

**UNITED STATES DISTRICT COURT  
DISTRICT OF MINNESOTA**

Village Bank, on behalf of itself and all  
others similarly situated,

Plaintiff,

v.

Caribou Coffee Company, Inc.,  
Bruegger's Enterprises, Inc., Einstein &  
Noah Corp., and Einstein Noah  
Restaurant Group, Inc.

Defendants.

Case No.

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

**CLASS ACTION COMPLAINT**

Plaintiff brings this action on behalf of itself and all others similarly situated against Defendants Caribou Coffee Company, Inc. ("Caribou"), Bruegger's Enterprises, Inc. ("Bruegger's"), Einstein & Noah Corp. ("Einstein Bros."), and Einstein Noah Restaurant Group, Inc. ("Einstein Noah") (collectively, "Coffee & Bagel Brands"<sup>1</sup> or "Defendants") and states:

**INTRODUCTION**

1. This class action lawsuit arises out of a data breach at 473 locations<sup>2</sup> located

---

<sup>1</sup> Caribou, Bruegger's and Einstein Bros. collectively refer to themselves as "Coffee & Bagel Brands." See <https://www.coffeeandbagels.com/> ("Our Brands": Caribou, Bruegger's, Einstein Bros. and others).

<sup>2</sup> Including 265 Caribou locations, 157 Bruegger's locations, and 51 Einstein Bros. locations.

throughout 24 different states<sup>3</sup> and operated by Coffee & Bagel Brands.

2. Despite the growing threat of computer system intrusion, Coffee & Bagel Brands systematically failed to comply with industry standards and their statutory and common law duties to protect the payment card data of their customers.

3. Coffee & Bagel Brands' systemic failure exposed their customers' payment cards from at least August 28, 2018 to December 3, 2018, and allowed hackers to steal that data and misuse it for various purposes.

4. Had Coffee & Bagel Brands put reasonable processes and procedures in place, they would have had a reasonable chance to prevent the breach. In fact, Coffee & Bagel Brands' data practices were so deficient that their customers' data was exposed for over three months and Coffee & Bagel Brands failed to detect any issues.

5. The costs and financial harm caused by Coffee & Bagel Brands' negligent conduct is borne primarily by financial institutions, like Plaintiff, that issued the payment cards compromised in this data breach. These costs include, but are not limited to, cancelling and reissuing compromised cards and reimbursing its members for fraudulent charges.

6. This class action is brought on behalf of financial institutions throughout the

---

<sup>3</sup> Alabama, Arizona, Colorado, Connecticut, Florida, Georgia, Iowa, Kansas, Kentucky, Massachusetts, Michigan, Minnesota, Missouri, Nebraska, New York, North Carolina, North Dakota, Ohio, Pennsylvania, South Dakota, Tennessee, Vermont, Virginia, and Wisconsin.

country to recover the costs that they and others similarly situated have been forced to bear as a direct result of the Coffee & Bagel Brands' data breach and to obtain other equitable relief. Plaintiff asserts claims for negligence, and declaratory and injunctive relief.

### **JURISDICTION AND VENUE**

7. This Court has original jurisdiction of this Action pursuant to the Class Action Fairness Act, 28 U.S.C § 1332(d)(2). The matter in controversy, exclusive of interest and costs, exceeds the sum or value of \$5,000,000 and at least some members of the proposed Class have a different citizenship from Defendants. There are more than 100 putative Class members.

8. This Court has personal jurisdiction over Defendants because Caribou, Bruegger's, and Einstein Bros. each regularly conduct business in Minnesota, and have sufficient minimum contacts in Minnesota. Caribou also maintains a principal place of business in Minnesota. Caribou, Bruegger's, and Einstein Bros. each intentionally availed itself of this jurisdiction by accepting and processing payments for its foods and other services within Minnesota.

9. Venue is proper under 18 U.S.C. § 1391(a) because Caribou's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

### **PARTIES**

10. Plaintiff Village Bank is a Minnesota state-chartered bank with locations in

Ramsey, Blaine, East Bethel, and St. Francis. Village Bank's main office is located at 3350 Bridge Street, Northwest, St. Francis, Minnesota, 55070.

11. Plaintiff is a Mastercard payment card issuer and received Account Data Compromise Alerts ("ADC alerts"). As a result of Coffee & Bagel Brands' actions and the breach of their data systems, Plaintiff has suffered, and continues to suffer, injury, including, *inter alia*, costs to cancel and reissue cards compromised in the data breach, costs to refund fraudulent charges, costs to investigate fraudulent charges, costs for customer fraud monitoring, and costs due to lost interest and transaction fees due to reduced card usage.

