NO. _____
(*ELECTRONICALLY FILED*)

JEFFERSON CIRCUIT COURT
DIVISION: _____
JUDGE: _____

ALISSA GOODLETT, individually,
and as the representative of a class
of similarly-situated persons,
123 Lakeview Drive
Lawrenceburg, Kentucky 40342

PLAINTIFF

VS.

COMPLAINT

BROWN-FORMAN CORPORATION
850 Dixie Highway
Louisville, Kentucky 40210

DEFENDANT

SERVE: Mary E. Barrazotto,
850 Dixie Highway
Louisville, KY 40210

* * * * * * * * * * * * *

COMES THE PLAINTIFF, ALISSA GOODLETT, individually, and as the representative of a class of similarly-situated persons (hereinafter Ms. "Goodlett" or "Plaintiff") by and through her attorneys, Bransetter Stranch & Jennings, PLLC, Thomas & Solomon LLP, and Finkelstein, Blankenship, Frei-Pearson, & Garber, LLP, that as and for her COMPLAINT pursuant to Kentucky Revised Statutes (hereinafter "KRS") TITLE XXIX – COMMERCE AND TRADE, Chapter 365 and Kentucky Rules of Civil Procedure Rule 23, hereby respectfully alleges, upon information and belief, as follows:

I. PARTIES, JURISDICTION AND VENUE

1. That the Plaintiff, Ms. Goodlett, resides at 123 Lakeview Drive, Lawrenceburg, Kentucky 40342, County of Anderson;

Filed 20-CI-005631 09/30/2020 David L. Nicholson, Jefferson Circuit Clerk

2. That at all times relevant hereto, the Defendant, Brown-Forman Corporation (hereinafter "Brown-Forman"), was and is a Delaware corporation, with its principal place of business located at 850 Dixie Highway Louisville, KY 40210, organized and existing under the laws of the Delaware with the power to sue and be sued and it is subject to the venue and jurisdiction of this court pursuant to KRS 454.210;

3. That Brown-Forman's agent for service of process listed on the official website for the Secretary of State of the Commonwealth of Kentucky is: Mary E. Barrazotto, 850 Dixie Highway Louisville, KY 40210;

4. That Ms. Goodlett is a former employee of Brown-Forman, and that she received a notice dated August 25, 2020 from Brown-Forman informing her that IT had disclosed her personal identification information ("PII") in a data breach;

5. That jurisdiction and venue are proper in this Court, as the amount in controversy exceeds $5,000.00, exclusive of interest and costs, Plaintiff seeks declaratory and equitable relief herein, and Defendant's principal place of business is located, and all relevant matters alleged herein occurred, in Jefferson County, Kentucky;

II. CLASS ALLEGATIONS

6. That the legal and factual allegations contained in Complaint Paragraph(s) One (1) through Five (5) are repeated and re-alleged as if fully set forth herein;

7. That the Plaintiff brings this suit against the Defendant as a class action, prosecuted by the named representative individually, and on behalf of a class of similarly situated persons, *to wit*, those individuals whose sensitive and personal information was compromised via a data security breach that occurred on or about July 28, 2020 (the "Data Breach"), pursuant to Kentucky Rules of Civil Procedure, Rule (hereinafter "CR") 23.01

and CR 23.02(b)-(c). Subject to additional information obtained through further investigation and/or discovery, the foregoing definition of the Plaintiff Class may be expanded or narrowed. The proposed Plaintiff Class is as follows:

> **Plaintiff Class:** All citizens of Kentucky who, like ALISSA GOODLETT, were the victims of a data security breach that occurred on or about July 28, 2020 wherein their sensitive and personal data was compromised;

8. That excluded from the Plaintiff Class are: (1) the Defendant, the Defendant's subsidiaries and any entity which the Defendant has a controlling interest in; and (2) the Judge assigned to this case and any member of his or her immediate family. The Plaintiff expressly reserves the right to modify the Plaintiff Class definition as further investigation and/or discovery so warrants;

9. That this action has been brought and may properly be maintained as a class action pursuant to CR 23 and the case law thereunder;

10. **Numerosity:** That the members of the Plaintiff Class are so numerous that joinder of all members is impracticable. The Plaintiff reasonably believes that the Plaintiff Class is comprised of numerous individuals throughout the Commonwealth of Kentucky and elsewhere;

