JS 44 (Rev. 06/17)

CIVIL COVER SHEET

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

I. (a) PLAINTIFFS

MARIE ABDELMESSIH, individually and on behalf of all others similarly situated,

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

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
LEVIN SEDRAN & BERMAN, 510 Walnut Street, Suite 500
Philadelphia, PA 19106, Telephone: (215) 592-1500

DEFENDANTS

FIVE BELOW. INC.

County of Residence of First Listed Defendant Philadelphia County
(IN U.S. PLAINTIFF CASES ONLY)

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

Attorneys *(If Known)*

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

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

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

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

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

Click here for: Nature of Suit Code Descriptions.

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

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

TORTS

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

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

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

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

PRISONER PETITIONS

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

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

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

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

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

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

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark

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

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

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

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

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

VI. CAUSE OF ACTION

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

Brief description of cause:
Negligence, Invasion of Privacy, Breach of Implied Contract, Negligence Per Se, Breach of Fiduciary Duty

VII. REQUESTED IN COMPLAINT:

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

DEMAND $ 5,000,000.00

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

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE 04/08/2019

SIGNATURE OF ATTORNEY OF RECORD

FOR OFFICE USE ONLY

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

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

DESIGNATION FORM
(to be used by counsel or pro se plaintiff to indicate the category of the case for the purpose of assignment to the appropriate calendar)

Address of Plaintiff: 476 Dogwood Court, Altamonte Springs, Florida 32714

Address of Defendant: 701 Market Street, Suite 300, Philadelphia, PA 19106

Place of Accident, Incident or Transaction: Altamonte Springs, Florida

RELATED CASE, IF ANY:

Case Number: _____ Judge: _____ Date Terminated: _____

Civil cases are deemed related when *Yes* is answered to any of the following questions:

1.	Is this case related to property included in an earlier numbered suit pending or within one year previously terminated action in this court?	Yes ☐	No ☑
2.	Does this case involve the same issue of fact or grow out of the same transaction as a prior suit pending or within one year previously terminated action in this court?	Yes ☐	No ☑
3.	Does this case involve the validity or infringement of a patent already in suit or any earlier numbered case pending or within one year previously terminated action of this court?	Yes ☐	No ☑
4.	Is this case a second or successive habeas corpus, social security appeal, or pro se civil rights case filed by the same individual?	Yes ☐	No ☑

I certify that, to my knowledge, the within case ☐ is / ☒ is not related to any case now pending or within one year previously terminated action in this court except as noted above.

DATE: 04/08/2019 _____ 76259
Attorney-at-Law / Pro Se Plaintiff *Attorney I.D. # (if applicable)*

CIVIL: (Place a √ in one category only)

A. Federal Question Cases:

- ☐ 1. Indemnity Contract, Marine Contract, and All Other Contracts
- ☐ 2. FELA
- ☐ 3. Jones Act-Personal Injury
- ☐ 4. Antitrust
- ☒ 5. Patent
- ☐ 6. Labor-Management Relations
- ☐ 7. Civil Rights
- ☐ 8. Habeas Corpus
- ☐ 9. Securities Act(s) Cases
- ☐ 10. Social Security Review Cases
- ☐ 11. All other Federal Question Cases
  (Please specify): _____

B. Diversity Jurisdiction Cases:

- ☐ 1. Insurance Contract and Other Contracts
- ☐ 2. Airplane Personal Injury
- ☐ 3. Assault, Defamation
- ☐ 4. Marine Personal Injury
- ☐ 5. Motor Vehicle Personal Injury
- ☐ 6. Other Personal Injury *(Please specify):* _____
- ☐ 7. Products Liability
- ☐ 8. Products Liability – Asbestos
- ☑ 9. All other Diversity Cases
  (Please specify): Other statutory actions

ARBITRATION CERTIFICATION
(The effect of this certification is to remove the case from eligibility for arbitration.)

I, Charles E. Schaffer, counsel of record *or* pro se plaintiff, do hereby certify:

☑ Pursuant to Local Civil Rule 53.2, § 3(c) (2), that to the best of my knowledge and belief, the damages recoverable in this civil action case exceed the sum of $150,000.00 exclusive of interest and costs:

☐ Relief other than monetary damages is sought.

DATE: 04/08/2019 _____ 76259
Attorney-at-Law / Pro Se Plaintiff *Attorney I.D. # (if applicable)*

NOTE: A trial de novo will be a trial by jury only if there has been compliance with F.R.C.P. 38.

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

DESIGNATION FORM

(to be used by counsel or pro se plaintiff to indicate the category of the case for the purpose of assignment to the appropriate calendar)

Address of Plaintiff: 476 Dogwood Court, Altamonte Springs, Florida 32714

Address of Defendant: 701 Market Street, Suite 300, Philadelphia, PA 19106

Place of Accident, Incident or Transaction: Altamonte Springs, Florida

RELATED CASE, IF ANY:

Case Number: _____ Judge: _____ Date Terminated: _____

Civil cases are deemed related when *Yes* is answered to any of the following questions:

1. Is this case related to property included in an earlier numbered suit pending or within one year previously terminated action in this court? Yes ☐ No ☑
2. Does this case involve the same issue of fact or grow out of the same transaction as a prior suit pending or within one year previously terminated action in this court? Yes ☐ No ☑
3. Does this case involve the validity or infringement of a patent already in suit or any earlier numbered case pending or within one year previously terminated action of this court? Yes ☐ No ☑
4. Is this case a second or successive habeas corpus, social security appeal, or pro se civil rights case filed by the same individual? Yes ☐ No ☑

I certify that, to my knowledge, the within case ☐ is / ☑ is not related to any case now pending or within one year previously terminated action in this court except as noted above.

DATE: 04/08/2019 _____ 76259

Attorney-at-Law / Pro Se Plaintiff *Attorney I.D. # (if applicable)*

CIVIL: **(Place a √ in one category only)**

A. Federal Question Cases:

- ☐ 1. Indemnity Contract, Marine Contract, and All Other Contracts
- ☐ 2. FELA
- ☐ 3. Jones Act-Personal Injury
- ☐ 4. Antitrust
- ☐ 5. Patent
- ☐ 6. Labor-Management Relations
- ☐ 7. Civil Rights
- ☐ 8. Habeas Corpus
- ☐ 9. Securities Act(s) Cases
- ☐ 10. Social Security Review Cases
- ☐ 11. All other Federal Question Cases
  (Please specify): _____

B. Diversity Jurisdiction Cases:

- ☐ 1. Insurance Contract and Other Contracts
- ☐ 2. Airplane Personal Injury
- ☐ 3. Assault, Defamation
- ☐ 4. Marine Personal Injury
- ☐ 5. Motor Vehicle Personal Injury
- ☐ 6. Other Personal Injury *(Please specify):* _____
- ☐ 7. Products Liability
- ☐ 8. Products Liability – Asbestos
- ☑ 9. All other Diversity Cases
  (Please specify): Other statutory actions

ARBITRATION CERTIFICATION

(The effect of this certification is to remove the case from eligibility for arbitration.)

I, Charles E. Schaffer, counsel of record *or* pro se plaintiff, do hereby certify:

☑ Pursuant to Local Civil Rule 53.2, § 3(c) (2), that to the best of my knowledge and belief, the damages recoverable in this civil action case exceed the sum of $150,000.00 exclusive of interest and costs:

☐ Relief other than monetary damages is sought.

