UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

FEDERAL TRADE COMMISSION, Plaintiff, v. BLUESNAP, INC., a corporation, BLUESNAP PAYMENT SERVICES LTD, a corporation, RALPH DANGELMAIER, individually and as an officer of BLUESNAP, INC., and TERRY MONTEITH, individually and as an officer of BLUESNAP, INC., Defendants.	**Case No. _____** **COMPLAINT FOR PERMANENT INJUNCTION, MONETARY JUDGMENT, AND OTHER RELIEF**

Plaintiff, the Federal Trade Commission ("FTC" or "Commission"), for its Complaint alleges:

1. The FTC brings this action for Defendants' violations of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), and the Telemarketing Sales Rule ("TSR"), 16 C.F.R. Part 310. For these violations, the FTC seeks relief, including a permanent injunction, monetary relief, and other relief, pursuant to Sections 13(b) and 19 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §§ 53(b) and 57b, and

the Telemarketing and Consumer Fraud and Abuse Prevention Act ("Telemarketing Act"), 15 U.S.C. §§ 6101–6108.

SUMMARY OF THE CASE

2. Defendant BlueSnap, Inc. ("BlueSnap") is a global payment facilitator that enables businesses to accept debit and credit card payments from consumers. For years, BlueSnap—at the direction of two senior executives, Defendants Ralph Dangelmaier ("Dangelmaier") and Terry Monteith ("Monteith")—has knowingly processed payments for deceptive and fraudulent merchants.

3. For example, from 2016 through 2021, BlueSnap opened and maintained multiple merchant accounts for a deceptive debt relief telemarketing scam known as ACRO Services, among other names, which bilked consumers out of tens of millions of dollars. BlueSnap continued to process consumers' payments for ACRO Services despite repeated warnings and direct evidence that the operation was engaged in fraud.

4. In 2019, for instance, a payment processor told BlueSnap that it should look to close one of ACRO Services' merchant accounts due to excessively high chargebacks—over 30% in the last 30 days—but BlueSnap ignored this warning and kept the account open. Shortly thereafter, the account was placed in Visa's fraud monitoring program, where it remained for over a year and experienced fraud to sales ratios as high as 29% and 40% in some months, leading

Visa to issue a $75,000 fine in April 2021 due to excessive levels of fraud on the account. About two months before the fine, in February 2021, American Express emailed Monteith several times about this same account, instructing her to stop processing American Express transactions on the account due to high fraud rates and consumers reporting they were being scammed by the merchant. Also around April 2021, BlueSnap's Director of Fraud Strategy reported to Dangelmaier and Monteith that ACRO Services was making illegal, deceptive calls to consumers, that it was charging consumers' cards without authorization, and that a bank had sent an investigator to ACRO Services' headquarters because so many of the bank's credit cardholders had been defrauded by the company.

5. Despite these warnings and other obvious indicators of fraud, BlueSnap, Dangelmaier, and Monteith not only continued to facilitate payment processing for ACRO Services, they also actively helped the scam conceal its illegal activity and evade industry fraud monitoring programs. In April and May 2021, Dangelmaier told the scam's principals how to continue processing their deceptive charges under the radar through a shell company, directing them to apply for a merchant account for a "new" business and under a different principal's name. Dangelmaier and Monteith further aided the scam by helping the principals disguise and misrepresent their "new" business as a type of "education" service to evade heightened scrutiny by acquiring banks and card networks. BlueSnap

processed the scam's payments through the new account until BlueSnap's payment processing partner demanded the account be terminated after less than one month of suspicious processing activity. Undeterred by this termination, BlueSnap continued to allow—and Dangelmaier and Monteith even directed—ACRO Services to process transactions through yet another account that had not yet been terminated. BlueSnap did not stop processing for ACRO Services until July 2021, when its processing partner opened an investigation and forced BlueSnap to stop processing on all ACRO Services accounts.

6. Defendants' willingness to facilitate payment processing in the face of blatant warning signs and to conceal the true nature of their clients' unlawful business activity was not limited to ACRO Services. Defendants have repeatedly ignored warnings and direct evidence of fraud to keep processing for other deceptive and fraudulent merchants—including at least one merchant whose owner recently agreed to pay over $400,000 to New York's Attorney General to settle allegations that his companies were illegally advertising stalkerware to consumers. Defendants have repeatedly shown, in exchange for taking in higher fees, a willingness to tolerate excessive chargebacks stemming from fraudulent or deceptive practices.

7. Defendants' acts and practices have caused substantial harm to consumers by enabling fraudsters to circumvent industry rules and obtain and

maintain access to payment processing services. If Defendants had not concealed this fraudulent activity and turned a blind eye to repeated evidence of fraud, ACRO Services and other scammers would not have been able to process tens of millions of dollars in consumer payments.

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337(a), and 1345.

9. Venue is proper in this District under 28 U.S.C. §§ 1391(b)(2), (c)(2), (c)(3), and 15 U.S.C. § 53(b).

PLAINTIFF

10. The FTC is an independent agency of the United States Government created by the FTC Act, which authorizes the FTC to commence this district court civil action by its own attorneys. 15 U.S.C. §§ 41-58. The FTC enforces Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits unfair or deceptive acts or practices in or affecting commerce. The FTC also enforces the TSR, 16 C.F.R. Part 310, which prohibits deceptive and abusive telemarketing acts or practices.

