber/chipotle-says-hackers-hitmost-restaurants-in-data-breach-idUSKBN18M2BY>) (last visited August 7, 2020).

1 system; watch for large amounts of data being transmitted from the system; and have a
2 response plan ready in the event of a breach.

3
4 45. The FTC also published a document entitled “FTC Facts for Business,”
5 which highlights the importance of having a data security plan, regularly assessing risks
6 to computer systems, and implementing safeguards to control such risks.

7
8 46. The FTC has issued orders against businesses that have failed to employ
9 reasonable measures to secure sensitive customer data. These orders provide further
10 guidance to businesses regarding their data security obligations.

11
12 47. In the years leading up to the Data Breach, and during the course of the
13 breach itself, Drizly failed to follow guidelines set forth by the FTC and actively
14 mishandled the management of its IT security. Furthermore, by failing to have reasonable
15 data security measures in place, Drizly engaged in an unfair act or practice within the
16 meaning of Section 5 of the FTC Act.

17
18 **The Data Breach Damaged Plaintiffs and the Class.**

19
20 48. As a result of Defendants’ deficient security measures and failure to timely
21 and adequately detect the Data Breach, Plaintiffs and Class Members have been harmed
22 by the compromise of their sensitive customer data in the Data Breach.

23
24 49. Plaintiffs and Class members also face a substantial and imminent risk of
25 identity theft and fraudulent charges on credit and/or debit cards. Criminals carried out
26 the Data Breach and stole the sensitive customer data with the intent to use it for
27 fraudulent purposes and/or to sell it, as evidenced by the dark web posting listing Drizly
28 users’ sensitive customer data available for purchase.

1 50. Furthermore, Plaintiffs and Class members will experience an increased
2 likelihood of identity theft and fraud going forward. This is especially true as their email
3 addresses, dates of birth, passwords, address, phone numbers, IP addresses were
4 compromised, and their credit card numbers are currently available for purchase by
5 criminals on the dark web.
6

7
8 51. Also, many Class members will incur out of pocket costs for protective
9 measures such as identity theft protection, credit monitoring fees, credit report fees, credit
10 freeze fees, fees for replacement cards, and similar costs related to the Data Breach.
11

12 52. Plaintiffs and Class members also suffered a “loss of value” of their credit
13 and debit card information when it was stolen by the hacker in the Data Breach. A robust
14 market exists for stolen card information, which is sold on the dark web at specific
15 identifiable prices. This market serves as a means to determine the loss of value to
16 Plaintiffs and Class members.
17

18 53. Plaintiffs and Class members also suffered “benefit of the bargain”
19 damages. Plaintiffs and Class members overpaid for goods that should have been—but
20 were not—accompanied by adequate data security. Part of the price Plaintiffs and Class
21 members paid to Drizly was intended to be used to fund adequate data security. Class
22 members did not get what they paid for.
23

24
25 54. Plaintiffs and Class members have spent and will continue to spend
26 substantial amounts of time monitoring their payment card accounts for identity theft and
27 fraud, disputing fraudulent transactions, and reviewing their financial affairs more closely
28 than they otherwise would have done but for the Data Breach. Plaintiffs and Class

1 members will also spend time obtaining replacement cards and resetting automatic
2 payment links to their new cards. These efforts are burdensome and time-consuming.

3
4 55. Class members who experience actual identity theft and fraud will also be
5 harmed by the inability to use their credit or debit cards when their accounts are
6 suspended or otherwise rendered unusable due to the fraudulent charges. To the extent
7 Class members are charged monthly/annual fees for their credit and/or debit accounts,
8 they are left without the benefit of that bargain while they await receipt of their
9 replacement cards. Class members will also be harmed by the loss of use of and access to
10 their account funds and credit lines or being limited in the amount of money they are
11 permitted to obtain from their accounts. Class members will further be harmed by the loss
12 of rewards points or airline mileage available on credit cards that consumers lost credit
13 for as a result of having to use alternative forms of payment while awaiting replacement
14 cards. This includes missed payments on bills and loans, late charges and fees, and
15 adverse effects on their credit, including decreased credit scores and adverse credit
16 notations.
17
18
19
20

21 56. A victim whose payment card information has been stolen or compromised
22 may not see the full extent of identity theft or fraud until long after the initial breach.
23 Additionally, a victim whose payment card information has been stolen may not become
24 aware of charges when they are nominal, as typical fraud-prevention algorithms may not
25 capture such charges. Those charges may be repeated, over and over again, on a victim's
26 account.
27
28