DATE: 04/08/2019 _____ 76259

Attorney-at-Law / Pro Se Plaintiff *Attorney I.D. # (if applicable)*

NOTE: A trial de novo will be a trial by jury only if there has been compliance with F.R.C.P. 38.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

CASE MANAGEMENT TRACK DESIGNATION FORM

MARIE ABDELMESSIH, individually and on behalf of all others similarly situated,	CIVIL ACTION
v.	
FIVE BELOW, INC.	NO.

In accordance with the Civil Justice Expense and Delay Reduction Plan of this court, counsel for plaintiff shall complete a Case Management Track Designation Form in all civil cases at the time of filing the complaint and serve a copy on all defendants. (See § 1:03 of the plan set forth on the reverse side of this form.) In the event that a defendant does not agree with the plaintiff regarding said designation, that defendant shall, with its first appearance, submit to the clerk of court and serve on the plaintiff and all other parties, a Case Management Track Designation Form specifying the track to which that defendant believes the case should be assigned.

SELECT ONE OF THE FOLLOWING CASE MANAGEMENT TRACKS:

(a) Habeas Corpus – Cases brought under 28 U.S.C. § 2241 through § 2255. ( )

(b) Social Security – Cases requesting review of a decision of the Secretary of Health and Human Services denying plaintiff Social Security Benefits. ( )

(c) Arbitration – Cases required to be designated for arbitration under Local Civil Rule 53.2. ( )

(d) Asbestos – Cases involving claims for personal injury or property damage from exposure to asbestos. ( )

(e) Special Management – Cases that do not fall into tracks (a) through (d) that are commonly referred to as complex and that need special or intense management by the court. (See reverse side of this form for a detailed explanation of special management cases.) (X)

(f) Standard Management – Cases that do not fall into any one of the other tracks. ( )

04/08/2019	Charles E. Schaffer	Plaintiff, Marie Abdelmessih
Date	**Attorney-at-law**	**Attorney for**
(215) 592-1500	(215) 592-4663	cschaffer@lfsblaw.com
Telephone	**FAX Number**	**E-Mail Address**

(Civ. 660) 10/02

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

MARIE ABDELMESSIH, individually and on behalf of all others similarly situated, Plaintiff, v. FIVE BELOW. INC. Defendant.	Case No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Marie Abdelmessih ("Plaintiff"), individually and on behalf of Classes defined below of similarly situated persons, brings this Complaint and alleges the following against Five Below Inc. ("Five Below" or "Defendant"), based upon personal knowledge as to herself, and on information and belief as to all other matters.

NATURE OF THE ACTION

1. This is a putative class action lawsuit brought against Five Below for its failure to properly secure and safeguard the payment card data ("PCD") and personally identifiable information ("PII") (collectively "Customer Data") of its on-line customers and for its failure to provide them timely, accurate and adequate notice that such information had been compromised.

2. On or about February 14, 2019, Five Below publicly revealed that "customers' payment card information, including name, address, credit card number, expiration date, and security code (CVD)" had be compromised, accessed and subsequently stolen by an unauthorized third party ("Data Breach").

3. According the announcement, the Data Breach was first noticed by Five Below on January 11, 2019, and subsequently confirmed on January 17, 2019. Despite this, neither affected consumers, not the public, were informed of the Data Breach for another month, during

which time the unauthorized third parties had unfettered use of the Customer Data.

4. Five Below disregarded the rights of Plaintiff and Class members[1] by: intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected; failing to disclose the material fact that it neither had adequate security practices, nor sufficient safeguards in place to protect the Customer Data with which it was entrusted; failing to take available steps to prevent the Data Breach; failing to monitor and timely detect the Data Breach; and failing to provide Plaintiff and putative class members prompt and accurate notice of the Data Breach.

5. As a result of Defendant's failure to implement and follow standard security procedures Plaintiff's and Class members' Customer Data is in the hands of thieves. As a result of Defendant's basic failures Plaintiff and Class members now face an increased risk of identity theft and will have to spend significant amounts of time and money to protect themselves. Indeed, Plaintiff has already suffered financial harm and adverse credit events as a result of the Data Breach and has expended significant amounts of time in an effort to mitigate its deleterious effects.

6. Plaintiff, on behalf of herself and classes of similarly situated individuals, seeks to remedy the harms suffered as a result of the Data Breach and to ensure that the Customer Data, which remains in the possession of Defendant, is protected from further breaches.

7. Defendant's conduct gives rise to claims for negligence, negligence per se, breach of implied contract, breach of fiduciary duty, breach of confidence, breach of privacy and is in violation of Florida's Deceptive and Unfair Trade Practices Act. Plaintiff, individually, and on behalf of those similarly situated, seeks damages, equitable relief, injunctive relief, restitution,

[1] See, Infra at ¶66.

and all other remedies this Court deems proper.

JURISDICTION AND VENUE

8. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act 28 U.S.C. § 1332(d) ("CAFA"), as the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs, there are more than 100 Class members, and at least one class Member is a citizen of a state different from Defendant.

9. This Court has personal jurisdiction over Defendant because Five Below is incorporated in Pennsylvania, regularly conducts business in this District, and maintains its principal place of business in this District at 701 Market Street, Suite 300, Philadelphia, PA 19106.

10. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because the Defendant's principal places of business is in this District and a substantial part of the events or omissions giving rise to this action, particularly decisions related to data security and the acts which lead to the Data Breach, occurred in this District.

PARTIES

11. Plaintiff Marie Abdelmessih is a citizen and resident of Altamonte Springs, Florida. Between November 13, 2018 and January 11, 2019, Ms. Abdelmessih made a purchase through the Five Below website located at www.fivebelow.com ("Website"). As a prerequisite for conducting the transaction, Ms. Abdelmessih was required to, and did, provide Five Below with sensitive personal information including her name, address, credit card number, expiration date and CVV.

12. As a direct result of the Data Breach, Ms. Abdelmessih's Customer Data was compromised, and thereafter fraudulently used by third parties. The fraudulent activity included,

but was not limited to: (a) hijacking Ms. Abdelmessih cell phone number in an effort to falsify two-factor authentication required by some of her accounts; (b) multiple attempts to fraudulently transfer money from her account via Western Union; (c) transfer of $10,000 from her savings account to her checking account in an effort to transfer the sum out of the account. As a result, Ms. Abdelmessih spent many hours of her time in an effort to stop the fraud from continuing and to prevent it from reoccurring. Among other things, Ms. Abdelmessih contacted her bank's fraud department, filed a police report, spoke with the Publix manager where the fraudulent Western Union transaction was attempted and contacted all three major credit bureaus to freeze her credit . In addition, Ms. Abdelmessih had to physically visit her bank to open new accounts, reset passwords, and obtain a new Visa card.

13. Ms. Abdelmessih continues to spend her valuable time to protect the integrity of her finances and credit – time which she would not have had to expend but for the Data Breach.

14. Defendant Five Below is a publicly traded company with its principal place of business located at 701 Market Street, Suite 300 , Philadelphia, Pa. 19106 and is dedicated to retail sales of teen and pre-teen merchandise under five dollars. It claims to be "one of the fastest growing retailers in the world" with 750 stores across the United States and a robust on-line presence via its website www.fivebelow.com.