DEFENDANTS

11. Defendant BlueSnap, Inc. is a California corporation with its principal place of business at 800 South Street, Suite 640, Waltham, Massachusetts 02453.

BlueSnap transacts or has transacted business in this District and throughout the United States.

12. Defendant BlueSnap Payment Services Ltd is a United Kingdom company with its principal place of business at 2 Sheraton St. Medius House, London UK W1F 8BH. BlueSnap Payment Services Ltd is a wholly owned subsidiary of BlueSnap, Inc. BlueSnap Payment Services Ltd transacts or has transacted business in this District and throughout the United States.

13. Defendant Ralph Dangelmaier was the Chief Executive Officer of BlueSnap from 2013 through 2023 and remains an advisor to BlueSnap. At all times relevant to this Complaint, acting alone or in concert with others, he has formulated, directed, controlled, had the authority to control, or participated in the acts and practices of BlueSnap and BlueSnap Payment Services Ltd, including the acts and practices set forth in this Complaint. Dangelmaier knew, consciously avoided knowing, or should have known that BlueSnap was processing for merchants that were engaged in fraudulent and deceptive conduct. He received numerous alerts and direct evidence that BlueSnap merchants were engaged in fraud, including warnings from his own employees. With ACRO Services in particular, he communicated directly with the scam's principals about the high rates of fraud on their accounts and various strategies to evade fraud controls and continue processing with BlueSnap. Dangelmaier, along with Monteith, made

decisions about whether to terminate or keep processing for merchants suspected of engaging in fraudulent activity. Dangelmaier, in connection with the matters alleged herein, transacts or has transacted business in this District and throughout the United States.

14. Defendant Terry Monteith is the Senior Vice President, Global Acquiring and Payments of BlueSnap. At all times relevant to this Complaint, acting alone or in concert with others, she has formulated, directed, controlled, had the authority to control, or participated in the acts and practices set forth in this Complaint. Monteith knew, consciously avoided knowing, or should have known that BlueSnap was processing for merchants that were engaged in fraudulent and deceptive conduct. She was responsible for risk management at BlueSnap, oversaw BlueSnap's fraud prevention team, and communicated frequently, if not daily, with fraud prevention staff. She also regularly communicated with payment processors and acquirers about merchants that were flagged for excessive chargebacks or fraud and that were placed on the card networks' fraud monitoring programs. Monteith personally received numerous alerts and direct evidence that BlueSnap merchants were engaged in fraud, including warnings from other BlueSnap employees. Monteith, along with Dangelmaier, made decisions about whether to terminate or keep processing for merchants suspected of engaging in fraudulent activity. Monteith, in connection with the matters alleged herein,

transacts or has transacted business in this District and throughout the United States.

COMMERCE

15. At all times relevant to this Complaint, Defendants have maintained a substantial course of trade in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

THE CREDIT CARD SYSTEM AND MERCHANT ACCOUNTS

The Role of Payment Facilitators in Payment Processing

16. BlueSnap is in the business of offering credit and debit card processing services to businesses and helping them establish merchant accounts with a financial institution (known as an "acquiring bank" or "acquirer") that is a member of the credit card networks (e.g., Visa and Mastercard). Without access to a merchant account through an acquirer, businesses are not able to accept consumer credit or debit card payments.

17. There are a number of entities that act as intermediaries between businesses (otherwise referred to as "merchants") and acquiring banks. These entities include payment processors, independent sales organizations, and payment facilitators.

18. Unlike other payment intermediaries, a payment facilitator often does not procure a separate merchant account for each of its merchant-clients. Instead,

the payment facilitator itself is a merchant registered by an acquirer to facilitate transactions on behalf of other merchants (sometimes referred to as sub-merchants). The payment facilitator typically receives settlement of transaction proceeds from the acquirer on behalf of each sub-merchant and disburses the funds to each sub-merchant. The payment facilitator enters into contracts with acquirers to provide payment services to sub-merchants, and it enters into a separate contract with each sub-merchant to enable payment acceptance. When a cardholder makes a purchase with a sub-merchant, the transaction typically gets processed through the payment facilitator's master merchant account.

19. In an effort to deter fraud, increase transparency, and reduce risk to the payment system, card networks impose operating rules and restrictions on registered members and third parties, including acquirers and payment facilitators.

20. The card networks' rules require payment facilitators to conduct due diligence before "onboarding" a merchant to ensure that the merchant is engaged in a legitimate business and screen out merchants engaged in potentially fraudulent or illegal activity. For example, Visa rules require that before entering into an agreement with a merchant, a payment facilitator must ensure that the prospective merchant is financially responsible and not engaged in any activity that could cause harm to the Visa system or the Visa brand, and the payment facilitator must determine that there is no significant derogatory background information about any

of the merchant's principals. Visa rules also require the payment facilitator to conduct an adequate due diligence review, including a site visit to the business premises or suitable alternative, to ensure that only legal transactions will be submitted by the merchant.