11. **Commonality:** That common questions of law and fact exist as against the Defendant in this action. These common questions predominate over any questions affecting only individual Plaintiff Class members. These common legal and factual questions include, but are not limited to, the following:

- whether or not the Defendant owed the members of the Plaintiff Class a duty to safeguard their information;
- whether or not the Defendant breached that duty;
- whether or not the Defendant has invaded the privacy of the members of the Plaintiff Class;

Filed 20-CI-005631 09/30/2020 David L. Nicholson, Jefferson Circuit Clerk

- whether or not the Plaintiff Class members have sustained monetary loss, and the proper measure of that loss;
- whether or not the Plaintiff Class members are entitled to punitive and/or exemplary damages; and
- whether or not the Plaintiff Class members are entitled to declaratory and injunctive relief.

These and other questions of law and/or fact are common to members of the Plaintiff Class and predominate over any questions affecting only individual members of it;

12. **Typicality:** That the Plaintiff's claims against the Defendant are typical of the claims of the similarly situated members of the Plaintiff Class, as the Plaintiff asserts claims against the Defendant flowing from a single security breach that occurred on or about July 28, 2020. Conversely, the Defendant, by and through one or more agent(s) thereof, engaged in a unitary course of conduct that forms the basis of this lawsuit. The Plaintiff is advancing the same claims and legal theories on behalf of herself and all absent members of the Plaintiff Class;

13. **Adequacy:** That the Plaintiff's claims are made in a representative capacity on behalf of the other members of the Plaintiff Class. The Plaintiff has no interests antagonistic to the interests of the other members of the Plaintiff Class and is subject to no unique defenses;

14. That the Plaintiff is similarly situated in interest to all members of the proposed Plaintiff Class and is committed to the vigorous prosecution of this action and has retained competent counsel experienced in the prosecution of class actions. Accordingly, the Plaintiff is an adequate representative of the Plaintiff Class and will fairly and adequately protect the interests of the members of the Plaintiff Class;

Filed 20-CI-005631 09/30/2020 David L. Nicholson, Jefferson Circuit Clerk

15. That this suit may be maintained as a class action under CR 23.02(b) because Defendant has acted or refused to act on grounds generally applicable to the Plaintiff Class, thereby making appropriate final injunctive or corresponding declaratory relief with respect to the class as a whole. Defendant is still in possession of Plaintiff Class' PII, and absent court intervention requiring Defendant to enhance its inadequate security measures, there is a substantial likelihood that further unauthorized disclosures will occur; and

16. That this suit may be maintained as a class action under CR 23.02(c) because a class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by the Defendant's conduct. It would be virtually impossible for members of the Plaintiff Class individually to redress the wrongs perpetrated upon them. Even if the members of the Plaintiff Class could afford such litigation, the court system cannot. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents no management difficulties, and provides the benefits of single adjudication, economy of scale and comprehensive supervision by a single court;

III. CAUSE(S) OF ACTION

AS AND FOR A FIRST CAUSE OF ACTION NEGLIGENCE

17. That the legal and factual allegations contained in Complaint Paragraph(s) One (1)

Filed 20-CI-005631 09/30/2020 David L. Nicholson, Jefferson Circuit Clerk

through Sixteen (16) are repeated and re-alleged as if fully set forth herein;

18. That on or about July 28, 2020, an unauthorized third party accessed the Defendant's servers and systems resulting in the Data Breach and exposure of the PII of thousands of persons;

19. That the unauthorized third party responsible for the cyber-attack is Sodinokibi ("REvil"), a group similar to other cyber gangs;

20. That REvil not only compromised the Defendant's computer network but has acknowledged that they spent over one month examining the general structure of the computer network, as well as user services and cloud data storage;

21. That according to REvil, one terabyte of corporate data was taken, and REvil has shared screenshots of file names as proof, with some files dating back ten years;

22. That the Defendant has confirmed that the Data Breach occurred and has acknowledged that information, including employee data, was impacted;

23. That the Plaintiff received a letter dated August 25, 2020 from Brown-Forman informing her of the Breach;

24. That the correspondence received by the Plaintiff informed her that as a result of the Breach, her PII was compromised, which could include her name, Social Security number, work contact information, home address, position, business title, and salary-related information;

25. That the correspondence sent by Brown-Forman further indicates that the cybercriminals are attempting to contact employees by phone, voicemail, and email;

26. That by disclosing the Plaintiff's PII to cybercriminals, the Defendant put the

Filed 20-CI-005631 09/30/2020 David L. Nicholson, Jefferson Circuit Clerk

Plaintiff and the Plaintiff Class at risk;