12. Defendant Caribou Coffee Company, Inc. ("Caribou") is a Minnesota corporation with its principal place of business located in Brooklyn Center, Minnesota. Caribou is a business that accepts payment for its goods and services through a point-of-sale ("POS") network. Consumers swipe payment cards, which are issued by Plaintiff and other members of the Class, at Caribou's POS terminals to effectuate payment for Caribou's goods and services. Caribou is a subsidiary of JAB Holding Company, headquartered in Luxembourg City, Luxembourg.

13. Defendant Bruegger's Enterprises, Inc. ("Bruegger's") is a Delaware corporation with its principal place of business located in Burlington, Vermont. Bruegger's is a business that accepts payment for its goods and services through a POS network. Consumers swipe payment cards, which are issued by Plaintiff and other members of the

Class, at Bruegger's' POS terminals to effectuate payment for Bruegger's' goods and services. Bruegger's is a subsidiary of JAB Holding Company, headquartered in Luxembourg City, Luxembourg.

14. Defendant Einstein & Noah Corp. ("Einstein Bros.") is a Delaware corporation with its principal place of business located in Lakewood, Colorado. Einstein Bros. is a business that accepts payment for its goods and services through a POS network. Consumers swipe payment cards, which are issued by Plaintiff and other members of the Class, at Einstein Bros.'s POS terminals to effectuate payment for Einstein Bros.'s goods and services. Defendant Einstein Bros. is a wholly owned subsidiary of Einstein Noah Restaurant Group, Inc., a Delaware corporation with its principal place of business located in Lakewood, Colorado.

15. Defendant Einstein Noah Restaurant Group, Inc. ("Einstein Noah") is a Delaware corporation with its principal place of business located in Lakewood, Colorado. Einstein Noah is a business that accepts payment for its goods and services through a POS network. Consumers swipe payment cards, which are issued by Plaintiff and other members of the Class, at Einstein Noah's POS terminals to effectuate payment for Einstein Noah's goods and services. Einstein Noah is a subsidiary of JAB Holding Company, headquartered in Luxembourg City, Luxembourg.

16. Defendants Caribou, Bruegger's, Einstein Bros., and Einstein Noah

collectively refer to themselves as “Coffee & Bagel Brands.”<sup>4</sup>

### **STATEMENT OF FACTS**

17. Coffee & Bagels Brands are chain coffee shops/restaurants consisting of several brands, including Caribou, Bruegger’s, and Einstein Bagels. Coffee & Bagels Brands include the following locations affected by the breach:

- a. 265 Caribou-owned locations located throughout 11 states: Colorado, Florida, Georgia, Iowa, Kansas, Minnesota, Missouri, North Carolina, North Dakota, South Dakota, and Wisconsin;
- b. 157 Bruegger’s-owned locations located throughout 17 states: Alabama, Connecticut, Florida, Iowa, Kentucky, Massachusetts, Michigan, Minnesota, Nebraska, New York, North Carolina, Ohio, Pennsylvania, Tennessee, Vermont, Virginia, and Wisconsin; and
- c. 51 Einstein Bros.-owned locations located throughout 9 states: Arizona, Colorado, Florida, Georgia, Iowa, Minnesota, North Dakota, South Dakota, and Wisconsin.

18. Recently, financial institutions have experienced an unprecedented number of Compromised Account Management System (“CAMS”) alerts on their members’ accounts from VISA and ADC alerts on their members’ accounts from MasterCard. CAMS

---

<sup>4</sup> See <https://www.coffeeandbagels.com/> (“Our Brands”: Caribou, Bruegger’s, Einstein Bros. and others).

and ADC alerts typically are issued by VISA and MasterCard when there is some event that jeopardizes the security of a financial institution's customers' accounts.

19. The alert Plaintiff received estimates the "exposure window" for the breach of Coffee & Bagel Brands' computer systems runs from at least August 28, 2018 to December 3, 2018, meaning Coffee & Bagel Brands failed to prevent or stop hackers from accessing their systems and stealing cardholder data for over three months.

20. The alert further indicates that both Track 1 and Track 2 data may have been compromised in the data breach. Track 1 and Track 2 data normally includes credit and debit card information such as cardholder name, primary account number, expiration date, and in certain instances PIN number.

21. The alert corresponds with information contained in the official public announcement made by Coffee & Bagel Brands regarding the breach of their data processing systems on December 20, 2018.<sup>5</sup> According to the notice, on November 28, 2018, Coffee and Bagel Brands identified unusual activity on their networks. Coffee & Bagel Brands began working with Mandiant, a cyber security firm, and on November 30, 2018, Mandiant reported that it detected unauthorized access to Coffee & Bagel Brands' POS systems, exposing their customers' data.