FACTUAL ALLEGATIONS

A. The Five Below Data Breach

15. On or about January 11, 2018, Defendant "learned of suspicious activity" on its website. On January 17, 2019, an investigation concluded that an unauthorized third party gained access to Five Below Customer Data including, names, addresses, credit card numbers, credit card expiration dates and security codes. Customers who transacted on Five Below's website

from November 13, 2018 to January 11, 2019 were affected.[2]

16. On February 14, 2019, approximately a full month after discovering the Data Breach, Defendant publicly announced that its Customer Data had been exposed and compromised. The Notice of Data Breach was publicly disseminated to Attorney General Offices across the United Sates and stated as follows:

> **Notice of Data Breach**
>
> Five Below, Inc. ("Five Below") understands the importance of protecting the payment card information of our customers. We are writing to inform you of a recent incident that may have involved that information. This letter explains the incident, measures we have taken, and steps you can take in response.
>
> **What Happened?**
>
> Our security team learned of suspicious activity on our website on January 11, 2019. We immediately began an investigation with the assistance of a leading computer security firm. On January 17, 2019, the investigation identified the potential for unauthorized access to payment card data. Purchases made in our stores were not affected by this incident.
>
> **What Information Was Involved?**
>
> Findings from the investigation suggest that certain of our customers' payment card information, including name, address, payment card number, expiration date, and card security code (CVV), may have been obtained by an unauthorized third party. We believe the incident only involved customers who entered information on our website's checkout page between November 13, 2018 and January 11, 2019. We are notifying you because you placed or attempted an order on www.fivebelow.com during that time using a payment card ending in <<Last 4 Card #>>.
>
> **What We Are Doing.**
>
> We take the security of our customers' personal information very seriously. To help prevent a similar incident from occurring in the future we have further enhanced the security measures for our website. In addition, we are working with the payment card networks so that banks that issue payment cards can be made aware.
>
> **What You Can Do.**

[2] Notice of Data Breach attached hereto as Exhibit A.

> We encourage you to closely review your payment card statements for any unauthorized charges. You should immediately report any such charges to the bank that issued your card because payment card network rules generally provide that cardholders are not responsible for unauthorized charges that are timely reported. The phone number to call is usually on the back of your payment card.
>
> As a precaution, we have secured the services of Experian to offer you a complimentary one-year membership of Experian's® IdentityWorks. This product provides you with identity detection and resolution of identity theft services. For more information on IdentityWorks, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you can take to protect yourself, please see the pages that follow this letter.[3]
>
> **For More Information.**
>
> If you have any questions, please call 877-363-7794, Monday through Friday, from 9:00 a.m. to 9:00 p.m. Eastern Time.

17. On or about February 14, 2019, Plaintiff received a letter from Five Below reflecting the same, and stating in relevant part:

> Five Below, Inc. ("Five Below") understands the importance of protecting the payment card information of our customers. We are writing to inform you of the recent incident that may have involved that information. This letter explains the incident, measures we have taken, and steps you can take in response.
>
> Our security team learned of suspicious activity on our website on January 11, 2019. We immediately began an investigation with the assistance of the leading computer security firm on January 17, 2019, investigation identified the potential for unauthorized access to payment card data. Findings from the investigation suggest that certain of our customers payment card information, including name, address, payment card number, expiration date, and card security code (CBV), may have been obtained by an unauthorized third party. We believe the incident only involved customers who entered information on our websites checkout page between November 13, 2018 and January 11, 2019. We are notifying you because you placed or attempted in order on www.fivebelow.com during that time using a payment card ending

[3] See e.g., https://www.oag.ca.gov/system/files/FB_CA_Notice_0.pdf (last visited April 2, 2019)

> in XXXX. Purchases made in our stores were not affected by this incident.
>
> We encourage you to closely review your payment card statements for any unauthorized charges. You should immediately report any such charges to the bank that issued your card because payment card network rules generally provide that cardholders are not responsible for unauthorized charges that are timely reported. The phone number to call is usually on the back of your payment card.
>
> As a precaution, we have secured the services of Experian to offer you a complimentary one-year membership of Experian's IdentityWorks. This product provides you with identity detection and resolution of identity theft services. For more information on IdentityWorks, including instructions on how to activate your complementary one-year membership, as well as some additional steps you can take to protect yourself, please see the pages that follow this letter.
>
> We take the security of our customers personal information very seriously. To help prevent a similar incident from occurring in the future we further enhance the security measures for our website. In addition, we are working with the payment card networks so that banks that issue payment cards can be made aware.[4]

B. Security Breaches Lead to Identity Theft

18. Customer Data has become a valuable commodity among computer hackers. Once obtained, it is quickly sold on the black market where it can often be re-traded among miscreants for years.[5] Customer Data is particularly valuable to identity thieves who can use victims' personal data to open new financial accounts, take out loans, incur charges, or clone ATM, debit, and credit cards. As reported by the Identity Theft Resource Center, there were 1,579 data breaches in 2017, representing a 44.7 percent increase over the then-record high

[4] Five Below letter to Marie Abdelmessih, February 14, 2019, attached hereto as Exhibit B.

[5] *Guide for Assisting Identity Theft Victims*, FTC (Sep. 2013), *available at*: https://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf (the "FTC Guide").

figures reported for 2016.[6]

19. Professionals tasked with trying to stop fraud and other misuse know that Customer Data has real monetary value as evidenced by criminals' relentless efforts to obtain this data.[7] Experian reports that a stolen credit or debit card number can sell for $5-110 on the dark web[8] and a complete set of bank account credentials can fetch a thousand dollars or more (depending on the associated credit score or balance available to criminals).[9]

DEFENDANT'S PRIVACY POLICIES AND PROMISES TO KEEP CUSTOMER DATA CONFIDENTIAL

20. As a condition of transacting on the Five Below Website, Defendant required its customers to provide them with certain personal information including their names, addresses, and credit card information.. This information was subsequently maintained by Five Below in the ordinary course of its business.

21. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and the Class members' PII and PCD, Defendant assumed legal and equitable duties to those individuals and knew or should have known that it was responsible for protecting Plaintiff's and Class members' PII and PCD from disclosure.

22. At all relevant times, Plaintiff and the Class members have taken reasonable steps

---

[6] *2017 Annual Data Breach Year-End Review,* https://www.idtheftcenter.org/2017-data-breaches, (last visited January 23, 2019).

[7] *Data Breaches Rise as Cybercriminals Continue to Outwit IT, CIO Magazine,* https://www.cio.com/article/2686167/data-breach/data-breaches-rise-as-cybercriminals-continue-to-outwit-it.html (last visited January 23, 2019).

[8] *Here's How Much Your Personal Information Is Selling for on the Dark Web* https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/, (last visited January 23, 2019).