27. That the Defendant negligently failed to take the necessary precautions required to safeguard and protect the Plaintiff's PII from unauthorized disclosure. The Defendant's actions and/or inactions represent a flagrant disregard of the Plaintiff's rights, both as to privacy and property;

28. That PII is of great value to hackers and cyber criminals, and the data compromised in the Data Breach can be used in a variety of unlawful manners;

29. That the PII of individuals is of high value to criminals, as evidenced by the prices they will pay through the dark web. For example, personal information can be sold at prices ranging from $40 to $200. *See Your personal data is for sale on the dark web. Here's how much it costs.* Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Sept. 17, 2020);

30. That there is a strong likelihood that the Plaintiff is already or will become a victim of identity theft and fraud, given the breadth of PII about her that has been released, disclosed, and published;

31. That it has been reported that this Data Breach was a ransomware attack by REvil, and that screenshots showing internal communications, directory trees, financial documents, contracts, and personnel data, have been posted by REvil to substantiate the breach;

32. That the possibility that the Plaintiff's Social Security numbers can be purchased on the dark web as a result of the Data Breach is particularly significant. For instance, REvil has auctioned off sensitive data from other companies hit by REvil's ransomware on

Filed 20-CI-005631 09/30/2020 David L. Nicholson, Jefferson Circuit Clerk

their dark web blog, "Happy Blog";

33. That Neal O'Farrell, a security and identity theft expert for Credit Sesame, calls a Social Security number "your secret sauce," that is "as good as your DNA to hackers." *See* Cameron Huddleston, *How to Protect Your Kids From the Anthem Data Breach*, Kiplinger, (Feb. 10, 2015), https://www.kiplinger.com/article/credit/t048-c011-s001-how-to-protect-your-kids-from-the-anthem-data-brea.html (last accessed Sept. 17, 2020);

34. That the Plaintiff has to wait until she becomes a victim of Social Security number misuse before she can obtain a new one. Even then, the Social Security Administration warns "that a new number probably won't solve all [] problems . . . and won't guarantee . . . a fresh start." In fact, "[f]or some victims of identity theft, a new number actually creates new problems." *See* Social Security Admin., *Identity Theft and Your Social Security Number*, at 6, https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Sept. 17, 2020);

35. That one of those new problems is that a new Social Security number will have a completely blank credit history, making it difficult to get credit for years unless it is linked to the old compromised number;

36. That given the nature of this Breach, it is foreseeable that cybercriminals can and will use the compromised PII in a variety of different ways;

37. That as part of her employment, the Defendant required the Plaintiff and the Plaintiff Class to surrender their PII including names, addresses, and social security numbers, as well as the names, addresses and social security numbers of their beneficiaries, and were entrusted with properly holding, safeguarding, and protecting against unlawful disclosure of PII;

38. That the Data Breach was a direct result of the Defendant's failure to implement

Filed 20-CI-005631 09/30/2020 David L. Nicholson, Jefferson Circuit Clerk

adequate and reasonable cyber-security procedures and protocols necessary to protect the Plaintiff's PII;

39. That the Defendant maintained the PII in a reckless manner. In particular, the PII was maintained on the Defendant's servers in a condition vulnerable to cyberattacks;

40. That the Defendant knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences that would occur if the Plaintiff's PII was stolen, including the significant costs the Plaintiff would incur as a result of a breach;

41. That the mechanism of the cyberattack and potential for improper disclosure of the Plaintiff's PII was a known risk to the Defendant, and thus the Defendant was on notice that failing to take steps necessary to secure the PII from those risks left that information in a dangerous condition;

42. That the Defendant disregarded the rights of the Plaintiff by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard the Plaintiff's PII; and failing to take standard and reasonably available steps to prevent the Data Breach;

43. That the Federal Trade Commission has issued an abundance of guidance for companies to protect the PII in their possession. *See e.g.*, *Protecting Personal Information: A Guide for Business*, FTC, *available at* https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business;

44. That the Defendant, as a large and sophisticated employer, was well aware of the risks of data breaches and that the Defendant knew or should have known of the risks of

data breaches and thus should have ensured that the adequate protections were in place;

45. That the Plaintiff entrusted the Defendant with her sensitive PII;

46. That the Plaintiff has suffered or will suffer actual injury as a direct result of the Data Breach. These actual injuries include out-of-pocket expenses and the value of her time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

- Closely reviewing and monitoring bank accounts and credit reports;
- Purchasing credit monitoring and identity theft prevention;
- Addressing her inability to withdraw funds linked to compromised accounts;
- Placing "freezes" and "alerts" with credit reporting agencies; and
- Contacting financial institutions and closing or modifying financial accounts.