1 57. The risk of identity theft and fraud will persist for years. Identity thieves
2 often hold stolen data for months or years before using it, to avoid detection. Also, the
3 sale of stolen information on the dark web may take months or more to reach end-users,
4 in part because the data is often sold in small batches as opposed to in bulk to a single
5 buyer. Thus, Plaintiffs and Class members must vigilantly monitor their financial
6 accounts forever.
7

8
9 58. Identity thieves can combine data stolen in the Data Breach with other
10 information about Plaintiffs and Class members gathered from underground sources,
11 public sources, or even plaintiffs' and Class members' social media accounts. Thieves
12 can use the combined data to send highly targeted phishing emails to Plaintiffs and Class
13 members to obtain more sensitive information. Thieves can use the combined data to
14 commit potential crimes including, e.g., opening new financial accounts in Plaintiffs and
15 Class members' names, taking out loans in Plaintiffs and Class members' names, using
16 Plaintiffs and Class members' information to obtain government benefits, filing
17 fraudulent tax returns using Plaintiffs and Class members' information, obtaining driver's
18 licenses in Plaintiffs and Class members' names but with another person's photograph,
19 and giving false information to police during an arrest. Furthermore, the sensitive
20 customer data stolen from Drizly can be used to drain debit card-linked bank accounts,
21 make "clone" credit cards, or to buy items on certain less-secure websites.
22

23
24 59. Drizly acknowledged that Plaintiffs and Class members face a significant
25 risk of various types of identity theft stemming from the Data Breach. Shifting the burden
26 of responding to the Data Breach to consumers, Drizly recommended that affected
27
28

1 customers undertake the following daunting tasks: “reset your Drizly password,”
2 “continue monitoring your account for any unusual activity,” and “consider changing
3 your passwords across any sites/apps that use the same password as your Drizly account.”
4

5 60. Thus, by virtue of that statement, Drizly acknowledges that Plaintiffs and
6 Class members face an actual imminent risk of identity theft beyond just fraudulent credit
7 and debit card transactions.
8

9 61. Drizly has taken no affirmative steps—beyond notifying consumers of the
10 Data Breach—to protect against these broad-based types of identity theft and fraud, such
11 as offering free credit monitoring and identity theft insurance to all customers whose
12 sensitive customer data was stolen in the Data Breach. Drizly’s efforts are wholly
13 insufficient to combat the indefinite and undeniable risk+ of identity theft and fraud
14

15 **CLASS ALLEGATIONS**
16

17 62. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P.
18 23(a), 23(b)(2) and (b)(3) on behalf of a Nationwide Class.
19

20 All persons in the United States whose sensitive consumer data was
21 compromised in the Data Breach made Public by Drizly on July 28, 2020.

22 63. Excluded from the Class is Drizly and its subsidiaries and affiliates; all
23 employees of Drizly and its subsidiaries and affiliates; all persons who make a timely
24 election to be excluded from the Class; government entities; and the judge to whom this
25 case is assigned, including his/her immediate family and court staff.
26
27
28

1 64. Plaintiffs reserve the right to modify, expand or amend the above Class
2 definitions or to seek certification of a class or Classes defined differently than above
3 before any court determines whether certification is appropriate following discovery.
4

5 65. Certification of Plaintiffs' claims for class-wide treatment is appropriate
6 because all elements of Fed. R. Civ. P. 23(a) and (b)(2)-(3) are satisfied. Plaintiffs can
7 prove the elements of their claims on a class-wide basis using the same evidence as
8 would be used to prove those elements in an individual action alleging the same claims.
9

10 66. **Numerosity:** All requirements of Fed. R. Civ. P. 23(a)(1) are satisfied.
11 The members of the Class are so numerous and geographically dispersed that individual
12 joinder of all Class members is impracticable. While Plaintiffs are informed and
13 believes that there are millions of members of the Class, the precise number of Class
14 members is unknown to Plaintiffs. These estimates are based on the fact that Drizly has
15 admitted that "up to 2.5 million accounts have been affected." Class members may be
16 identified through objective means. Class members may be notified of the pendency of
17 this action by recognized, court-approved notice dissemination methods, which may
18 include U.S. mail, electronic mail, internet postings, and/or published notice.
19
20

21 67. **Commonality and Predominance:** All requirements of Fed. R. Civ. P.
22 23(a)(2) and 23(b)(3) are satisfied. This action involves common questions of law and
23 fact, which predominate over any questions affecting individual Class members,
24 including, without limitation:
25