[9] *Here's How Much Thieves Make By Selling Your Personal Data Online, Business Insider,* http://www.businessinsider.com/heres-how-much-your-personal-data-costs-on-the-dark-web-2015-5, May 27, 2015.

to maintain the confidentiality of their PII and PCD. Plaintiff and the Class members, as current and former customers, relied on Defendant to keep their PII and PCD confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. ("We take reasonable measures to help protect information about you from loss, theft, misuse and unauthorized access, disclosure, alteration and destruction.")[10]

23. Five Below is acutely aware of its legal obligations to maintain the privacy and sanctity of Customer Data with which it is entrusted. It is also acutely aware of the ramifications for the failure to do so. Five Below makes this point clear in its Annual Report filed on Form 10-K which warns its investors as follows:

> We are subject to customer payment related risks that could increase operating costs or exposure to fraud or theft, subject us to potential liability and potentially disrupt our business.
>
> We accept payments using a variety of methods, including cash, credit and debit cards and gift cards. Acceptance of these payment options subjects us to rules, regulations, contractual obligations and compliance requirements, including payment network rules and operating guidelines, data security standards and certification requirements, and rules governing electronic funds transfers. Any inability to comply with such requirements may subject us to increased risk of liability fraudulent transactions and may adversely affect our business and operating results.
>
> For certain payment methods, including credit and debit cards, we pay interchange and other fees, which may increase over time and raise our operating costs. We rely on third parties to provide payment processing services, including the processing of credit cards, debit cards, and other forms of electronic payment. If these companies become unable to provide these services to us, or if their systems are compromised, it could potentially disrupt our business. The payment methods that we offer also subject us to potential fraud and theft by criminals, were becoming increasingly more sophisticated, seeking to obtain unauthorized access to or exploit weaknesses that may exist in the payment systems. If we fail to comply with applicable rules or

[10] See, Five Below Privacy Policy, available at https://www.fivebelow.com/privacy-policy (last visited April 2, 2019)

> requirements for the payment methods we accept, or if payment related data is compromised due to a breach or misuse of data, we may be liable for costs incurred by payment card issuing banks and other third parties or subject to fines and higher transaction fees, or our ability to accept or facilitate certain types of payments may be impaired. In addition, our customers can lose confidence in certain payment types, which may result in a shift to other payment types or potential changes to our payment systems that may result in higher costs. As a result, our business and operating results could be adversely affected.[11]

24. The same sentiment was echoed five years earlier in the Company's Prospectus statement to investors in 2012, and has been repeated in similar form every year since.

> ***If we are unable to secure our customers' confidential or credit card information, or other private data relating to our employees or our Company, we could be subject to negative publicity, costly government enforcement actions or private litigation, which could damage our business reputation and adversely affect our financial results.***
>
> The protection of our customer, employee and company data is critical to us. We have procedures and technology in place to safeguard our customers' debit and credit card, and other personal information, our employees' private data and company records and intellectual property. However, if we experience a data security breach of any kind, we could be exposed to negative publicity, government enforcement actions, private litigation or costly response measures. In addition, our reputation within the business community and with our customers may be affected, which could result in our customers discontinuing the use of debit or credit cards in our stores, or not shopping in our stores altogether. This could cause us to lose market share to our competitors and could have an adverse effect on our financial results.[12]

25. Five Below reassured its customers and investors that it was aware of its legal obligations to protect confidential customer information; that it has sufficient procedures and

---

[11] 2017 Annual Report available at http://investor.fivebelow.com/financial-information/annual-reports-and-proxy-statements/default.aspx (last visited April 2, 2019)

[12] Form S-1 Registration Statement, April 17, 2012. Available at http://d18rn0p25nwr6d.cloudfront.net/CIK-0001177609/089f844b-363e-45d3-9f14-8f3bb66aa50f.pdf (last visited April 2, 2019).

policies in place to do so; and that a security breach would be costly to the company and its customers.

26. Despite espousing the importance of securing its customer data year after year in sworn public statements, Five Below failed to implement or maintain the most basic procedures and protocols necessary to achieve this goal.

27. Asa result of this failure, in September 2018, Five Below publicly revealed that the very website at issue here was subject to an earlier data breach that exposed Customer Data in August and September 2018. In a near verbatim announcement to the Data Breach at issue here, Defendant stated

> Five Below Inc. understands the importance of protecting the payment card information of our customers. We are writing to inform you of the recent incident may have involved that information. This letter explains the incident, measures we have taken, and steps you can take in response.
>
> On August 28, 2018, our security team observed suspicious activity on our website. We immediately began an investigation with the assistance of a leading computer security firm on September 10, 2018, the investigation identified the potential for unauthorized access to payment card data. Findings from the investigation suggest that certain of our customers order information and payment card information, including name, address, payment card number, expiration date, and card security code (CVV), may have been obtained by an unauthorized third party. We believe the incident only involved customers who placed or attempted to place orders on our website August 14, 2018 and August 28, 2018 or between September 18, 2018 and September 19, 2018. We are notifying you because you placed or attempted an order on www.fivebelow.com during those time periods using a payment card ending in _____. Purchases made in our stores were not affected by the since.
>
> We encourage you to closely review your payment card statements for any unauthorized charges. You should immediately report any such charges to the bank that issued your car's payment card network rules generally provide that cardholders are not responsible for unauthorized charges that are timely reported. The phone number to call is usually on the back of your payment card.
>
> Today, we have no information that any of your personal information was misused in any way. As a precaution, we've secured the services of Experian

> offer you a complimentary one-year membership of experience identity works. This product provides you with identity detection and resolution of identity theft services. For more information on identity works, including instructions on how to activate a complimentary one-year membership, as well as some additional steps you can take to protect yourself, we see the pages that follow this letter.
>
> We take the security of our customers personal information very seriously. To help prevent a similar incident from occurring in the future we have further enhanced the security measures for our website. In addition we are working with the payment card networks so that banks that issue payment cards can be made aware.[13]

28. Five Below reiterated that they "take the security of our customers personal information very seriously" and that "[t]o help prevent a similar incident from occurring in the future we have further enhanced the security measures for our website." The veracity of these representations, however, were completely belied by the fact that less than two months later, Five Below was subject to a near identical data breach.

FIVE BELOW FAILED TO COMPLY WITH INDUSTRY STANDARDS

29. The major payment card industry brands typically set forth specific security measures in their Card Operating Regulations which are binding on merchants such as Five Below and require them to: (1) protect cardholder data and prevent its unauthorized disclosure; (2) store data, even in encrypted form, no longer than necessary to process the transaction; and (3) comply with all industry standards.

30. The Payment Card Industry Data Security Standard ("PCI DSS") is an information security standard for organizations that handle branded credit cards. The standard

[13] https://ago.vermont.gov/blog/2018/10/05/five-below-inc-notice-of-data-breach-to-consumers/ (last visited on April 2, 2019).

was created to increase controls around cardholder data to reduce credit card fraud.[14] Compliance with PCI DSS is mandated by credit card companies.

31. The PCI DSS "was developed to encourage and enhance cardholder data security" by providing "a baseline of technical and operational requirements designed to protect account data."[15] PCI DSS sets the minimum level of what must be done, not the maximum.

32. PCI DSS requires the following: [16]

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

33. Among other things, PCI DSS required Five Below to properly secure and protect payment card data; not store cardholder data beyond the time necessary to authorize a transaction; maintain up-to-date antivirus software and a proper firewall; protect systems against malware; regularly test security systems; establish a process to identify and timely fix security vulnerabilities; and encrypt payment card data at the point of sale.