47. That the Plaintiff is at an increased risk that the cybercriminals will use her PII for the rest of her life;

48. That because of this increased risk that her PII will be misused, the Plaintiff purchased identify theft protection and monitoring services;

49. That the Plaintiff brings this action because as a direct and/or proximate result of the Defendant's wrongful actions and/or inaction and the resulting Data Breach, the Plaintiff has incurred and will continue to incur damages in the form of, *inter alia*, attempted identity theft, time and expenses mitigating harms (*e.g.*, the costs of engaging credit monitoring and protection services), increased risk of harm, diminished value of PII, and/or loss of privacy. The Defendant's omissions and/or commissions were a substantial

factor in the Plaintiff and the other Plaintiff Class members incurring those damages;

50. By this action, the Plaintiff seeks to hold the Defendant responsible for the harm caused by its negligence;

51. That in addition, as a direct and/or proximate result of the Defendant's wrongful actions and/or inaction and the resulting Data Breach, the Plaintiff have been deprived of the value of her PII, for which there is a well-established national and international market;

52. That the Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed the Plaintiff at an imminent, immediate, and continuing increased risk of identity theft and identity fraud. Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported;

53. That the cybercriminals who obtained the Plaintiff's and the absent members of the Plaintiff Class's PII continue to exploit the data themselves and/or sell the data in the so-called "dark markets." Having obtained the Plaintiff and the absent members of the Plaintiff Class's names, addresses and Social Security numbers, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Plaintiff's name, including but not limited to:

Filed 20-CI-005631 09/30/2020 David L. Nicholson, Jefferson Circuit Clerk

a. obtaining employment;

b. obtaining a loan;

c. applying for credit cards or spending money;

d. filing false tax returns;

e. obtaining medical care;

f. stealing Social Security and other government benefits; and

g. applying for a driver's license, birth certificate or other public document;

54. That the Defendant has failed to provide adequate compensation to the Plaintiff harmed by its negligence. To date, the Defendant has offered the Plaintiff just twelve (12) months of credit monitoring through IdentityWorks℠. Even if a Plaintiff signs up for IdentityWorks℠, it will not provide the Plaintiff any compensation for the costs and burdens associated with fraudulent activity resulting from the Data Breach that took place prior to the Plaintiff signing up;

55. That because of the inadequate identity theft coverage offered by the Defendants, the Plaintiff was required to purchase her own independent identity theft protection services to have adequate protection of her PII;

56. That the Defendant owed the Plaintiff and the absent members of the Plaintiff Class a duty of ordinary and reasonable care to safeguard their personal and sensitive information, to the same extent that a reasonably prudent person would behave under the circumstances;

57. That the Defendant had full knowledge of the sensitivity of the PII and the types of harm that the Plaintiff and class members could and would suffer if that information was wrongfully disclosed. The Defendant had a duty to the Plaintiff and each Plaintiff Class

Filed 20-CI-005631 09/30/2020 David L. Nicholson, Jefferson Circuit Clerk

member to exercise reasonable care in holding, safeguarding and protecting that information. The Plaintiff and the Plaintiff Class members were the foreseeable victims of any inadequate safety and security practices. The Plaintiff and the other class members had absolutely no ability to protect their data that was in the Defendant's possession;

58. That the Defendant's duty to the Plaintiff and other Plaintiff Class members included, *inter alia*, establishing processes and procedures to protect the personal and sensitive information from wrongful disclosure and training employees who had access to that information as to those processes and procedures. The Defendant's officers, directors and management knew or should have known of the risks associated with the wrongful disclosure of that entrusted information and the threats to that information posed by hackers, scammers, and other cybercriminals;

59. That the acts and/or omissions of the Defendant and/or its agents thereof complained of herein were wanton and/or willful, that they were conducted in such a reckless manner and with such patent disregard for the rights of the Plaintiff and the members of the Plaintiff Class, whereby the Defendant is liable to them for punitive and/or exemplary damages, as permitted by law; and, further, that the Plaintiff and the members of the Plaintiff Class seek an amount in punitive and/or exemplary damages that is fair and reasonable as shown by the evidence; and