- 26 a. Whether Drizly engaged in active misfeasance and misconduct alleged
27 herein;
28

- 1 b. Whether Drizly owed a duty to Class members to safeguard their sensitive
- 2 customer data;
- 3 c. Whether Drizly breached its duty to Class members to safeguard their
- 4 sensitive customer data;
- 5 d. Whether a computer hacker obtained class members' sensitive customer
- 6 data in the Data Breach;
- 7 e. Whether Drizly knew or should have known that its data security systems
- 8 and monitoring processes were deficient;
- 9 f. Whether Plaintiffs and Class members suffered legally cognizable
- 10 damages as a result of the Data Breach;
- 11 g. Whether Drizly's failure to provide adequate security proximately caused
- 12 Plaintiffs' and class members' injuries; and
- 13 h. Whether Plaintiffs and Class members are entitled to declaratory and
- 14 injunctive relief.

15 68. **Typicality:** All requirements of Fed. R. Civ. P. 23(a)(3) are satisfied.

16 Plaintiffs are members of the Class. Plaintiffs' claims are typical of the claims of all

17 Class members because Plaintiffs, like other Class members, suffered a theft of their

18 sensitive customer data in the Data Breach.

19 69. **Adequacy of Representation:** All requirements of Fed. R. Civ. P.

20 23(a)(4) are satisfied. Plaintiffs are adequate Class representatives because they are

21 members of the class and their interests do not conflict with the interests of other class

22 members that they seek to represent. Plaintiffs are committed to pursuing this matter for

23 the class with the class's collective best interests in mind. Plaintiffs have retained

24 counsel competent and experienced in complex class action litigation of this type and

25 Plaintiffs intends to prosecute this action vigorously. Plaintiffs, and their counsel, will

26 fairly and adequately protect the class's interests.

27

28

1 70. **Predominance and Superiority:** All requirements of Fed. R. Civ. P.
2 23(b)(3) are satisfied. As described above, common issues of law or fact predominate
3 over individual issues. Resolution of those common issues in Plaintiffs' case will also
4 resolve them for the class's claims. In addition, a class action is superior to any other
5 available means for the fair and efficient adjudication of this controversy and no
6 unusual difficulties are likely to be encountered in the management of this class action.
7 The damages or other financial detriment suffered by Plaintiffs and other Class
8 members are relatively small compared to the burden and expense that would be
9 required to individually litigate their claims against Drizly, so it would be impracticable
10 for members of the Class to individually seek redress for Drizly's wrongful conduct.
11 Even if Class members could afford individual litigation, the court system could not.
12 Individualized litigation creates a potential for inconsistent or contradictory judgments
13 and increases the delay and expense to all parties and the court system. By contrast, the
14 class action device presents far fewer management difficulties and provides the benefits
15 of single adjudication, economies of scale, and comprehensive supervision by a single
16 court.
17
18
19
20
21

22 71. **Cohesiveness:** All requirements of Fed. R. Civ. P. 23(b)(2) are satisfied.
23 Drizly has acted, or refused to act, on grounds generally applicable to the Class such
24 that final declaratory or injunctive relief appropriate.
25
26
27
28

**COUNT I
NEGLIGENCE**

1
2
3 72. Plaintiffs re-alleges and incorporates by reference all preceding
4 allegations as if fully set forth herein.

5
6 73. Drizly obtained Plaintiffs' and Class members' sensitive customer data in
7 connection with class members' purchases on Drizly.

8 74. By collecting and maintaining sensitive customer data, Drizly had a duty
9 of care to use reasonable means to secure and safeguard the sensitive customer data and
10 to prevent disclosure of the information to unauthorized individuals. Drizly's duty
11 included a responsibility to implement processes by which it could detect a data breach
12 of this type and magnitude in a timely manner.

13
14
15 75. Drizly owed a duty of care to Plaintiffs and Class members to provide
16 data security consistent with the various requirements and rules discussed above.

17
18 76. Drizly's duty of care arose as a result of, among other things, the special
19 relationship that existed between Drizly and its customers. Drizly was the only party in
20 a position to ensure that its systems were sufficient to protect against the foreseeable
21 risk that a data breach could occur, which would result in substantial harm to
22 consumers.