---

<sup>5</sup> Identical breach notification letters were sent out from Caribou, Bruegger's, and Coffee and Bagels, available at <https://assets.coffeeandbagels-static.com/cariboucoffee/Data-Security-Notice.pdf>, <https://assets.coffeeandbagels-static.com/brueggers/Data-Security-Notice.pdf>, and <https://assets.coffeeandbagels-static.com/coffeeandbagels/Data-Security-Notice.pdf>, respectively.

22. The breach of Coffee & Bagel Brands' data systems occurred when hackers installed malware on Coffee & Bagel Brands' POS networks that allowed hackers to steal payment card data from remote locations as a card was swiped for payment.

23. The breach was made possible because Coffee & Bagel Brands disregarded the security of their POS networks and the potential danger of a data breach, and failed to put in place reasonable systems and procedures to prevent the harm that their actions have caused.

24. Coffee & Bagel Brands knew the danger of not safeguarding their POS network as various high-profile data breaches have occurred in the same way, including the highly publicized data breaches of Target, Home Depot, and Wendy's.

25. Despite this knowledge, Coffee & Bagel Brands acted unreasonably and failed to adequately and reasonably protect the data of their customers.

26. Coffee & Bagel Brands' failure is particularly egregious because various state and federal statutes obligate Coffee & Bagel Brands to act reasonably in protecting the data of the members of Plaintiff and the Class.

27. First, the payment card industry (MasterCard, VISA, Discover, and American Express), long before the breach of Coffee & Bagel Brands' data systems, issued Card Operating Regulations that: (1) are binding on Coffee & Bagel Brands; (2) required Coffee & Bagel Brands to protect cardholder data and prevent their unauthorized disclosure; (3) prohibited Coffee & Bagel Brands from storing such data, even in encrypted



form, longer than necessary to process the transaction; and (4) mandated Coffee & Bagel Brands comply with industry standards.

28. Second, the payment card industry set rules requiring all businesses, including Coffee & Bagel Brands, to upgrade to new card readers that accept EMV chips. EMV chip technology uses imbedded computer chips instead of magnetic stripes to store payment card data. Unlike magnetic-stripe cards that use static data (the card information never changes), EMV cards use dynamic data. Every time an EMV card is used, the chip creates a unique transaction code that cannot be used again. Such technology greatly increases payment card security because if an EMV chip's information is stolen, the unique number cannot be used by the hackers making it much more difficult for criminals to profit from what is stolen.

29. The set deadline for businesses to transition their systems from magnetic-stripe to EMV technology was October 1, 2015, a deadline Coffee & Bagel Brands, on information and belief, did not meet.

30. Under the Card Operating Regulations that are binding on Coffee & Bagel Brands, businesses accepting payment cards but not meeting the October 1, 2015, deadline agree to be liable for damages resulting from any data breaches.

31. Third, the Payment Card Industry Security Standards Council promulgates minimum standards, which apply to all organizations that store, process, or transmit payment card data. These standards are known as the Payment Card Data Security Standard

(“PCI DSS”). PCI DSS is the industry standard governing the security of payment card data, although it sets the minimum level of what must be done, not the maximum.

32. PCI DSS 3.2, the version of the standards in effect at the time of the data breach, sets forth detailed and comprehensive requirements that must be followed to meet each of the following twelve “high-level” mandates:

33. Among other things, PCI DSS required Coffee & Bagel Brands to:
- a. properly secure payment card data;
  - b. not store cardholder data beyond the time necessary to authorize a transaction;
  - c. maintain up-to-date antivirus software and a proper firewall;
  - d. restrict access to payment card data on a need-to-know basis;
  - e. establish a process to identify and timely fix security vulnerabilities;
  - f. assign unique identification numbers to each individual with access to their systems; and
  - g. encrypt payment card data at the point of sale.

34. Fourth, according to the Federal Trade Commission (“FTC”), the 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 Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45.

35. In 2007, the FTC published guidelines that establish reasonable data security

practices for businesses. The guidelines note businesses should:

- a. protect the personal customer information that they keep;
- b. properly dispose of personal information that is no longer needed;
- c. encrypt information stored on computer networks;
- d. understand their network's vulnerabilities; and
- e. implement policies for installing vendor-approved patches to correct security problems.

36. The guidelines also recommend that businesses consider:

- a. using an intrusion detection system to expose a breach as soon as it occurs;
- b. monitor all incoming traffic for activity indicating someone may be trying to hack the system;
- c. watch for large amounts of data being transmitted from the system; and
- d. have a response plan ready in the event of a breach.

37. The FTC also has published a document entitled "FTC Facts for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

38. The FTC has issued orders against businesses that failed to employ reasonable measures to secure customer data. These orders provide further guidance to businesses with regard to their data security obligations.