60. That pursuant to CR 8.01, the amount in controversy exceeds the minimum threshold of the Jefferson County Circuit Court;

AS AND FOR A SECOND CAUSE OF ACTION
NEGLIGENCE PER SE

61. That the legal and factual allegations contained in Complaint Paragraph(s) One (1)

Filed 20-CI-005631 09/30/2020 David L. Nicholson, Jefferson Circuit Clerk

through Sixty (60) are repeated and re-alleged as if fully set forth herein;

62. That the Kentucky General Assembly enacted AN ACT relating to the security of personal information (hereinafter the "Personal Information Security Law"), which was created by House Bill 232, and signed into law on April 10, 2014;

63. That the Personal Information Security Law is codified in KRS TITLE XXIX – COMMERCE AND TRADE, Chapter 365: Trade Practices (hereinafter "KRS 365"), and that those pertinent sections of the KRS are hereby made a part hereof as if the same was herein fully set forth at length;

64. That Section 720 of KRS 365: "Definitions for KRS 365.720 to 365.730" (3) defines the term "Individual" as a "natural person";

65. That Section 732 of KRS 365: "Notification to affected persons of computer security breach involving their unencrypted personally identifiable information" (hereinafter "KRS 365.732") (1)(a) defines the term "Breach of the security of the system" as an:

> **unauthorized acquisition of unencrypted and unredacted computerized data** that compromises the security, confidentiality, or integrity of personally identifiable information maintained by the information holder as part of a database regarding multiple individuals that **actually causes, or leads the information holder to reasonably believe has caused or will cause, identity theft or fraud against any resident of the Commonwealth of Kentucky**…

KRS 365.732(1)(a) (emphasis added);

66. That KRS 365.732(1)(b) further defines the term "Information holder" as "any… business entity that conducts business in [the Commonwealth of Kentucky]";

67. That KRS 365.732(1)(c) further defines "Personally identifiable information" as "an individual's first name or first initial and last name in combination with any one (1) or

Filed 20-CI-005631 09/30/2020 David L. Nicholson, Jefferson Circuit Clerk

more of the following data elements, when the name or data element is not redacted: 1. Social Security number…";

68. That KRS 365.732(2) mandates that:

> [a]ny information holder **shall disclose any breach of the security of the system**, following discovery or notification of the breach in the security of the data, to any resident of Kentucky whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. **The disclosure shall be made in the most expedient time possible and without unreasonable delay**…

KRS 365.732(2) (emphasis added);

69. That the Plaintiff and the absent members of the Plaintiff Class are natural persons and individuals for the purposes of KRS 365.720(3);

70. That the Defendant encountered a breach of the security of its system(s) on or about July 28, 2020;

71. That the Defendant did not notify the Plaintiff and the absent members of the Plaintiff Class until August 25, 2020, almost a month after the breach;

72. That as a direct and/or proximate result of the Defendant's delay in notifying the Plaintiff and Plaintiff Class members of the breach, the Plaintiff was subject to potentially avoidable harm which could have been mitigated by: (i) purchasing identity protection services earlier; (ii) monitoring bank accounts, credit cards and other financial accounts earlier; and (iii) taking other steps to protect against identity theft and the fraudulent use of PII by third parties; and

73. That pursuant to CR 8.01, the amount in controversy exceeds the minimum threshold of the Jefferson County Circuit Court;

Filed 20-CI-005631 09/30/2020 David L. Nicholson, Jefferson Circuit Clerk

AS AND FOR A THIRD CAUSE OF ACTION
INVASION OF PRIVACY

74. That the legal and factual allegations contained in Complaint Paragraph(s) One (1) through Seventy-Three (73) are repeated and re-alleged as if fully set forth herein;

75. That the Defendant, through its agent(s), publicized private, sensitive, and personal facts of or concerning the Plaintiff and the absent members of the Plaintiff Class to thousands of people on the dark web;

76. That the Plaintiff and the absent members of the Plaintiff Class had an actual and reasonable expectation of privacy in their sensitive PII which was publicized;

77. That the matters publicized are of a kind that would be highly offensive to a reasonable person;

78. That the matters publicized are not of legitimate concern to the public;

79. That as a direct and proximate result of the aforesaid publication, the Plaintiff and the absent members of the Plaintiff Class suffered damages, as their sensitive and personal information is literally in the hands of cybercriminals who intend to use that information for nefarious purposes;