34. Although it was well aware of its data security obligations, Five Below's

[14] *Payment Card Industry Data Security Standard* available at https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss (last visited January 23, 2019).
[15] *Id.*
[16] *Id.*

treatment of PCD and PII fell far short of its legal obligations to protect Customer Data. Five Below failed to ensure that access to its data systems was reasonably safeguarded, failed to acknowledge and act upon industry warnings and failed to use proper security systems to detect and deter the type of attack that occurred and is at issue here. Cumulatively, its failures resulted in the Data Breach.

FIVE BELOW FAILED TO COMPLY WITH FTC REQUIREMENTS

35. Federal and State governments have likewise established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guidelines for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[17]

36. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[18] The guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large

[17] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited January 23, 2019).

[18] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited January 23, 2019).

amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

37. Embracing standard industry practices, the FTC recommends that companies not maintain cardholder information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[19]

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

39. Five Below's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

40. In this case, Five Below was at all times fully aware of its obligation to protect the financial data of Five Below's customers because of its participation in payment card processing networks. Five Below was also aware of the significant repercussions if it failed to do so because Five Below collected payment card data from tens of thousands of customers daily and they knew that this data, if hacked, would result in injury to consumers, including Plaintiff and Class members.

---

[19] FTC, *Start With Security*, *supra* note 17.

41. Despite understanding the consequences of inadequate data security, Five Below failed to comply with PCI DSS requirements, FTC Guidelines and standard industry practices designed to ensure the integrity of PII and PCD.

FIVE BELOW'S FAILURE TO TIMELY WARN OF THE DATA BREACH CAUSED ADDIITONAL HARM

42. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[20] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[21]

43. Personal identifying information is a valuable commodity to identity thieves. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[22]

44. Identity thieves can use personal information, such as that of Plaintiff and Class members, which Five Below failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

45. Compounding Five Below's failure to protect Customer Data, was the fact that it

[20] 17 C.F.R § 248.201 (2013).
[21] *Id.*
[22] Federal Trade Commission, *Warning Signs of Identity Theft*, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited January 23, 2019).

failed to timely inform affected customers that their PCD and PII had been illegally exposed. A 2016 survey of 5,028 consumers found "[t]he quicker a financial institution, credit card issuer, wireless carrier or other service provider is notified that fraud has occurred on an account, the sooner these organizations can act to limit the damage. Early notification can also help limit the liability of a victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act."[23]

46. As a result of Five Below's delay in notifying consumers of the Data Breach, the risk of fraud for Plaintiff and Class members has been driven even higher.

HARM CAUSED BY THE DATA BREACH IS ONGOING

47. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the past six years.[24]

48. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[25]

49. An independent financial services industry research study conducted for

---

[23] *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, February 1, 2017, available at https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new (last visited January 23, 2019).

[24] *See* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited January 23, 2019).

[25] Victims of Identity Theft, 2014 (Sept. 2015) available at: http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited January 23, 2019).

BillGuard – a private enterprise that automates the consumer task of finding unauthorized transactions that might otherwise go undetected–calculated the average per-consumer cost of all unauthorized transactions at roughly US $215 per cardholder incurring these charges[26], some portion of which could go undetected and thus must be paid entirely out-of-pocket by consumer victims of account or identity misuse.

50. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII or PCD is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[27]

51. Thus, Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and the Class are incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred by them and the resulting loss of use of their credit and access to funds, regardless of whether such charges are ultimately reimbursed by banks and credit card companies.

PLAINTIFF AND THE CLASSES SUFFERED DAMAGES

52. The Customer Data belonging to Plaintiff and Class members is private and

---

[26] Hadley Malcom, *Consumers rack up $14.3 billion in gray charges, research study commissioned for Billguard by Aite Research, USA Today* (July 25, 2013), available at: **https://www.usatoday.com/story/money/personalfinance/2013/07/25/consumers-unwanted-charges-in-billions/2568645/** (last visited January 23, 2019).

[27] GAO, Report to Congressional Requesters, at 29 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (last visited January 23, 2019).

sensitive in nature and was left inadequately protected by the Defendant. Defendant did not obtain Plaintiff's or Class members' consent to disclose their Customer Data to any other person as required by applicable law and industry standards.

53. The Data Breach was a direct and proximate result of Defendant's failure to properly safeguard and protect Plaintiff's and Class members' Customer Data from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Defendant's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' Customer Data to protect against reasonably foreseeable threats to the security or integrity of such information.

54. According to year end data breach statistics compiled by the Identity Theft Resource Center, of the 1,244 breaches reported in 2018, 571 were attributed to businesses, making them the most targeted group by data hackers.[28]

55. Defendant was acutely aware of the dangers of data breaches and that customer retail data was a particularly high value target. Defendant had the resources necessary to prevent such a breach yet neglected to adequately invest in data security. Defendant designed and implemented their policies and procedures regarding the security of Customer Data. These policies and procedures failed to adhere to reasonable and best industry practices in safeguarding protected PII and PCD.

56. Affected individuals face a real, concrete, and actual risk of harm and future identity theft as the PCD and PII contained confidential biographical information. Had

[28] https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf (last visited April 2, 2019)

Defendant remedied the deficiencies in its data security systems, adopted security measures recommended by experts in the field, Defendant would have prevented the intrusion and, ultimately, the theft of PCD and PII belonging to Five Below customers.

57. As a direct and proximate result of Defendant's wrongful actions and inaction, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured.

58. Notwithstanding the seriousness of the Data Breach, the Defendant have not offered to provide Plaintiff nor Class members any meaningful assistance or compensation for the costs and burdens—current and future—associated with the unauthorized exposure of their PII.

59. Other than providing generic advice on what to do when one's PII has been exposed in a data breaches, and a free credit report, which is already available to every U.S. consumer, Defendant frugally offered one year free credit monitoring with Experian's IdentityWorks.[29]

60. This offer is wholly insufficient to protect the Plaintiff and Class members from the threats they face, particularly in light of the nature of the PII that was stolen.

[29] Exhibit A.

61. Moreover, rather than automatically enrolling Plaintiff and Class members in credit monitoring services upon discovery of the breach. Defendant' inadequate credit monitoring offer places the onus on Plaintiff and Class members, rather than Defendant, to investigate and protect themselves from Defendant' tortious acts that resulted in the Data Breach.

62. Furthermore, a free credit report and the ability to freeze their accounts is not only a right that every citizen enjoys, it is grossly inadequate to protect the Plaintiff and Class members from the threats they face resulting from the PII that was exposed. Although credit monitoring can help detect fraud after it has already occurred, it has very little value as a preventive measure and does nothing to prevent fraudulent tax filings. As noted by security expert Brian Krebs, "although [credit monitoring] services may alert you when someone opens or attempts to open a new line of credit in your name, most will do little — if anything — to block that activity. My take: If you're being offered free monitoring, it probably can't hurt to sign up, but you shouldn't expect the service to stop identity thieves from ruining your credit."[30]

63. As a result of the Defendant' failures to prevent the Data Breach, Plaintiff and Class members have suffered and will continue to suffer damages. They have suffered, or are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their PCD/PII;

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

c. Lost opportunity costs and lost wages associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future

[30] *Krebs on Security*, March 19, 2014, https://krebsonsecurity.com/2014/03/are-credit-monitoring-services-worth-it/ (last visited on April 2, 2019)

consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

d. The continued risk to their PCD/PII, which remains in the possession of the Defendant and is subject to further breaches so long as the Defendant fails to undertake appropriate measures to protect the PCD/PII in their possession; and

e. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of Plaintiff's and Class members' lives.