21. Card networks also prohibit the practice of processing credit card transactions through another company's merchant account, known as "credit card laundering." Many fraudulent merchants engage in credit card laundering to conceal their real identities from consumers, the acquiring bank, the card networks, or law enforcement. They may do this by creating shell companies that act as fronts, applying for merchant accounts in the names of the shell companies, and then laundering their own transactions through the shell companies' merchant accounts. They may also launder their transactions through an existing merchant account that purports to do another type of business. Laundering helps fraudulent merchants circumvent underwriting or monitoring criteria established by acquirers or payment processors—criteria they may be unable to satisfy under their own names if, for example, they previously have been flagged for excessive chargebacks or potential fraud.

22. After a payment facilitator "onboards" a merchant and starts facilitating payment processing for that merchant, card network rules require the

payment facilitator to monitor the merchant's sales transaction activity for indicators of fraudulent or deceptive activity.

Chargebacks and Fraud Monitoring Programs

23. One of the primary indicators of fraudulent or deceptive conduct on a merchant account is a high chargeback rate. Chargebacks occur when customers contact their credit card issuing bank to dispute a charge appearing on their credit card account statement.

24. When a customer successfully disputes a transaction through a chargeback, the merchant is required to refund the customer's money. If a payment facilitator's sub-merchant does not have sufficient funds to pay refunds to all the customers with successful chargebacks, the payment facilitator will be liable for the refunds.

25. To manage risk and minimize fraud, the card networks have developed formal programs to monitor merchant accounts with excessive chargebacks. Merchant accounts that trigger certain chargeback thresholds are subject to heightened monitoring requirements, and the card networks may impose fines or even terminate merchant accounts if the merchants' chargeback rates do not improve after being monitored under these programs.

26. For example, Visa monitors merchants through its Visa Dispute Monitoring Program ("VDMP") when the merchant has at least 100 disputes

(chargebacks) in a single month and the ratio of disputed transactions to total transactions (the "chargeback ratio") is 0.9% or higher. Visa also monitors merchants that generate an excessive level of fraud through the Visa Fraud Monitoring Program ("VFMP"). Visa places merchants on the VFMP when the merchant has or exceeds $75,000 in fraudulent transactions (i.e., transactions disputed due to fraud) in a single month and the ratio of sales from fraudulent transactions to total transactions (measured in dollars) is 0.9% or higher. Once a merchant is placed on either the VDMP or VFMP programs, the merchant remains on the program until its chargeback/fraud levels stay below the program thresholds for three consecutive months. Merchants who remain on the program for several months are typically assessed fines and required to submit a remediation plan explaining how they will reduce their chargebacks or reported fraud. If a merchant remains on the program for twelve months, the merchant may be permanently disqualified from processing transactions with Visa.

27. When a merchant is terminated by an acquirer for an adverse reason, the merchant is often added to a database maintained by Mastercard known as the Mastercard Alert to Control High-risk Merchants ("MATCH"). Reasons for adding a merchant to MATCH include excessive chargebacks, excessive fraud, laundering activity, bankruptcy, or violations of card network standards. Acquirers and payment facilitators are typically required to check whether a

prospective merchant is listed on MATCH when they perform their due diligence, and merchants who are listed on MATCH often have difficulty obtaining merchant accounts, as they are deemed to be too high risk by many acquirers and payment facilitators.

Restrictions on High-Risk Merchants

28. The card networks, acquirers, and other entities involved in payment processing impose additional restrictions on certain categories of merchants they deem to present a higher risk to the payment system. The highest-risk merchants, such as those engaged in illegal activity, are prohibited from processing any payments. Other merchants deemed to be high risk are subjected to heightened underwriting and monitoring requirements.

29. Merchants are typically classified as high risk based on the nature of the products or services they sell or the manner in which they sell them. Every entity involved in payment processing has slightly different rules regarding which merchants it considers to be high risk. In general, merchants with physical retail establishments that accept payments from customers in person ("card present" transactions) are considered to be much lower risk than merchants that process payments over the phone or the internet ("card not present" or "card absent" transactions). At various times during the relevant period, certain card network

rules have prohibited payment facilitators from offering payment services to merchants engaged in outbound telemarketing.

30. The card networks use the same four-digit merchant category codes ("MCCs") to classify the type of business in which a merchant is engaged. A merchant is assigned an MCC when it first obtains a merchant account, and card network rules require that merchants be assigned the MCC that most accurately describes their business. Proper MCC classification ensures that merchant accounts are subjected to the appropriate level of risk monitoring.

BLUESNAP'S ROLE IN PROCESSING PAYMENTS

31. BlueSnap advertises itself to merchants as an "all-in-one payment orchestration platform." BlueSnap tells merchants that, by signing a contract with BlueSnap, the merchant can quickly start accepting consumer card payments around the world due to the company's "expedited onboarding" and integrations with major banks and processors worldwide. BlueSnap also tells merchants that it actively manages their payments to optimize their returns—for example, by strategically routing a merchant's payments to particular banks or processors to maximize the merchant's transaction success rate (i.e., the number of successfully processed payments divided by the total attempted payments).

32. BlueSnap operates as a registered payment facilitator in the United States, Canada, Europe, and Australia. During the relevant time period, BlueSnap

has had agreements with multiple acquirers to act as a payment facilitator on behalf of sub-merchants in the United States. Each of these acquirers imposes various obligations on BlueSnap in acting as a payment facilitator, including the requirement that BlueSnap comply with all applicable card network rules and policies. BlueSnap also has relationships with multiple payment processors acting on behalf of acquirers, including Fiserv, Inc. (formerly known as First Data) ("Fiserv").