39. Fifth, several states have enacted data breach statutes that impose data

security obligations on merchants, such as the Minnesota Plastic Card Security Act, Minn. Stat. § 325E.64, or otherwise require merchants to use reasonable care to guard against unauthorized access to consumer information, such as California Civil Code § 1798.81.5(b) and Wash. Rev. Code § 19.255. States have also adopted unfair and deceptive trade practices acts, which prohibit unfair trade practices, including the failure to employ reasonable security processes to protect payment card data. Moreover, most states have enacted statutes requiring merchants to provide notice if their data security systems are breached. These statutes, implicitly or explicitly, support the use of reasonable data security practices and reflect the public policy of protecting sensitive customer data.

40. Coffee & Bagel Brands' failure to employ practices and procedures reasonably capable of securing the cardholder data of the members of Plaintiff and the Class violated all of these statutory- and industry-imposed obligations and caused substantial damage to Plaintiff and the Class.

41. Indeed, the fact that cardholder data was left exposed for over three months and the fact that Coffee & Bagel Brands continuously failed to detect this vulnerability demonstrates their complete lack of procedural and other safeguards with respect to their customers' data.

42. Plaintiff and the Class were required to act immediately to mitigate the massive fraudulent transactions being made on payment cards that they had issued, while simultaneously taking steps to prevent future fraud. Consumers are ultimately protected

from most fraud loss, but Plaintiff and Class members are not. Financial institutions bear primary responsibility for reimbursing members for fraudulent charges on the payment cards they issue.

43. Plaintiff suffered actual financial loss due to fraud on its cardholders' accounts.

44. As a result of the Coffee & Bagel Brands' data breach, Plaintiff and Class members have been forced to cancel and reissue payment cards, change or close accounts, notify members that their cards were compromised, investigate claims of fraudulent activity, refund fraudulent charges, increase fraud monitoring on potentially impacted accounts, and take other steps to protect themselves and their members. They also lost interest and transaction fees due to reduced card usage. Furthermore, debit and credit cards belonging to Class members and Plaintiff—as well as the account numbers on the face of the cards—were devalued.

45. The financial damages suffered by Plaintiff and members of the Class are massive and continue to increase.

46. As a result of the data breach, Plaintiff is incurring significant costs associated with, among other things, notifying members of issues related to the data breach, closing out and opening new customer/member accounts, reissuing members' cards, and/or refunding members' losses resulting from the unauthorized use of their accounts.

### CLASS ALLEGATIONS

47. Plaintiff brings this action on behalf of itself and all other similarly situated Class members pursuant to Rule 23(a), (b)(2) and (b)(3) of the Federal Rules of Civil Procedure and seeks certification of the following Class:

All banks, credit unions, financial institutions, and other entities in the United States (including its Territories and the District of Columbia) that issued payment cards (including debit or credit cards) used by consumers to make purchases from Defendants while malware was installed on their payment card systems.

48. Excluded from the Class are Coffee & Bagel Brands and their subsidiaries and affiliates; all employees of Coffee & Bagel Brands; all persons who make a timely election to be excluded from the Class; government entities; and the judge to whom this case is assigned and his/her immediate family and his/her court staff.

49. **Numerosity:** All requirements of Fed. R. Civ. P. 23(a)(1) are satisfied. The members of the Class are so numerous and geographically dispersed that individual joinder of all Class members is impracticable. While Plaintiff is informed and believes that there are thousands of members of the Class, the precise number of Class members is unknown to Plaintiff. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

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

- a. Whether Coffee & Bagel Brands engaged in the misconduct alleged;
- b. Whether Coffee & Bagel Brands owed a duty to Plaintiff and the Class members and whether Coffee & Bagel Brands violated that duty;
- c. Whether Plaintiff and the Class members were injured and suffered damages or other ascertainable loss as a result of Coffee & Bagel Brands' conduct; and
- d. Whether Plaintiff and the Class members are entitled to relief and the measure of such relief.

51. **Typicality:** All requirements of Fed. R. Civ. P. 23(a)(3) are satisfied. Plaintiff is a member of the Class, having issued payment cards that were compromised in the data breach of Coffee & Bagel Brands' data systems. Plaintiff's claims are typical of the other Class members' claims because, among other things, all Class members were comparably injured through Coffee & Bagel Brands' conduct.

52. **Adequacy:** All requirements of Fed. R. Civ. P. 23(a)(4) are satisfied. Plaintiff is an adequate Class representative because it is a member of the Class and its interests do not conflict with the interests of the other members of the Class that it seeks to

represent. Plaintiff is committed to pursuing this matter for the Class with the Class' collective best interests in mind. Plaintiff has retained counsel competent and experienced in complex class action litigation of this type, and Plaintiff intends to prosecute this action vigorously. Plaintiff and its counsel will fairly and adequately protect the Class's interests.