64. Additionally, Defendant continues to hold the PCD/PII of its customers. Particularly, because Defendant has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiff and Class members have an undeniable interest in ensuring that their PCD/PII is secure, remains secure, and is not subject to further theft.

65. Defendant disregarded the rights of Plaintiff and Class members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that their PCD/PII was safeguarded; failing to take available steps to prevent an unauthorized disclosure of data; and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PCD/PII of Plaintiff and Class members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class members have a continuing interest in ensuring that their information is and remains safe. In addition to damages, Plaintiff and Class members are entitled to injunctive and other equitable relief.

CLASS ACTION ALLEGATIONS

66. Plaintiff brings this suit as a class action on behalf of herself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), (b)(3) and (c)(4) of the Federal Rules of Civil Procedure. Plaintiff seeks certification of a Nationwide and Florida Sub classes defined as follows:

> **All persons residing in the United States who entered credit or debit card information at Five Below's website www.fivebelow.com during the period of the Data Breach (the "Nationwide Class").**
>
> **All persons residing in the state of Florida who entered credit or debit card information at Five Below's website www.fivebelow.com during the period of the Data Breach (the "Florida Sub Class").**

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

68. Numerosity. Fed. R. Civ. P. 23(a)(1). The Class members are so numerous that joinder of all Members is impractical. While the exact number of Class members is unknown to Plaintiff at this time. The exact number is generally ascertainable by appropriate discovery as Defendant have knowledge of the customers whose PCD/PII was breached.

69. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether and to what extent Defendant had a duty to protect the PCD/PII of Class members;

b. Whether Defendant was negligent in collecting and storing Plaintiff's and Class

members' PCD/PII;

c. Whether Defendant had a duty not to disclose the PCD/PII of Class members to unauthorized third parties;

d. Whether Defendant took reasonable steps and measures to safeguard Plaintiff's and Class members' PCD/PII;

e. Whether Defendant failed to adequately safeguard the PCD/PII of Class members;

f. Whether Defendant breached its duty to exercise reasonable care in handling Plaintiff's and Class members' PCD/PII;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether implied contracts existed between Five Below, on the one hand, and Plaintiff and Class members on the other;

i. Whether Defendant had respective duties not to use the PCD/PII of Class members for non-business purposes;

j. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class members that their PCD/PII had been compromised;

k. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PCD/PII of Class members;

l. Whether Class members are entitled to actual, damages, statutory damages, and/or punitive damages as a result of Defendant's wrongful conduct;

m. Whether Plaintiff and Class members are entitled to restitution as a result of Defendant' wrongful conduct; and,

n. Whether Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

70. Typicality. Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of those of other Class members because Plaintiff's PCD/PII, like that of every other Class member, was disclosed by Defendant. Plaintiff's claims are typical of those of the other Class members because, *inter alia*, all Members of the Class were injured through the common misconduct of Defendant. Plaintiff is advancing the same claims and legal theories on behalf of himself and all other Class members, and there are no defenses that are unique to Plaintiff. Plaintiff's claims and those of Class members arise from the same operative facts and are based on the same legal theories.

71. Policies Generally Applicable to the Class. This class action is also appropriate for certification because Defendant have acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class members, and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

72. Adequacy of Representation. Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the Class in that he has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages he has suffered are typical of other Class members. Plaintiff has retained

counsel experienced in complex consumer class action litigation, and Plaintiff intends to prosecute this action vigorously.

73. Superiority of Class Action. Fed. R. Civ. P. 23(b)(3). The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

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

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

76. Adequate notice can be given to Class members directly using information maintained in Defendant' records.

77. Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

78. Unless a Class-wide injunction is issued, Defendant may continue in their failure to properly secure the PCD/PII of Class members, Defendant may continue to refuse to provide proper notification to Class members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

79. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, using, and safeguarding their PCD/PII;

b. Whether Defendant breached a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, using, and safeguarding their PCD/PII;

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

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

e. Whether Five Below breached the implied contract;

f. Whether Defendant timely, adequately, and accurately informed Class members that their PCD/PII had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PCD/PII of Class members; and,

i. Whether Class members are entitled to actual damages, statutory damages, injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of the Nationwide and Florida Sub Classes)

80. Plaintiff restates and realleges paragraphs 1 through 70 above as if fully set forth herein.

81. As a condition of utilizing Five Below's services customers were obligated to provide Defendant with certain PCD/PII, including their names, addresses, credit card numbers, credit card expiration dates at CVV

82. Plaintiff and the Class members entrusted their PCD/PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their

PCD/PII for business purposes only, and/or not disclose their PCD/PII to unauthorized third parties.

83. Defendant have full knowledge of the sensitivity of the PCD/PII and the types of harm that Plaintiff and Class members could and would suffer if the PCD/PII were wrongfully disclosed.

84. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of their customers' PCD/PII involved an unreasonable risk of harm to Plaintiff and Class members, even if the harm occurred through the criminal acts of a third party.

85. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant' security protocols to ensure that Plaintiff and Class members' information in Defendant' possession was adequately secured and protected, and that employees tasked with maintaining such information were adequately trained on security measures regarding the security of customers' personal and medical information.

86. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class members' PCD/PII.

87. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class members was reasonably foreseeable, particularly in light of Defendant' inadequate information security practices.

88. Plaintiff and the Class members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew of should have known of the

inherent risks in collecting and storing the PCD/PII of Plaintiff and the Class, the critical importance of providing adequate security of that PCD/PII, and that they had inadequate employee training and education and IT security protocols in place to secure the PCD/PII of Plaintiff and the Class.

89. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and Class members. Defendant' misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant' misconduct also included their decisions not to comply with industry standards for the safekeeping of the PCD/PII of Plaintiff and Class members.

90. Plaintiff and the Class members had no ability to protect their PCD/PII that was in Defendant's possession.

91. Defendant was in a position to protect against the harm suffered by Plaintiff and Class members as a result of the Data Breach.

92. Defendant had and continues to have a duty to adequately disclose that the PCD/PII of Plaintiff and Class members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of information that were compromised and when. Such notice was necessary to allow Plaintiff and the Class members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PCD/PII by third parties.

93. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PCD/PII of Plaintiff and Class members.

94. Defendant has admitted that the PCD/PII of Plaintiff and Class members was wrongfully disclosed to unauthorized third persons as a result of the Data Breach.

95. Defendant, through their actions and/or omissions, unlawfully breached their duties to Plaintiff and Class members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PCD/PII of Plaintiff and Class members during the time the PCD/PII was within Defendant's possession or control.

96. Defendant improperly and inadequately safeguarded the PCD/PII of Plaintiff and Class members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

97. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect customers' PCD/PII in the face of increased risk of theft.

98. Defendant, through its actions and/or omissions, unlawfully breached their duty to Plaintiff and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of their customers' PCD/PII.

99. Defendant, through its actions and/or omissions, unlawfully breached their duty to adequately and timely disclose to Plaintiff and Class members the existence and scope of the Data Breach.

100. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class members, the PCD/PII of Plaintiff and Class members would not have been compromised.