33. In addition to operating as a registered payment facilitator, BlueSnap offers a "merchant of record" service to merchants in which BlueSnap's subsidiary, BlueSnap Payment Services Ltd, acts as a "reseller" of the merchant's goods. BlueSnap has relationships with multiple payment processors and acquirers to process payments as a "merchant of record."

BlueSnap Fees

34. BlueSnap's revenues are driven primarily by the fees it charges its merchants. Like most payment facilitators, BlueSnap charges merchants a transaction fee for each payment transaction it facilitates. The transaction fee is typically calculated as a percentage of the transaction price plus a fixed amount (e.g., 2.9% plus $0.30 per card transaction). BlueSnap charges higher transaction fees for high-risk merchants.

35. BlueSnap also charges its merchants fees for each chargeback that a customer submits against a merchant account. If a merchant's chargeback ratio meets or exceeds 0.65% and the merchant has at least 75 chargebacks in a single month, BlueSnap places the merchant into its own "Excessive Chargeback Monitoring Program" and charges the merchant even higher chargeback fees, in some cases as much as $135 per chargeback.

36. To cover liabilities associated with potential chargebacks and refunds, BlueSnap often requires merchants, especially high-risk merchants, to deposit funds into a reserve account.

37. Given BlueSnap's fee structure, high-risk merchants with large amounts of chargebacks on their accounts, such as ACRO Services, generated significant revenues for BlueSnap.

BlueSnap's Obligations to Underwrite and Monitor Merchants

38. BlueSnap is required by card network rules and its agreements with acquiring banks and payment processors to conduct significant due diligence before it boards any new merchant and to monitor merchant traffic for potential signs of fraud or other problematic or suspicious activity.

39. For example, BlueSnap's agreement with Fiserv requires that before it processes any transactions for a sub-merchant, BlueSnap must conduct screening procedures and due diligence aimed at verifying the legitimacy of the sub-

merchant, understanding the sub-merchant's products or services and sales practices, and assessing the sub-merchant's ability to meet current and future obligations. Among other things, BlueSnap is required to take all necessary actions to verify that prospective sub-merchants are engaged in bona fide, lawful business operations, including confirming the nature of the sub-merchant's business, its products or services sold, the validity of the business entity, and its financial profile. Under its agreement with Fiserv, BlueSnap is required to establish policies and procedures for detecting and preventing its sub-merchants from engaging in conduct that violates state or federal law regarding unfair or deceptive acts or practices, or actions that violate the TSR or Section 5 of the FTC Act, as well as engagement in tactics to avoid fraud detection and monitoring. For sub-merchants that conduct business over the internet, BlueSnap must conduct thorough reviews of all websites used by the business to identify, among other things, signs that the business may be engaged in deceptive marketing practices. BlueSnap's own underwriting policy states that for sub-merchants that engage in telemarketing, BlueSnap must review the call scripts—which "should not be deceptive in any manner to the consumer"—and check that the sub-merchant is in compliance with the TSR, as well as all other applicable laws and regulations. Fiserv also requires BlueSnap to determine whether the sub-merchant or its principals have previously been terminated from payment processing, including by

checking for listings on MATCH.

40. Additionally, BlueSnap is required to classify the risk level associated with a prospective sub-merchant and conduct more stringent underwriting and back-end risk monitoring for merchants with higher risk profiles. Fiserv's industry risk classifications specify that merchants that sell by mail order or telephone should be classified as "high risk." Underwriting for high-risk merchants requires analysis of financial statements to determine creditworthiness and review of Better Business Bureau and other consumer complaint websites for evidence that the sub-merchant's business activity may result in a high level of chargebacks.

41. BlueSnap's agreement with Fiserv also requires BlueSnap to monitor the activity of its sub-merchants on an ongoing basis—consistent with the highest industry standards—to ensure that all transactions are being submitted in accordance with card network rules and applicable laws, to detect and deter unusual, fraudulent, or wrongful activity, and to fully mitigate risk and exposure to risk for all relevant parties. BlueSnap is required to notify Fiserv immediately if it becomes aware of any non-compliance or potential non-compliance by a sub-merchant with card network rules or applicable laws or if it learns that a sub-merchant is accepting transactions that do not constitute a bona fide sale of products or services by such sub-merchant.

42. For high-risk sub-merchants, BlueSnap is required to conduct ongoing reviews on at least an annual basis, with more frequent or ongoing reviews for high-risk merchants in poor financial condition or with excessive chargebacks or questionable processing history.

43. BlueSnap's agreements also require it to terminate processing for sub-merchants when the merchant account poses an unacceptable level of risk exposure. In determining whether to terminate a sub-merchant, BlueSnap is required to consider a variety of factors, including excessive levels of chargebacks and violations of card network rules or applicable laws.

THE ACRO SERVICES SCAM

44. From approximately 2016 until 2022, ACRO Services LLC and a series of related companies (collectively, "ACRO Services") perpetrated a deceptive telemarketing scheme selling bogus debt relief services to consumers. The principals behind the scheme—Sean Austin, John Steven Huffman, and John Preston Thompson (together, the "ACRO owners")—used multiple business entities and aliases to conduct its operations, including: American Consumer Rights Organization, Music City Ventures, Inc., also doing business as Tri Star Consumer Group; Thacker & Associates Int'l LLC; Nashville Tennessee Ventures, Inc.; First Call Processing LLC; Reliance Solutions, LLC; and Consumer Protection Resources, LLC.