80. That the acts and/or omissions of the Defendant and/or its agents thereof complained of herein were wanton and/or willful, that they were conducted in such a reckless manner and with such patent disregard for the rights of the Plaintiff and the members of the Plaintiff Class, whereby the Defendant is liable to them for punitive and/or exemplary damages, as permitted by law; and, further, that the Plaintiff and the members of the Plaintiff Class seek an amount in punitive and/or exemplary damages that is fair and reasonable as shown by the evidence; and

81. That pursuant to CR 8.01, the amount in controversy exceeds the minimum

threshold of the Jefferson County Circuit Court;

AS AND FOR A FOURTH CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT

82. That the legal and factual allegations contained in Complaint Paragraph(s) One (1) through Eighty-One (81) are repeated and re-alleged as if fully set forth herein;

83. That the Plaintiff and the absent members of the Plaintiff Class provided their PII in connection with their employment with the Defendant in order to verify their identity, receive compensation and in order for the Defendant to have complete employee records for tax purposes, amongst other things;

84. That the Plaintiff and the absent members of the Plaintiff Class provided various sensitive and personal information to the Defendant as a condition precedent to their employment with Defendant, or in connection with employer sponsored benefits;

85. That, understanding the sensitive nature of the PII, the Defendant implicitly promised the Plaintiff and the Plaintiff Class members that it would take adequate measures to protect their sensitive and personal information;

86. That a material term of this contract is a covenant by the Defendant that it will take reasonable efforts to safeguard that information;

87. That the Plaintiff and the Plaintiff Class members relied upon that covenant and would not have disclosed their PII without assurances that it would be properly safeguarded. Moreover, the covenant to adequately safeguard the PII is an implied term, to the extent it is not an express term;

88. That the Plaintiff and the Plaintiff Class members fulfilled their obligations under the contract by providing their PII to the Defendant;

Filed 20-CI-005631 09/30/2020 David L. Nicholson, Jefferson Circuit Clerk

89. That the Defendant, however, failed to safeguard and protect the PII. The Defendant's breach of its obligations under the contract between the parties directly caused the Plaintiff and the Plaintiff Class members to suffer injuries;

90. That the Plaintiff and the Plaintiff Class members respectfully request that this honorable Court award all relevant damages for the Defendant's breach of contract; and

91. That pursuant to CR 8.01, the amount in controversy exceeds the minimum threshold of the Jefferson County Circuit Court;

AS AND FOR A FIFTH CAUSE OF ACTION
INTENTIONAL AND/OR NEGLIGENT INFLICTION OF EMOTIONAL DISTRESS

92. That the legal and factual allegations contained in Complaint Paragraph(s) One (1) through Ninety-One (91) are repeated and re-alleged as if fully set forth herein;

93. That the Defendant engaged in extreme or outrageous conduct;

94. That the afore-described conduct was intended to cause and/or the Defendant's actions indicate reckless disregard for the risk of causing, and did indeed cause severe emotional distress to the Plaintiff and the absent members of the Plaintiff Class;

95. That the acts and/or omissions of the Defendant and/or its agents thereof complained of herein were wanton and/or willful, that they were conducted in such a reckless manner and with such patent disregard for the rights of the Plaintiff and the members of the Plaintiff Class, whereby the Defendant is liable to them for punitive and/or exemplary damages, as permitted by law; and, further, that the Plaintiff and the members of the Plaintiff Class seek an amount in punitive and/or exemplary damages that is fair and

Filed 20-CI-005631 09/30/2020 David L. Nicholson, Jefferson Circuit Clerk

reasonable as shown by the evidence; and

96. That pursuant to CR 8.01, the amount in controversy exceeds the minimum threshold of the Jefferson County Circuit Court;

AS AND FOR A SIXTH CAUSE OF ACTION
INJUNCTIVE/DECLARATORY RELIEF

97. That the legal and factual allegations contained in Complaint Paragraph(s) One (1) through Ninety-Six (96) are repeated and re-alleged as if fully set forth herein;

98. That Defendant acted or refused to act on grounds that apply generally to Plaintiff and the Plaintiff Class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the Plaintiff Class within the meaning of CR 23.02(b);

99. That Plaintiff seeks a declaration that Defendant's acts and omissions as alleged herein violate applicable state law as well as such other and further relief as may follow from the entry of such a judgment and request that the Court issue declaratory relief declaring Defendant's practice of using insecure, outdated, and inadequate email and computer systems and software that can be breached by third parties unlawful;