23
24 77. Also, Drizly had a duty to employ reasonable security measures under
25 Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits
26 "unfair . . . practices in or affecting commerce," including, as interpreted and enforced
27 by the FTC, failing to use reasonable measures to protect confidential consumer data.
28

1 78. Drizly’s duty to use reasonable care in protecting cardholder data arose as
2 a result of the common law, statutes, and regulations described above, but also because
3 Drizly is bound by industry standards and PCI DSS rules to protect sensitive customer
4 data.
5

6 79. Drizly was subject to an “independent duty” untethered to any contract
7 between Plaintiffs and Class members and Drizly.
8

9 80. Drizly breached its duties, and thus was negligent, by failing to use
10 reasonable measures to protect cardholder information. Drizly’s negligent acts and
11 omissions include, but are not limited to, the following:
12

- 13 a. failure to delete cardholder information after the time period necessary to
14 authorize the transaction;
- 15 b. failure to employ systems and educate employees to protect against
16 malware;
- 17 c. failure to comply with industry standards for software and payment
18 system security;
- 19 d. failure to track and monitor access to its network and cardholder data;
- 20 e. failure to limit access to those with a valid purpose;
- 21 f. failure to adequately staff and fund its data security operation;
- 22 g. failure to use due care in hiring, promoting, and supervising those
23 responsible for its data security operations; and
- 24 h. failure to recognize that hackers were stealing sensitive customer data
25 from its network while the Data Breach was taking place.

26 81. It was foreseeable to Drizly that a failure to use reasonable measures to
27 protect sensitive customer data could result in injury to consumers. Further, actual and
28 attempted breaches of data security were reasonably foreseeable to Drizly given the

1 known frequency of payment card data breaches and various warnings from card brands
2 and industry experts.

3
4 82. Plaintiffs and Class members suffered various types of damages as alleged
5 above.

6
7 83. Drizly's wrongful conduct was a proximate cause of Plaintiffs' and Class
8 members' damages.

9
10 84. Plaintiffs and Class members are entitled to compensatory and
11 consequential damages suffered as a result of the Data Breach.

12
13 85. Plaintiffs and Class members are also entitled to injunctive relief requiring
14 Drizly to (among other things): (i) strengthen its data security systems and monitoring
15 procedures; (ii) submit to future annual audits of those systems; and (iii) provide several
16 years of free credit monitoring and identity theft insurance to all Class members.

17
18 **COUNT II**
NEGLIGENCE *PER SE*

19
20 86. Plaintiffs reallege and incorporate all previous allegations as though fully
21 set forth herein.

22
23 87. As alleged above, pursuant to the FTC Act, 15 U.S.C. § 45, Drizly had a
24 duty to provide fair and adequate computer systems and data security practices to
25 safeguard plaintiffs' and Class members' sensitive customer data.

26
27 88. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting
28 commerce," including, as interpreted and enforced by the FTC, the unfair act or practice
by businesses, such as Drizly, of failing to use reasonable measures to protect sensitive

1 customer data. The FTC publications and orders described above also form part of the
2 basis of Drizly's duty.

3
4 89. Drizly violated Section 5 of the FTC Act by failing to use reasonable
5 measures to protect sensitive customer data and not complying with applicable industry
6 standards, including PCI DSS, as described in detail herein. Drizly's conduct was
7 particularly unreasonable given the nature and amount of sensitive customer data it
8 collected and stored and the foreseeable consequences of a data breach, including,
9 specifically, the immense damages that would result to consumers.

10
11 90. Plaintiffs and members of the Class are within the class of persons that
12 Section 5 of the FTC Act was intended to protect, because the FTC Act was expressly
13 designed to protect consumers from "substantial injury."

14
15 91. The harm that has occurred is the type of harm the FTC Act is intended to
16 guard against. Indeed, the FTC has pursued numerous enforcement actions against
17 businesses that, as a result of their failure to employ reasonable data security measures
18 and avoid unfair and deceptive practices, caused the same harm as that suffered by
19 Plaintiffs and Class members.
20
21

22 92. Drizly had a duty to Plaintiffs and Class members to implement and
23 maintain reasonable security procedures and practices to safeguard plaintiffs' and Class
24 members' sensitive customer data.
25

26 93. Drizly breached its duties to Plaintiffs and Class members under the FTC
27 Act, by failing to provide fair, reasonable, or adequate computer systems and data
28 security practices to safeguard plaintiffs' and Class members' sensitive customer data.

1 94. Drizly's violation of Section 5 of the FTC Act and its failure to comply
2 with applicable laws and regulations constitutes negligence *per se*.