45. To lure consumers into purchasing their services, ACRO Services' telemarketers falsely promised consumers that the company could eliminate or substantially reduce their credit card debt within 12 to 18 months. ACRO Services convinced consumers that their debt was invalid through various misrepresentations, including by telling consumers that credit card companies had over-charged them, that consumers qualified for a debt forgiveness program, or that creditors could not collect the debt based on federal laws such as the Fair Debt Collection Practices Act. ACRO Services also often falsely claimed that the company was affiliated with a bank, credit card company, or credit reporting agency in an effort to appear more legitimate.

46. ACRO Services charged consumers thousands of dollars each in upfront fees to join their "program," often charging one or more of their credit cards up to its credit limit. ACRO Services told consumers to stop making payments and to stop communicating with their credit card companies, deceiving them into believing that doing so would enable ACRO Services to eliminate or substantially reduce their credit card debt 12 to 18 months later. ACRO Services even told consumers that its hefty upfront fees would be part of the credit card debt that would be eliminated, meaning its services would essentially be free to the consumer.

47. In truth, ACRO Services did little or nothing to reduce consumers' credit card debt. Consumers who signed up for ACRO Services' program were left worse off, having paid substantial fees to ACRO Services for no reduction in their debt, ruined credit, and in many cases being sued by their credit card companies.

48. On November 7, 2022, the FTC sued the individuals and entities behind the ACRO Services scam for deceptive acts or practices in violation of Section 5 of the FTC Act and the TSR. The U.S. District Court for the Middle District of Tennessee entered a Temporary Restraining Order, which included a finding that the FTC had demonstrated a "strong likelihood of success on the merits." *FTC v. ACRO Servs. LLC*, Case 3:22-cv-00895 (M.D. Tenn. Nov. 21, 2022). In the Temporary Restraining Order and the following Stipulated Preliminary Injunction, the court froze the defendants' assets, appointed a receiver over the corporate entities, and enjoined defendants from further violating the FTC Act and the TSR. *See* Dkt. Nos. 26 (Nov. 21, 2022 Temporary Restraining Order), 49 (Dec. 13, 2022 Stipulated Preliminary Injunction). On April 28, 2023, the court entered stipulated orders imposing permanent injunctions and monetary judgments against the individual defendants. On August 9, 2023, the court entered a default judgment order imposing similar permanent injunctions and monetary judgments against the eight remaining entity defendants.

ACRO Services' Merchant Accounts with BlueSnap

49. Bluesnap processed ACRO Services' debt relief payments through at least three separate merchant accounts.

50. First, in August 2016, John Preston Thompson ("Thompson") applied for a merchant account with BlueSnap on behalf of the entity Thacker & Associates Int'l LLC ("Thacker"), located at 503A Ligon Drive in Nashville, Tennessee. The merchant application identified Thompson and John Steven Huffman ("Huffman") as co-owners of Thacker and indicated that the company had an annual sales volume of approximately $5 million. BlueSnap opened a merchant account for Thacker and began processing payments through this account in October 2016, assigning it an internal merchant ID number ("MID") of 1090909. At various times, BlueSnap identified the merchant for this account as Thacker & Associates (or a related alias such as "Thacker International"), Music City Ventures, Inc. ("Music City Ventures"), Tristar Consumer Group, and ACRO Services.

51. In February 2018, Thompson applied for another merchant account with BlueSnap on behalf of the entity Nashville Tennessee Ventures, Inc. ("Nashville Ventures"), also located at 503A Ligon Drive in Nashville, Tennessee. The merchant application identified Thompson and Huffman as co-owners, identified the DBA for the business as "Help4Timeshare Owners," and described

the services offered by Nashville Ventures as "Consultation for Timeshare Owners." BlueSnap opened a merchant account for Nashville Ventures and began processing payments through the account in March 2018, assigning it a MID of 1122444.

52. In May 2021, Huffman applied for a merchant account with BlueSnap on behalf of the entity First Call Processing LLC ("First Call Processing"), describing its business as "Consumer Protection Resources" and stating that the business was new to credit card processing. The application identified the address of the business as 530-B Harkle Road, Suite 100, Santa Fe, NM 87505, which is the office for a registered agent service. BlueSnap opened a merchant account for First Call Processing and began processing payments on this account in May 2021, assigning it a MID of 1253610.

53. When ACRO Services charged a consumer's credit card through one of these three merchant accounts, the statement would appear on the consumer's credit card statement under various billing descriptors, often preceded by a prefix such as "BLS*" or "BLN*" to indicate that the payment was facilitated by BlueSnap. Some of the descriptors that appeared on consumers' billing statements included "ACROSERVICES" and "RELIANCESOLUTIONS."

54. From 2016 through 2021, BlueSnap processed over $45 million through these three merchant accounts: Thacker (MID 1090909), Nashville Ventures (MID 1122444), and First Call Processing (MID 1253610).