100. That Plaintiff and the Plaintiff Class further request the Court enter an injunction requiring Defendant to cease the unlawful practices described herein, and enjoining Defendant from disclosing or using PII without first adequately securing or encrypting it;

101. That Plaintiff and the Plaintiff Class members request the Court order Defendant to identify, seek, obtain, encrypt, and retain at the conclusion of this action all existing PII in their possession or the possession of third parties and provide it to Plaintiff and the Plaintiff Class members;

102. That Plaintiff and the Plaintiff Class members request that the Court enter an injunction ordering that Defendant:

Filed 20-CI-005631 09/30/2020 David L. Nicholson, Jefferson Circuit Clerk

a. engage a third-party ombudsman as well as internal compliance personnel to monitor, conduct, test, and audit Defendant's safeguards and procedures on a periodic basis;

b. audit, test, and train its internal personnel regarding any new or modified safeguards and procedures;

c. conduct regular checks and tests on its safeguards and procedures;

d. periodically conduct internal training and education to inform internal personnel how to immediately identify violations when they occur and what to do in response;

e. meaningfully educate its former and current employees about their privacy rights by, without limitation, written statements describing with reasonable specificity the precautionary steps Defendant is taking to update its security technology to adequately secure and safeguard employee PII; and

f. identify to each Plaintiff Class member in writing with reasonable specificity the PII and personal information of each such Plaintiff Class member that was stolen in the Data Breach.

IV. PRAYER FOR RELIEF

WHEREFORE, the Plaintiff, ALISSA GOODLETT, individually, and as the representative of a class of similarly-situated persons respectfully prays this Court to grant an Order, pursuant to Kentucky Revised Statutes TITLE XXIX – COMMERCE AND TRADE, Chapter 365 and Kentucky Rules of Civil Procedure Rule 23: **(A)** certifying this case as a class action, appointing the Plaintiff as class representative and appointing the Plaintiff's counsel to represent the classes; **(B)** holding that the Defendant BROWN-

FORMAN, INC. breached its duty to safeguard and protect the Plaintiff's and the Plaintiff Class members' personal and sensitive information that was compromised; **(C)** awarding the Plaintiff and class members appropriate relief, including actual damages, punitive and/or exemplary damages and statutory damages as permitted by law; **(D)** awarding equitable, injunctive and declaratory relief as appropriate; **(E)** awarding all costs, including experts' fees and attorneys' fees, and the costs of prosecuting this action; **(F)** awarding pre-judgment and post-judgment interest as permitted by law; **(G)** conducting trial by jury herein; **(H)** bestowing leave upon the Plaintiff to amend her COMPLAINT; and **(I)** for such other and further relief as may be just, proper, and equitable.

Dated: September 30, 2020
Louisville, Kentucky

Respectfully submitted,

/s/ Peter J. Jannace
Peter J. Jannace

BRANSTETTER, STRANCH & JENNINGS, PLLC

Gerard Stranch (to be admitted *pro hac vice*)
Peter J. Jannace
Attorneys for Plaintiff and Class Members
515 Park Avenue
Louisville, Kentucky 40208
Telephone: (502) 636-4333
Fax: (502) 636-4342
gerards@bsjfirm.com
peterj@bsjfirm.com

FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP

Jeremiah Frei-Pearson, Esq. (to be admitted *pro hac vice*)
D. Greg Blankinship, Esq. (to be admitted *pro hac vice*)
Attorneys for Plaintiff and Class Members

One North Broadway, Suite 900
White Plains, NY 10601
Telephone: 914-298-3284
jfrei-pearson@fbfglaw.com
gblankinship@fbfglaw.com

THOMAS & SOLOMON LLP

J. Nelson Thomas, Esq. (to be admitted *pro hac vice*)
Jessica L. Lukasiewicz, Esq. (to be admitted *pro hac vice*)
Jonathan W. Ferris, Esq. (to be admitted *pro hac vice*)
Attorneys for Plaintiff and Class Members
693 East Avenue
Rochester, New York 14607
Telephone: (585) 272-0540
nthomas@theemploymentattorneys.com
jlukasiewicz@theemploymentattorneys.com
jferris@theemploymentattorneys.com

Filed 20-CI-005631 09/30/2020 David L. Nicholson, Jefferson Circuit Clerk