3
4 95. But for Drizly's wrongful and negligent breach of its duties owed to
5 Plaintiffs and class members, Plaintiffs and Class members would not have been
6 injured.

7
8 96. The injury and harm suffered by Plaintiffs and Class members was the
9 reasonably foreseeable result of Drizly's breach of its duties. Drizly knew or should
10 have known that it was failing to meet its duties and that its breach would cause
11 Plaintiffs and Class members to suffer the foreseeable harms associated with the
12 exposure of their sensitive customer data.

13
14 97. Had Plaintiffs and Class members known that Drizly did and does not
15 adequately protect customer sensitive customer data, they would not have made
16 purchases on Drizly.

17
18 98. As a direct and proximate result of Drizly's negligence *per se*, Plaintiffs
19 and Class members have suffered harm, including but not limited to loss of time and
20 money resolving fraudulent charges; loss of time and money obtaining protections
21 against future identity theft; financial losses related to the purchases made at Drizly that
22 Plaintiffs and Class members would not have made had they known of Drizly's careless
23 approach to cyber security; lost control over the value of sensitive customer data;
24 unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit
25 and debit card limits and balances; harm resulting from damaged credit scores and
26 information; and other harm resulting from the unauthorized use or threat of
27
28

1 unauthorized use of stolen sensitive customer data, entitling them to damages in an
2 amount to be proven at trial.

3
4 **COUNT III**
5 **BREACH OF IMPLIED CONTRACT**

6 99. Plaintiffs re-allege and incorporate by reference all preceding allegations
7 as if fully set forth herein.

8 100. When Plaintiffs and Class members provided their sensitive customer data
9 to Drizly in exchange for Drizly's products, they entered into implied contracts with
10 Drizly under which Drizly agreed to take reasonable steps to protect the sensitive
11 customer data.

12 101. Drizly solicited and invited Plaintiffs and Class members to provide their
13 sensitive customer data as part of Drizly's regular business practices. Plaintiffs and
14 Class members accepted Drizly's offers and provided their sensitive customer data to
15 Drizly.

16 102. When entering into the implied contracts, Plaintiffs and Class members
17 reasonably believed and expected that Drizly's data security practices complied with
18 relevant laws, regulations, and industry standards.

19 103. Plaintiffs and Class members paid money to Drizly to purchase items on
20 Drizly.

21 104. Plaintiffs and Class members reasonably believed and expected that
22 Drizly would use part of those funds to obtain adequate data security. Drizly failed to
23 do so.
24
25
26
27
28

1 120. Drizly advertised, offered, or sold goods or services in Arizona and
2 engaged in trade or commerce directly or indirectly affecting the people of Arizona.

3
4 121. Drizly engaged in deceptive and unfair acts and practices,
5 misrepresentation, and the concealment, suppression, and omission of material facts
6 affecting the people of Arizona in connection with the sale and advertisement of
7 “merchandise” (as defined in Arizona Consumer Fraud Act, A.R.S. § 44-1521(5)) in
8 violation of A.R.S. § 44-1522(A), including:
9

- 10 a. Failing to implement and maintain reasonable security and privacy
11 measures to protect Plaintiffs and Arizona Class members’ Personal
12 Information, which was a direct and proximate cause of the Data Breach;
- 13 b. Failing to identify foreseeable security and privacy risks, remediate
14 identified security and privacy risks, and adequately improve security and
15 privacy measures following previous cybersecurity incidents, which was a
16 direct and proximate cause of the Data Breach;
- 17 c. Failing to comply with common law and statutory duties pertaining to the
18 security and privacy of Plaintiffs and Arizona Class members’ Personal
19 Information, including duties imposed by the FTC Act, 15 U.S.C. § 45,
20 which was a direct and proximate cause of the Data Breach;
- 21 d. Misrepresenting that it would protect the privacy and confidentiality of
22 Plaintiffs and Arizona Class members’ Personal Information, including by
23 implementing and maintaining reasonable security measures;
- 24 e. Misrepresenting that it would comply with common law and statutory
25 duties pertaining to the security and privacy of Plaintiffs and Arizona
26 Class members’ Personal Information, including duties imposed by the
27 FTC Act, 15 U.S.C. § 45;
- 28 f. Omitting, suppressing, and concealing the material fact that it did not
reasonably or adequately secure Plaintiffs and Arizona Class members’
Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not
comply with common law and statutory duties pertaining to the security

1 and privacy of Plaintiffs and Arizona Class members' Personal
2 Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