DEFENDANTS' UNFAIR AND DECEPTIVE BUSINESS PRACTICES

55. BlueSnap routinely has provided payment processing services to merchants that were engaged in fraud or other deceptive or unlawful practices, enabling those merchants to bilk tens of millions of dollars from consumers and evade detection by card associations, consumers, and law enforcement. BlueSnap has done so despite glaring evidence that these merchants' business practices were problematic, including sky-high chargeback rates, consumer complaints, and warnings from its payment processing partners.

56. For years, BlueSnap conducted cursory underwriting reviews of prospective merchants, knowing that it could later terminate fraudulent merchants who generated excessive chargebacks after those merchants had paid thousands of dollars in fees to BlueSnap. But BlueSnap repeatedly failed to terminate merchants even after they were placed on fraud monitoring programs, instead choosing to keep processing and making money off of these merchants until it was forced to stop processing by the card networks or its processing partners.

57. BlueSnap employed a fraud prevention team with multiple fraud analysts and a manager who were responsible for investigating merchants with

high chargeback ratios and other indicators of fraud. The fraud prevention team frequently reported its concerns about fraudulent merchants to Monteith, who oversaw the team in her role as Vice President of Product, Payments, and Risk (which later changed to the title Vice President of Global Acquiring and Payments), and to Dangelmaier. In almost all instances, Monteith and Dangelmaier had to give their approval before BlueSnap would terminate a fraudulent merchant. For merchants that generated lots of revenue for BlueSnap (such as ACRO Services), Monteith and Dangelmaier frequently refused to terminate processing despite objections and concerns raised by the fraud prevention team.

I. DEFENDANTS' PROCESSING FOR ACRO SERVICES

58. Defendants' actions in facilitating payments for fraudulent merchants are clearly illustrated with respect to ACRO Services, which was one of BlueSnap's most profitable merchants. As detailed below, Defendants knew or consciously avoided knowing that ACRO Services and the ACRO owners were engaged in deceptive telemarketing and defrauding consumers. Yet Defendants time and again disregarded warnings and continued processing for ACRO Services. Even worse, Defendants took affirmative steps to launder ACRO Services' payments and conceal the true nature of ACRO Services' business so that they could continue processing for the scheme.

A. BlueSnap Provided Payment Processing for ACRO Services Despite Glaring Warnings It Was Engaged in Deceptive or Unlawful Conduct

1) Defendants Ignored Consumer Complaints and the Problematic Backgrounds of ACRO Services' Principals

59. Throughout the time that BlueSnap facilitated payment processing for ACRO Services, BlueSnap ignored consumer complaints and other evidence that its various affiliated entities and the ACRO owners were engaged in deceptive and unfair business practices—including other scams beyond just debt relief.

60. For example, BlueSnap knew before opening the Nashville Ventures (DBA Help4Timeshare Owners) account that consumers had reported being scammed by businesses with the same name when trying to cancel their timeshares. In 2018, when BlueSnap was conducting underwriting for the Nashville Ventures merchant account application, BlueSnap searched for "Nashville Ventures" online and found several consumer complaints about companies named "Help For [T]imeshare [O]wners," "Help4TSO," and "Helping Timeshare Owners" on a website titled "Ripoff Report" (www.ripoffreport.com). BlueSnap included this Ripoff Report in its underwriting file, which featured the following complaints from consumers:

- "They charge $1200.00 for nothing. They claim to cancel contracts. No transfers at all! This company is scum!"
- "SCAM ALERT! BEWARE . . . . They charge thousands of dollars knowing[] they cannot cancel your Timeshare."

- "When your company guaranteed me they could get my timeshare contract terminated, I paid your company 2-1/2 years ago to do that. I am now years down that road and still get demands for payment, reportings [sic] on my credit report and can't even get my account representative to contact me back."

61. In the same underwriting file, BlueSnap included documents showing Nashville Ventures doing business as or being affiliated with the names "Help for Timeshare Owners," "Helping Timeshare Owners," and "Help4TSO."

62. In addition, BlueSnap's underwriting and risk management policy states that all merchant account applications are reviewed for reputational risk, including searches on LexisNexis and searches for ongoing or concluded legal actions. The policy also states that higher risk merchants—which would include ACRO Services based on its business model and high chargeback levels—are subject to enhanced ongoing monitoring after they have gone through underwriting and started processing. Enhanced ongoing monitoring specifically includes internet searches for lawsuits.

63. ACRO Services' various entities and its three principals were sued several times for deceptive and fraudulent acts while BlueSnap opened merchant accounts for them and continued processing for them. For example:

a. In 2017, a consumer filed suit in Pennsylvania against Thacker regarding unsolicited telemarketing calls offering debt relief services, including allegations that Thacker's sales agents were claiming their "government-approved

program could reduce your debt by thousands of dollars, and allow you to become financially free." Complaint at 2, *Abramson v. Thacker & Assocs. Int'l, LLC*, No. AR-17-001419 (Pa. Ct. C.P. Allegheny Cty. Mar. 20, 2017).

b. In 2017, developers of timeshare resorts and homeowners' associations sued Austin for violations of the law related to a deceptive timeshare cancellation scam. *See* Complaint, *Westgate Resorts, Ltd. v. Castle Law Grp., P.C.*, No. 6:17-cv-01063 (M.D. Fla. Jun. 12, 2017).