53. **Superiority:** The superiority requirement of Fed. R. Civ. P. 23(b)(3) is satisfied. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for members of the Class to individually seek redress for Coffee & Bagel Brands' wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

54. **Injunctive and Declaratory Relief:** All requirements of Fed. R. Civ. P. 23(b)(2) are satisfied. Coffee & Bagel Brands, through their uniform conduct, acted or



refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

## **COUNT I**

### **Negligence**

55. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

56. Coffee & Bagel Brands owed a duty to Plaintiff and the members of the Class to use and exercise reasonable and due care in obtaining, retaining, and securing cardholder data, and to provide security consistent with industry standards and requirements to ensure that their POS systems and networks adequately protected the personal and financial information of customers who used credit and debit cards issued by Plaintiff and members of the Class to make purchases and Coffee & Bagel Brands locations. This duty arises from multiple sources.

57. Coffee & Bagel Brands owed a duty to Plaintiff and the Class because it was foreseeable that Coffee & Bagel Brands' data systems and the cardholder data those data systems processed would be targeted by hackers. It also was foreseeable that such hackers would extract cardholder data from Coffee & Bagel Brands' systems and misuse that information to the detriment of Plaintiff and the Class members, and that Plaintiff and the Class would be forced to mitigate such fraud or such potential fraud by cancelling and reissuing payment cards to their members and reimbursing their members for fraud losses.

58. Coffee & Bagel Brands' duty also arises from the special relationship that existed between Coffee & Bagel Brands and the Class. Plaintiff and the Class entrusted Coffee & Bagel Brands with the cardholder data contained on the payment cards Plaintiff and the Class issued to their members. Coffee & Bagel Brands, as the holders and processors of that information, were the only parties who realistically could ensure that their data systems were sufficient to protect the data they were entrusted to hold.

59. Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, further mandated Coffee & Bagel Brands to take reasonable measures to protect the cardholder data. Section 5 prohibits unfair practices in or affecting commerce, which requires and obligates Coffee & Bagel Brands to take reasonable measures to protect any cardholder data Coffee & Bagel Brands may hold or process. The FTC publications and data security breach orders described above further form the basis of Coffee & Bagel Brands' duty. In addition, individual states have enacted statutes based upon the FTCA that also created a duty.

60. Coffee & Bagel Brands are also obligated to perform their business operations in accordance with industry standards, including the PCI DSS, to which Coffee & Bagel Brands are bound. The industry standards create yet another source of obligations that mandate Coffee & Bagel Brands to exercise reasonable care with respect to Plaintiff and the Class.

61. Coffee & Bagel Brands, by their actions, have breached their duties to Plaintiff and the Class. Specifically, Coffee & Bagel Brands failed to act reasonably in protecting the cardholder data of the members of Plaintiff and the Class members, and did not have reasonably adequate systems, procedures and personnel in place to reasonably prevent the disclosure and theft of the cardholder data of Plaintiff and the Class's members.

62. Upon information and belief, the specific negligent acts and omissions committed by Coffee & Bagel Brands include, but are not limited to, some or all of the following:

- a. failure to delete cardholder information after the time period necessary to authorize the transaction;
- b. failure to employ systems to protect against malware;
- c. failure to regularly update their antivirus software;
- d. failure to maintain an adequate firewall;
- e. failure to track and monitor access to their network and cardholder data;
- f. failure to limit access to those with a valid purpose;
- g. failure to encrypt cardholder data at the point-of-sale;
- h. failure to transition to the use of EMV technology;
- i. failure to conduct frequent audit log reviews and vulnerability scans and remedy problems that were found;
- j. failure to assign a unique ID to each individual with access to their systems;

- k. failure to automate the assessment of technical controls and security configuration standards;
- l. failure to adequately staff and fund their data security operation;
- m. failure to use due care in hiring, promoting, and supervising those responsible for their data security operations;
- n. failure to recognize red flags signaling that Defendants' systems were inadequate, and that as a result, the potential for a massive data breach was increasingly likely; and
- o. failure to recognize that hackers were stealing Customer Data from their network while the data breach was taking place.

63. In connection with the conduct described above, Coffee & Bagel Brands acted wantonly, recklessly, and with complete disregard for the consequences.

64. As a direct and proximate result of Coffee & Bagel Brands' conduct, Plaintiff and the Class members have suffered and continue to suffer injury, including but not limited to cancelling and reissuing payment cards, changing or closing accounts, notifying members that their cards were compromised, investigating claims of fraudulent activity, refunding fraudulent charges, increasing fraud monitoring on potentially impacted accounts, and taking other steps to protect themselves and their members. They also lost interest and transaction fees due to reduced card usage resulting from the breach, and the cards they issued (and the corresponding account numbers) were rendered worthless.