3 122. Drizly's representations and omissions were material because they were
4 likely to deceive reasonable consumers about the adequacy of Drizly's data security and
5 ability to protect the confidentiality of consumers' Personal Information.
6

7 123. Drizly intended to mislead Plaintiffs and Arizona Class members and
8 induce them to rely on its misrepresentations and omissions.
9

10 124. Had Drizly disclosed to Plaintiffs and class members that its data systems
11 were not secure and, thus, vulnerable to attack, Drizly would have been unable to
12 continue in business and it would have been forced to adopt reasonable data security
13 measures and comply with the law. Instead, Drizly received, maintained, and compiled
14 Plaintiffs' and class members' Personal Information as part of the services Drizly
15 provided and for which Plaintiffs and class members paid without advising Plaintiffs
16 and class members that Drizly's data security practices were insufficient to maintain the
17 safety and confidentiality of Plaintiffs' and class members' Personal Information.
18 Accordingly, Plaintiffs and the Arizona Class members acted reasonably in relying on
19 Drizly's misrepresentations and omissions, the truth of which they could not have
20 discovered.
21
22

23 125. Drizly acted intentionally, knowingly, and maliciously to violate
24 Arizona's Consumer Fraud Act, and recklessly disregarded Plaintiffs and Arizona Class
25 members' rights. Drizly's past data breaches and breaches within the hospitality
26 industry put it on notice that its security and privacy protections were inadequate.
27
28

1 C. An award to Plaintiffs and the Classes of compensatory, consequential,
2 statutory, and treble damages as set forth above;

3
4 D. Ordering injunctive relief requiring Drizly to (among other things): (i)
5 strengthen its data security systems and monitoring procedures; (ii) submit to future
6 annual audits of those systems; and (iii) provide several years of free credit monitoring
7 and identity theft insurance to all Class members;

8
9 E. An award of attorneys' fees, costs, and expenses, as provided by law or equity;

10 F. An award of pre-judgment and post-judgment interest, as provided by law or
11 equity; and

12
13 G. Such other relief as the Court may allow.

14 **TRIAL BY JURY**

15 128. Plaintiffs are entitled to and hereby demand a trial by jury.

16
17 Dated: August 20, 2020.

Respectfully submitted,

18
19 s/ Russell S. Thompson, IV
20 Russell S. Thompson, IV (029098)
21 Thompson Consumer Law Group, PC
22 5235 E. Southern Ave., D106-618
23 Mesa, AZ 85206
24 602-388-8898
25 866-317-2674 facsimile
26 rthompson@consumerlawinfo.com
27 Attorneys for Plaintiffs
28

UNITED STATES DISTRICT COURT
DISTRICT OF ARIZONA

Civil Cover Sheet

This automated JS-44 conforms generally to the manual JS-44 approved by the Judicial Conference of the United States in September 1974. The data is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. The information contained herein neither replaces nor supplements the filing and service of pleadings or other papers as required by law. This form is authorized for use only in the District of Arizona.

The completed cover sheet must be printed directly to PDF and filed as an attachment to the Complaint or Notice of Removal.

Plaintiff(s): Mary Birdoes ; Jeff Bowlin
County of Residence: Maricopa
County Where Claim For Relief Arose: Maricopa

Defendant(s): Drizly, LLC ; The Drizly Group, Inc.
County of Residence: Outside the State of Arizona

Plaintiff's Atty(s):
Russell S. Thompson IV
Thompson Consumer Law Group, PC
5235 E. Southern Ave., D106-618
Mesa, Arizona 85206
6023888898

Defendant's Atty(s):

II. Basis of Jurisdiction: **3. Federal Question (U.S. not a party)**

III. Citizenship of Principal Parties (Diversity Cases Only)

Plaintiff:- **1 Citizen of This State**
Defendant:- **5 Non AZ corp and Principal place of Business outside AZ**

IV. Origin : **1. Original Proceeding**

V. Nature of Suit: **190 Other Contract**

VI. Cause of Action: **28 U.S. Code § 1332**

VII. Requested in Complaint

Class Action: **Yes**
Dollar Demand:
Jury Demand: **Yes**

VIII. This case is not related to another case.

Signature: s/Russell S. Thompson, IV

Date: 8/20/2020

If any of this information is incorrect, please go back to the Civil Cover Sheet Input form using the *Back* button in your browser and change it. Once correct, save this form as a PDF and include it as an attachment to your case opening documents.

Revised: 01/2014

ClassAction.org

This complaint is part of ClassAction.org's searchable [class action lawsuit database](#)