c. In 2018, timeshare companies sued Nashville Ventures for similar violations of law related to a deceptive timeshare cancellation scam. *See* Second Amended Complaint, *Diamond Resorts Int'l, Inc. v. Orlando Ventures, Inc.*, No. 6:17-cv-01771 (M.D. Fla. Oct. 8, 2018).

d. In early 2019, a company in the timeshare business sued Huffman, Thompson, and Nashville Ventures for breach of contract, including claims that Huffman and Thompson had committed fraud by diverting corporate funds for their personal use. *See Huffman v. Lonestar Transfer, LLC*, No. 05-20-00717-CV, 2021 WL 1608472 (Tex. App. Apr. 26, 2021) (referencing the original lawsuit filed in 2019).

e. In May 2019, a consumer sued American Consumer Rights Organization (another of the entities used to perpetrate ACRO Services' debt relief scheme) alleging that he had received unsolicited phone calls and a contract

attempting to persuade him to pay thousands of dollars to enroll in a program to "assist in resolving [his] unvalidated debt." Complaint at Ex. A, *Aussieker v. Nelson*, No. 2:19-CV-0868 (E.D. Cal. May 15, 2019). That lawsuit also named as a defendant "BLS Tristar Consumer Group," which was one of the billing descriptors that BlueSnap used when it processed payments for ACRO Services. BlueSnap knew that "Tristar Consumer Group" was a business alias for Music City Ventures as well as Thacker.

f. In early 2020, the same consumer who had filed suit against Thacker in 2017 filed another suit in Pennsylvania against Music City Ventures regarding similar unsolicited debt relief calls. *See* First Amended Complaint, *Abramson v. Am. Consumer Rights Org.*, No. AR-19-001446 (Pa. Ct. C.P. Allegheny Cty. Feb. 11, 2020).

g. In March 2020, all three of the ACRO owners were named as defendants along with Music City Ventures and Thacker in a lawsuit filed by a consumer alleging violations of the Telephone Consumer Protection Act and West Virginia consumer protection law in connection with debt relief telemarketing calls she had received. *See* First Amended Complaint, *Mey v. Castle Law Grp., P.C.*, No. 5:19-CV-185 (N.D. W. Va. Mar. 2, 2020). The consumer alleged that the defendants had falsely claimed to be affiliated with her credit card company and sent her a contract for "Unsecured Debt Validation" purporting to charge her a fee

of over $2,000. The court subsequently found that the calls at issue were misleading and entered a default judgment.

h. In September 2020, a consumer filed suit against Tri Star Consumer Group (a known DBA for Thacker) alleging that the company fraudulently induced her to enroll in a program to eliminate her credit card debt through the use of multiple misrepresentations about the nature of the services offered. *See* Complaint, *Ziegelbauer v. Tri Star Consumer Grp.*, No. 2020CV001808 (Wis. Cir. Ct. Dane Cty. Sep. 1, 2020).

64. All of these lawsuits were public records, and per its own policies, BlueSnap was required to regularly search for these records as part of enhanced ongoing monitoring of a higher risk merchant like ACRO Services. BlueSnap's fraud prevention team even notified Monteith about one of these lawsuits right before BlueSnap opened the First Call Processing account. Despite these lawsuits, as well as the online consumer complaints, BlueSnap continued processing for ACRO Services and its principals.

2) BlueSnap Kept Processing for ACRO Services Despite Excessive Chargeback Levels for Over a Year

65. From at least 2019 through 2021, the merchant accounts used by ACRO Services were repeatedly flagged for astronomical chargeback rates and placed into formal fraud monitoring programs.

66. In late 2019, the chargeback rates for ACRO Services were so high that Fiserv recommended that its merchant account be closed. In an email about "BlueSnap-Problem Merchants" dated December 10, 2019, a Fiserv official told Monteith: "I have been notified by the Credit/Risk Team the below merchants under BlueSnap Single-MID have been flagged for poor processing and should look[] to be closed." The email listed two merchant accounts with excessive chargeback rates: (1) "BLS*ACROServices" and (2) "BLS*POWERLINEGROUP." The chargeback rate for the ACRO Services account was listed as 30.21% over the past 30 days—***more than thirty times*** the threshold required to trigger chargeback monitoring programs. The chargeback rate for the Powerline Group account (which is discussed more in Paragraphs 116-118 and was the subject of the New York Attorney General action mentioned above in Paragraph 6) was also far above that threshold, at 6.39%. Despite this warning from Fiserv, BlueSnap continued processing for ACRO Services.

67. The following month, the chargeback rate on the ACRO Services account (the Thacker account with MID 1090909) increased to 33%—meaning nearly one out of every three ACRO Services customers disputed the charges. When Fiserv questioned BlueSnap about these exorbitant chargeback rates, BlueSnap reassured Fiserv that "[w]e have been working directly with this merchant on a chargeback reduction plan."

68. Despite BlueSnap's purported efforts, the Thacker merchant account continued to generate excessive chargebacks, and BlueSnap continued to process its transactions. In March 2020, Fiserv emailed several BlueSnap employees, including Monteith, directing them to review ten merchants with high chargeback and refund rates and advise about measures they were taking to mitigate these risks. Fiserv stated in the email that "[t]wo of these merchants are particularly concerning" and listed ACRO Services as one of them. A few days later, Fiserv again emailed Monteith and other BlueSnap employees about merchants with excessive chargebacks, including ACRO Services, and stated: "BlueSnap will need to address all of these merchants[,] which will include terminating many of them by month-end."