**COUNT II**

**Minnesota Plastic Card Security Act – Minn. Stat. § 325E.64**

65. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

66. Minn. Stat. § 325.64 is a Minnesota statute that specifically acknowledges Coffee & Bagel Brands' duty to safeguard transaction payment information owed to financial institutions such as Plaintiff and members of the Class.

67. Minn. Stat. § 325E.64, subd. 2, imposed a duty upon Coffee & Bagel Brands not to retain payment information from sales transactions for longer than 48 hours. The statute specifically requires that:

No person or entity conducting business in Minnesota that accepts an access device in connection with a transaction shall retain the card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data, subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction. A person or entity is in violation of this section if its service provider retains such data subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction.

68. Minn. Stat. § 325E.64, subd. 3 details a merchant's responsibilities should it breach the duties imposed by the statute, and then subsequently suffer a data breach. This subdivision provides that:

Whenever there is a breach of the security of the system of a person or entity that has violated this section, or that person's or entity's service provider, that person or entity shall reimburse the financial

institution that issued any access devices affected by the breach for the costs of reasonable actions undertaken by the financial institution as a result of the breach in order to protect the information of its cardholders or to continue to provide services to cardholders, including but not limited to, any cost incurred in connection with:

- (1) the cancellation or reissuance of any access device affected by the breach;
- (2) the closure of any deposit, transaction, share draft, or other accounts affected by the breach and any action to stop payments or block transactions with respect to the accounts;
- (3) the opening or reopening of any deposit, transaction, share draft, or other accounts affected by the breach;
- (4) any refund or credit made to a cardholder to cover the cost of any unauthorized transaction relating to the breach; and
- (5) the notification of cardholders affected by the breach.

The financial institution is also entitled to recover costs for damages paid by the financial institution to cardholders injured by a breach of the security of the system of a person or entity that has violated this section. Costs do not include any amounts recovered from a credit card company by a financial institution. The remedies under this subdivision are cumulative and do not restrict any other right or remedy otherwise available to the financial institution.

69. Coffee & Bagel Brands “conduct business” in the State of Minnesota.

70. Coffee & Bagel Brands regularly accept “access devices” (debit/credit cards) for the purpose of conducting their business.

71. Coffee & Bagel Brands violated Minn. Stat. § 325E.64 by retaining the card security code data, the PIN verification code number, and/or the full contents of Coffee & Bagel Brands’ customers’ magnetic stripe data in violation of the statute.

72. There was a breach of the security of Coffee & Bagel Brands’ systems.

73. As a direct and proximate result of Coffee & Bagel Brands' violation of Minn. Stat. § 325E.64, Plaintiff and members of the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

### **COUNT III**

#### **Negligence Per Se**

74. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

75. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or affecting commerce” including, as interpreted and enforced by the FTC, the unfair act or practice by retailers, restaurants, and other businesses such as Coffee & Bagel Brands of failing to use reasonable measures to protect cardholder data. The FTC publications and orders described above also form the basis of Coffee & Bagel Brands' duty.

76. Coffee & Bagel Brands violated Section 5 of the FTCA (and similar state statutes) by failing to use reasonable measures to protect cardholder data and not complying with applicable industry standards, including PCI DSS as described in detail previously in this complaint. Coffee & Bagel Brands' conduct was particularly unreasonable given the nature and amount of cardholder data they obtained and stored and the foreseeable consequences of a data breach at a national restaurant, including specifically the immense damages that would result to consumers and financial institutions.

77. Coffee & Bagel Brands' violation of Section 5 of the FTCA (and similar state statutes) constitutes negligence per se.

78. Plaintiff and the Class members are within the class of persons Section 5 of the FTCA (and similar state statutes) was intended to protect as they are engaged in trade and commerce and bear primary responsibility for reimbursing consumers for fraud losses. Moreover, Plaintiff and many Class members are credit unions, which are organized as cooperatives whose members are consumers.

79. The harm that has occurred is the type of harm the FTCA (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty 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 suffered by Plaintiff and the Class members.

80. Moreover, as described above, Coffee & Bagel Brands also violated Minn. Stat. § 325E.64 by improperly retaining the card security code data, the PIN verification code number, and/or the full contents of Coffee & Bagel Brands customers' magnetic stripe data from credit and debit cards issued by Plaintiff and members of the Class.

81. Plaintiff and members of the Class suffered harm, including, but not limited to, costs for reissuing credit/debit cards, changing or closing accounts, opening or reopening accounts, refunding or crediting cardholder accounts in response to fraudulent charges, issuing notice to potentially effected cardholders, and other actions necessary to



rectify, prevent and/or mitigate fraud as a result of Coffee & Bagel Brands' violation of Minnesota's Plastic Card Security Act, Minn. Stat. § 325E.64.

82. Plaintiff and members of the Class are entities that the Minnesota legislature intended to be protected by Minnesota's Plastic Card Security Act, Minn. Stat. § 325E.64.