101. There is a close causal connection between Defendant's failure to implement security measures to protect the PCD/PII of current and former customers, and the harm suffered or risk of imminent harm suffered by Plaintiff and the Class. Plaintiff's and Class members' PCD/PII was stolen and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PCD/PII by adopting, implementing, and maintaining appropriate security measures and encryption.

102. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PCD/PII is used; (iii) the compromise, publication, and/or theft of their PCD/PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PCD/PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PCD/PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the PCD/PII of customers in their continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PCD/PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class members; and (ix) the diminished value of Defendant's goods and services they received.

103. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

SECOND CAUSE OF ACTION
Invasion of Privacy
(On Behalf of the Nationwide and Florida Sub Classes)

104. Plaintiff restates and realleges paragraphs 1 through 70 above as if fully set forth herein.

105. Plaintiff and Class members had a legitimate expectation of privacy to their PCD/PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

106. Defendant owed a duty to Five Below customers, including Plaintiff and Class members, to keep their PCD/PII confidential.

107. Defendant failed to protect and released to unknown and unauthorized third parties data containing the PCD/PII of Plaintiff and Class members.

108. Defendant allowed unauthorized and unknown third parties access to and examination of the PCD/PII of Plaintiff and Class members, by way of Defendant's failure to protect the PCD/PII in its databases.

109. The unauthorized release to, custody of, and examination by unauthorized third parties of the PCD/PII of Plaintiff and Class members is highly offensive to a reasonable person.

110. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class members disclosed their PCD/PII to Defendant as part of their use of Defendant's services, but privately with an intention that the PCD/PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and Class members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

111. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff and Class members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

112. Defendant acted with a knowing state of mind when they permitted the Data Breach because they were with actual knowledge that their information security practices were inadequate and insufficient.

113. As a proximate result of the above acts and omissions of Defendant, the PCD/PII of Plaintiff and Class members was disclosed to third parties without authorization, causing Plaintiff and Class members to suffer damages.

114. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class members in that the PCD/PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons. Plaintiff and Class members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of the Nationwide and Florida Sub Classes)

115. Plaintiff restates and realleges paragraphs 1 through 70 above as if fully set forth herein.

116. Plaintiff and Class members were required to provide their PCD/PII, including their names, addresses, credit card numbers, expirations dates and security codes to Defendant as

a condition of purchasing products through Defendant's Website.

117. Plaintiff and Class members paid money to Five Below in exchange for goods and services, as well as Defendant's promises to protect their PCD/PII from unauthorized disclosure.

118. In their written privacy policy and sworn public statements, Defendant expressly promised Plaintiff and Class members that Defendant would only disclose PCD/PII under certain circumstances, none of which relate to the Data Breach.

119. Implicit in the agreement between the Defendant and its customers, including Plaintiff and Class members, was Defendant's obligation to use Customer Data for business purposes only, take reasonable steps to secure and safeguard Customer Data, and not make unauthorized disclosures of such data to unauthorized third parties.

120. Further, implicit in the agreement, Defendant was obligated to provide Plaintiff and Class members with prompt and sufficient notice of any and all unauthorized access and/or theft of their protected PCD/PII.

121. Without such implied contracts, Plaintiff and Class members would not have provided their PCD/PII to Defendant.

122. Defendant had an implied duty to reasonably safeguard and protect the PCD/PII of Plaintiff and Class members from unauthorized disclosure or uses.

123. Additionally, Defendant implicitly promised to retain this PCD/PII only under conditions that kept such information secure and confidential.

124. Plaintiff and Class members fully performed their obligations under the implied contract with Defendant; however, Defendant did not.

125. Defendant breached the implied contracts with Plaintiff and Class members by failing to reasonably safeguard and protect Plaintiff and Class members' PCD/PII, which was

compromised as a result of the Data Breach.

126. Defendant further breached the implied contracts with Plaintiff and Class members by otherwise failing to safeguard Plaintiff's and Class members' PCD/PII.

127. Defendant's failures to meet these promises constitute breaches of the implied contracts.

128. Because Defendant allowed unauthorized access to Plaintiff's and Class members' PCD/PII and failed to safeguard the PCD/PII, Defendant breached their contracts with Plaintiff and Class members.

129. A meeting of the minds occurred, as Plaintiff and Class members agreed, *inter alia*, to provide accurate and complete PCD/PII and to pay Defendant in exchange for Defendant's agreement to, *inter alia*, protect their PCD/PII.

130. Defendant breached their contracts by not meeting the minimum level of protection of Plaintiff's and Class members' protected PCD/PII.

131. Furthermore, the failure to meet their confidentiality and privacy obligations resulted in Defendant providing goods and services to Plaintiff and Class members that were of a diminished value.

132. As a direct and proximate result of Defendant's breach of their implied contracts with Plaintiff and Class members, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PCD/PII is used; (iii) the compromise, publication, and/or theft of their PCD/PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PCD/PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and

future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PCD/PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PCD/PII of customers in their continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PCD/PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class members; and (ix) the diminished value of Defendant's goods and services they received.

133. As a direct and proximate result of Defendant's breach of their implied contracts with Plaintiff and Class members, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

FOURTH CAUSE OF ACTION
Negligence Per Se
(On Behalf of the Nationwide and Florida Sub Classes)

134. Plaintiff restates and realleges paragraphs 1 through 70 above as if fully set forth herein.

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

136. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PCD/PII and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PCD/PII they obtained and stored, and the foreseeable consequences of a Data Breach for companies of Defendant's magnitude, including, specifically, the immense damages that would result to Plaintiff and Class members.

137. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se*.

138. Plaintiff and Class members are within the class of persons that the FTC Act was intended to protect.

139. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class members.

140. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PCD/PII is used; (iii) the compromise, publication, and/or theft of their PCD/PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PCD/PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes

on credit reports; (vii) the continued risk to their PCD/PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the PCD/PII of customers in their continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PCD/PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class members; and (ix) the diminished value of Defendant's goods and services they received.

FIFTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of the Nationwide and Florida Sub Classes)

141. Plaintiff restates and realleges paragraphs 1 through 70 above as if fully set forth herein.

142. In light of the special relationship between Defendant and their customers, whereby Defendant became guarantors of Plaintiff's and Class members' highly sensitive, confidential, personal, financial information, and other PCD/PII, Defendant were fiduciaries, created by their undertaking and guarantorship of the PCD/PII, to act primarily for the benefit of their customers, including Plaintiff and Class members, for: 1) the safeguarding of Plaintiff and Class members' PCD/PII; 2) timely notify Plaintiff and Class members' of a data breach or disclosure; and 3) maintain complete and accurate records of what and where Defendant's customers' information was and is stored.

143. Defendant had a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of their customer relationship, in particular to keep secure the PCD/PII of their customers.

144. Defendant breached their fiduciary duties to Plaintiff and Class members by failing to diligently investigate the Data Breach to determine the number of Members affected in a reasonable and practicable period of time.

145. Defendant breached their fiduciary duties to Plaintiff and Class members by failing to protect the databases containing Plaintiff's and Class members' PCD/PII.

146. Defendant breached their fiduciary duties to Plaintiff and Class members by failing to timely notify and/or warn Plaintiff and Class members of the Data Breach.