83. The injuries suffered by Plaintiffs and members of the Class were directly and proximately caused by Coffee & Bagel Brands' violation of Minnesota's Plastic Card Security Act, Minn. Stat. § 325E.64.

84. Coffee & Bagel Brands' violation of the Minnesota's Plastic Card Security Act, Minn. Stat. § 325E.64, thus constitutes negligence per se.

85. As a direct and proximate result of Coffee & Bagel Brands' negligence per se, the Plaintiff and the Class have suffered and continue to suffer injury, including but not limited to cancelling and reissuing payment cards, changing or closing accounts, notifying members that their cards were compromised, investigating claims of fraudulent activity, refunding fraudulent charges, increasing fraud monitoring on potentially impacted accounts, and taking other steps to protect themselves and their members. They also lost interest and transaction fees due to reduced card usage resulting from the breach, and the cards they issued (and the corresponding account numbers) were rendered worthless. Plaintiffs and members of the Class are entitled to recover damages in an amount to be proven at trial.

**COUNT IV**

**Declaratory and Injunctive Relief**

86. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

87. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, which are tortious and which violate the terms of the federal and state statutes described herein.

88. An actual controversy has arisen in the wake of the data breach at issue regarding Coffee & Bagel Brands' common law and other duties to act reasonably with respect to safeguarding the cardholder data of the members of Plaintiff and the Class. Plaintiff alleges Coffee & Bagel Brands' actions in this respect were inadequate and unreasonable and Coffee & Bagel Brands deny such allegations. Additionally, Plaintiff continues to suffer injury as additional fraud and other illegal charges are being made on payment cards Plaintiff and the Class members have issued.

89. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

- a. Coffee & Bagel Brands owed and continue to owe a legal duty to secure their customers' personal and financial information—specifically including

information pertaining to credit and debit cards used by persons who made purchases at Defendants' locations—under the common law, Section 5 of the FTCA, Card Operating Regulations, PCI DSS standards, their commitments, and various state statutes;

- b. Coffee & Bagel Brands breached this legal duty by failing to employ reasonable measure to secure their customers' personal and financial information;
- c. Coffee & Bagel Brands' breach of their legal duty proximately caused the data breach; and
- d. Banks, credit unions, and other institutions that reissued payment cards and were forced to pay for fraudulent transactions as a result of the Coffee & Bagel Brands' data breach are legally entitled to recover the costs they incurred from Coffee & Bagel Brands.

90. The Court also should issue corresponding injunctive relief requiring Coffee & Bagel Brands to employ adequate security protocols consistent with industry standards to protect their customers' personal and financial information. Specifically, this injunction should, among other things, direct Coffee & Bagel Brands to:

- a. utilize industry standard encryption to encrypt transmission of cardholder data at the point-of-sale and at all other times;
- b. implement encryption keys in accordance with industry standards;

- c. implement EMV technology;
- d. consistent with industry standards, engage third party auditors to test their systems for weakness and upgrade any such weakness found;
- e. audit, test, and train their data security personnel regarding any new or modified procedures and how to respond to a data breach;
- f. regularly test their systems for security vulnerabilities, consistent with industry standards;
- g. comply with all PCI DSS standards pertaining to the security of their customers' personal and confidential information; and
- h. install all upgrades recommended by manufacturers of security software and firewalls used by Coffee & Bagel Brands.

91. If an injunction is not issued, Plaintiff will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach of Coffee & Bagel Brands' data systems. The risk of another such breach is real, immediate, and substantial. If another breach of Coffee & Bagel Brands' data systems occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

92. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Coffee & Bagel Brands if an injunction is issued. Among other things, if Coffee & Bagel Brands suffer another massive data breach, Plaintiff and the members of

the Class will likely incur hundreds of millions of dollars in damage. On the other hand, the cost to Coffee & Bagel Brands of complying with an injunction by employing reasonable data security measures is relatively minimal and Coffee & Bagel Brands have a pre-existing legal obligation to employ such measures.

93. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiff, the Class, and the millions of consumers whose confidential information would be compromised.

#### **PRAYER FOR RELIEF**

94. Wherefore, Plaintiff, on behalf of itself and on behalf of the other members of the Class, requests that this Court award relief against Coffee & Bagel Brands as follows:

- a. An order certifying the Class and designating Plaintiff as the Class Representative and its counsel as Class Counsel;
- b. Awarding Plaintiff and the proposed Class members damages with pre-judgment and post-judgment interest;
- c. Enter a declaratory judgment in favor of Plaintiff and the Class as described above;
- d. Grant Plaintiff and the Class the injunctive relief requested above;
- e. Awarding attorneys' fees and costs; and

f. For such other and further relief as the Court may deem necessary or appropriate.

**JURY TRIAL DEMANDED**

95. Plaintiffs hereby demand a jury trial for all of the claims so triable.

Dated: June 21, 2019

**CHESTNUT CAMBRONNE PA**

By /s/ Karl L. Cambronne \_\_\_\_\_  
Karl L. Cambronne (#14321)  
Bryan L. Bleichner (#0326689)  
Jeffrey D. Bores (#227699)  
17 Washington Avenue North, Suite 300  
Minneapolis, MN 55401-2048  
Telephone: (612) 339-7300  
Fax: (612) 336-2940  
kcambronne@chestnutcambronne.com  
bbleichner@chestnutcambronne.com  
jbores@chestnutcambronne.com

Karen Hanson Riebel  
Kate M. Baxter-Kauf  
**LOCKRIDGE GRINDAL NAUEN P.L.L.P.**  
100 Washington Ave. S., Suite 2200  
Minneapolis, MN 55401  
Telephone: (612) 339-6900  
Fax: (612) 339-0981  
khriebel@locklaw.com  
kmbaxter-kauf@locklaw.com

Brian C. Gudmundson, (MN Bar No. 336695)

Michael J. Laird (MN Bar No. 0398436)

**ZIMMERMAN REED LLP**

1100 IDS Center

80 South 8th Street

Minneapolis, MN 55402

Telephone: (612) 341-0400

Fax: (612) 341-0844

brian.gudmundson@zimmreed.com

michael.laird@zimmreed.com

Gary F. Lynch

**CARLSON LYNCH LLP**

1133 Penn Avenue, 5<sup>th</sup> Floor

Pittsburgh, PA 15222

Direct: 412.253.6307

Office: 412.322.9243

Fax: 412.231.0246

glynch@carlsonlynch.com

Arthur M. Murray

Caroline T. White

**MURRAY LAW FIRM**

650 Poydras Street, Suite 2150

New Orleans, Louisiana 70130

Telephone: (504) 593-6473

Fax: (504) 584-5249

amurray@murray-lawfirm.com

cthomas@murray-lawfirm.com

Joseph P. Guglielmo  
Erin G. Comite  
**SCOTT+SCOTT ATTORNEYS AT LAW LLP**  
230 Park Avenue, 17th Floor  
New York, NY 10169  
Telephone: (212) 223-6444  
Fax: (212) 223-6334  
jguglielmo@scott-scott.com  
ecomite@scott-scott.com

**ATTORNEYS FOR PLAINTIFFS**



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

Village Bank, on behalf of itself and all others similarly situated,

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

(c) Attorneys (Firm Name, Address, and Telephone Number) Chestnut Cambronne PA 17 Washington Avenue North, Suite 300 Minneapolis, MN 55401 (612) 339-7300

DEFENDANTS

Caribou Coffee Company, Inc., Bruegger's Enterprises, Inc., Einstein & Noah Corp., and Einstein Noah Restaurant Group, Inc.

County of Residence of First Listed Defendant (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, 2 U.S. Government Defendant, 3 Federal Question (U.S. Government Not a Party), 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)

- Citizen of This State, Citizen of Another State, Citizen or Subject of a Foreign Country, PTF DEF, 1 1, 2 2, 3 3, 4 4, 5 5, 6 6

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

Table with 5 columns: CONTRACT, REAL PROPERTY, TORTS, CIVIL RIGHTS, PRISONER PETITIONS, FORFEITURE/PENALTY, LABOR, IMMIGRATION, BANKRUPTCY, SOCIAL SECURITY, FEDERAL TAX SUITS, OTHER STATUTES. Includes various legal categories like Personal Injury, Real Property, and Labor.

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

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)(2) Brief description of cause: Violation of Minn. Stat. § 325E.64, Negligence

VII. REQUESTED IN COMPLAINT:

CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P. DEMAND \$ CHECK YES only if demanded in complaint: JURY DEMAND: Yes No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE DOCKET NUMBER

DATE 6/21/2019 SIGNATURE OF ATTORNEY OF RECORD /s/ Karl L. Cambronne

FOR OFFICE USE ONLY

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE

**INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44**

## Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading 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. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

- I. (a) Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.
- (b) County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)
- (c) Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".
- II. Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
- United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
- United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
- Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
- Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)
- III. Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.
- IV. Nature of Suit.** Place an "X" in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.
- V. Origin.** Place an "X" in one of the six boxes.
- Original Proceedings. (1) Cases which originate in the United States district courts.
- Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441. When the petition for removal is granted, check this box.
- Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
- Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
- Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
- Multidistrict Litigation. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407. When this box is checked, do not check (5) above.
- VI. Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service
- VII. Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
- Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
- Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.
- VIII. Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

**Date and Attorney Signature.** Date and sign the civil cover sheet.