147. Defendant breached their fiduciary duties to Plaintiff and Class members by otherwise failing to safeguard Plaintiff's and Class members' PCD/PII.

148. As a direct and proximate result of Defendant's breaches of their fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PCD/PII is used; (iii) the compromise, publication, and/or theft of their PCD/PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PCD/PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PCD/PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the PCD/PII of customers in their continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PCD/PII compromised as a result of the

Data Breach for the remainder of the lives of Plaintiff and Class members; and (ix) the diminished value of Defendant's goods and services they received.

149. As a direct and proximate result of Defendant's breaches of their fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

SIXTH CAUSE OF ACTION
Violation of Florida's Deceptive and Unfair Trade Practices Act
(On Behalf of the Florida Sub Class)

150. Plaintiff restates and realleges paragraphs 1 through 70 above as if fully set forth herein.

151. Plaintiff and the Class Members are "consumers." Fla. Stat. § 501.203(7).

152. Plaintiff and Class Members purchased "things of value" from Defendant and through its Website. These purchases were made primarily for personal, family, or household purposes. Fla. Stat. § 501.203(9).

153. Defendant engaged in the conduct alleged in this Complaint by advertising and entering into transactions intended to result, and which did result, in the sale of goods or services, to consumers, including Plaintiff and the Class Members. Fla. Stat. § 501.203(8).

154. Defendant engaged in, and its acts and omissions affected trade and commerce. Defendant's acts, practices, and omissions were done in the course of Defendant's business of advertising, marketing, offering to sell, and selling and/or renting goods and services throughout Florida and the United States. Fla. Stat. § 501.203(8).

155. Defendant, operating in Florida, engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of Fla. Stat. § 501.204(1), including but not limited to the following:

a. representing (through advertisements and other publication) that it maintained, but in fact failed to maintain adequate computer systems and data security practices to safeguard PCD/PII (which also violated Fla. Stat. §§ 568.365(e), (s));

b. representing (through advertisements and other publication) that their data security practices were adequate, but in fact failed to disclose that their computer systems and data security practices were inadequate to safeguard PCD/PII from theft (which also violated Fla. Stat. §§ 568.365(e), (s));

c. failure to timely and accurately disclose the Data Disclosure to Plaintiff and the Class Members;

d. continued acceptance of credit and debit card payments and storage of other PCD/PII after Defendants knew or should have known of the Data Disclosure and before it allegedly remediated the Data Disclosure;

156. This conduct is considered unfair methods of competition, and constitute unfair and unconscionable acts and practices. Fla. Stat. § 501.204(1).

157. As a direct and proximate result of Defendants' violation of Florida's Deceptive and Unfair Trade Practices Act ("FDUTPA"), Plaintiff and the Class Members suffered actual damages by paying a premium for Defendants' goods and services with the understanding that at least part of the premium would be applied toward sufficient and adequate information security practices that comply with industry standards, when in fact no portion of that premium was applied toward sufficient and adequate information security practices. Fla. Stat. § 501.211(2).

158. Also as a direct result of Defendants' knowing violation of FDUTPA, Plaintiff and Class Members are not only entitled to actual damages, but also declaratory judgment that Defendants' actions and practices alleged herein violate FDUTPA, and injunctive relief, including, but not limited to:

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

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

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

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

e. Ordering that Defendants purge, delete, and destroy in a reasonable secure manner PCD/PII not necessary for their provisions of services;

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

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

h. Ordering Defendants to meaningfully educate their customers about the threats

they face as a result of the loss of their financial and personal information to third parties, as well as the steps Defendants' customers must take to protect themselves.

Fla. Stat. § 501.211(1).

159. Plaintiff brings this action on behalf of himself and the Class Members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff and the Class Members and the public from Defendants' unfair methods of competition and unfair, deceptive, fraudulent, unconscionable, and unlawful practices. Defendants' wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

160. The above unfair and deceptive practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and the Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

161. Defendants knew or should have known that the lack of encryption on their computer systems and data security practices were inadequate to safeguard the Class Members' PCD/PII and that the risk of a data disclosure or theft was high.

162. Defendants' actions and inactions in engaging in the unfair practices and deceptive acts described herein were negligent, knowing and willful, and/or wanton and reckless

163. Plaintiff and the Class Members seek relief under Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. §§ 501.201, *et seq.*, including, but not limited to, damages, injunctive relief, and attorneys' fees and costs, and any other just and proper relief.

SEVENTH CAUSE OF ACTION
Breach of Confidence
(On Behalf of the Nationwide and Florida Sub Classes)

164. Plaintiff restates and realleges paragraphs 1 through 70 above as if fully set forth herein.

165. At all times during Plaintiff's and Class members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class members' PCD/PII that Plaintiff and Class members provided to Defendant.

166. As alleged herein and above, Defendant's relationship with Plaintiff and Class members was governed by terms and expectations that Plaintiff's and Class members' PCD/PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

167. Plaintiff and Class members provided their PCD/PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit PCD/PII to be disseminated to any unauthorized parties.

168. Plaintiff and Class members also provided their PCD/PII to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that PCD/PII from unauthorized disclosure, such as following basic principles of information security practices.

169. Defendant voluntarily received in confidence Plaintiff's and Class members' PCD/PII with the understanding that the PCD/PII would not be disclosed or disseminated to the public or any unauthorized third parties.

170. Due to Defendant's failure to prevent, detect, or avoid the Data Breach from occurring by, *inter alia*, following industry standard information security practices to secure

Plaintiff's and Class members' PCD/PII, Plaintiff's and Class members' PCD/PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class members' confidence, and without their express permission.

171. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class members have suffered damages.

172. But for Defendant's disclosure of Plaintiff's and Class members' PCD/PII in violation of the parties' understanding of confidence, their protected PCD/PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class members' protected PCD/PII, as well as the resulting damages.

173. The injury and harm Plaintiff and Class members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class members' PCD/PII.

174. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PCD/PII is used; (iii) the compromise, publication, and/or theft of their PCD/PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PCD/PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PCD/PII, which remain in Defendant's

possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the PCD/PII of customers in their continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PCD/PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class members; and (ix) the diminished value of Defendant's goods and services they received.

175. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

PRAYER FOR RELIEF

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

a. For an Order certifying the Class as defined herein, and appointing Plaintiff and her Counsel to represent the Class;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class members' PCD/PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class members;

c. For equitable relief compelling Defendant to use appropriate cyber security methods and policies with respect to PCD/PII collection, storage, and protection, and to disclose with specificity to Class members the type of PCD/PII compromised;

d. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

e. For an award of punitive damages;

f. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

g. For prejudgment interest on all amounts awarded; and

h. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: April 8, 2019

Respectfully submitted,

Charles E. Schaffer
Daniel C. Levin
LEVIN SEDRAN & BERMAN
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Telephone: (215) 592-1500
Facsimile: (215) 592-4663
cschaffer@lfsblaw.com
dlevin@lfsblaw.com

MORGAN & MORGAN COMPLEX LITIGATION GROUP
John A. Yanchunis (*pro hac vice to be submitted*)
Patrick A. Barthle (*pro hac vice to be submitted*)
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402
jyanchunis@ForThePeople.com
pbarthle@ForThePeople.com

Attorneys for Plaintiff and the Proposed Class

ClassAction.org