69. That same month, March 2020, Visa placed the account on the Visa Fraud Monitoring Program, citing "excessive Visa fraud that occurred in February" including "30 fraud transactions totaling $88,246.11 and a fraud to sales ratio of 17.24%"—far exceeding the VFMP threshold ratio of 0.90%. Over the next 14 months, from March 2020 through May 2021, the Thacker account remained on the VFMP due to consistently high fraud rates—with some months reaching a fraud to sales ratio as high as 29% and 40%. During this time, Fiserv sent over a dozen emails to Monteith and other BlueSnap employees about this account remaining on the VFMP month after month.

70. As part of the VFMP, ACRO Services was required to submit multiple remediation plans explaining how it was addressing consumers' fraud complaints and making efforts to reduce chargebacks. Between June 2020 and March 2021, Monteith reviewed and signed at least 5 such remediation plans on behalf of ACRO Services. In those plans, Monteith identified the merchant as "BlueSnap on behalf of Acro Services (Music City Ventures)" and identified the principals as "Ralph Dangelmaier, CEO (BlueSnap), John Steven Huffman, John Preston Thompson."

71. While the Thacker account remained on VFMP, the Nashville Ventures account (MID 1122444) also was in trouble. In December 2020, Fiserv notified Monteith that both the Nashville Ventures account and the Thacker account had been flagged for excessive chargebacks and refunds for the previous month, with chargeback rates (measured in dollars) of 20% and 14%, respectively. With respect to the Nashville Ventures account, BlueSnap responded, "Merchant encountered URL and fraud issues. BS has been in constant contact with the merchant, working with them in resolving their issues." BlueSnap did not explain how a merchant that makes sales to consumers over the phone could experience a spike in chargebacks due to "URL" issues. Moreover, despite its assurances to Fiserv, BlueSnap failed to take action to stop these merchant accounts from causing excessive chargebacks and further harm to consumers.

72. Again, the high chargebacks on the Nashville Ventures account persisted. By March 2021, the Nashville Ventures account had qualified for placement on the VFMP, and BlueSnap was notified that it must submit a remediation plan for that account as well when it entered its second month on the VFMP.

73. In April 2021, Visa imposed a $75,000 fine on the acquirer, Santander Bank, under the VFMP due to excessive levels of fraud on the Thacker account. Fiserv subsequently notified BlueSnap that it would be responsible for paying this fine. Despite notice of this fine, BlueSnap did not terminate the Thacker account, the Nashville Ventures account, or its relationship with ACRO Services.

3) Defendants Disregarded Direct Evidence that ACRO Services Was Engaged in Deceptive and Unlawful Conduct

74. In addition to all the warnings from sky-high chargebacks and mandatory fraud monitoring programs, Defendants were presented with direct evidence that ACRO Services was defrauding customers and engaging in unlawful activity.

75. For example, when Monteith was reviewing and signing VFMP remediation plans on behalf of ACRO Services, she reviewed direct evidence that the company was engaged in unlawful and deceptive practices in connection with the sale of debt relief services via telemarketing. Among other things, Monteith saw references to the ACRO Services website and a copy of a purported ACRO

Services customer agreement, which together betrayed the deceptive nature of the business.

76. The website and customer service agreement contradicted each other and even contradicted themselves. For example, ACRO Services' website claimed that the company "provide[d] financial coaching" with coaches "certified through the National Association of Certified Credit Counselors," but the customer agreement made no mention of financial coaching. The website advertised, "Need Debt Relief? ACRO Services LLC is Your Life Boat," but the customer agreement stated that it was "not for [] Debt Relief Services." The agreement further stated that "[t]he Company is experienced in disputing debts using federal and state statutory authority" and made misleading claims about consumers' ability to "invalidate" their debts using "statutory authority." The agreement also included contradictory claims regarding legal representation, at one point describing the scope of "Legal Services" provided and what the consumer owed for "Legal Fees, Costs, and Expenses," while elsewhere stating that "[t]he Company is not a law firm" and that it provides "No Legal Work." Finally, the agreement clearly disclosed that ACRO Services was charging advance fees for debt relief services, which is a violation of the FTC's TSR. *See* 16 C.F.R. § 310.4(a)(5)(i).

77. In addition to Monteith reviewing ACRO Services' deceptive and self-contradictory materials, she received multiple emails from American Express

about ACRO Services reportedly scamming consumers. At least four times during February 2021, American Express sent emails to Monteith about the Thacker account (with MID 1090909), each one noting that "[m]ultiple Cardholder[s] are stating this merchant scammed them" and that "11% of approved charges at this merchant have been claimed fraud since Sep[tember] 2020." In each email, American Express stated that it was "requiring cancellation of this account within 48 hours." BlueSnap only stopped processing American Express transactions on the Thacker account on March 1, 2021, nearly a month after first being requested to do so.

78. BlueSnap's fraud prevention team also obtained direct evidence of consumers being deceived by ACRO Services, including at least one recording of a telephone conversation between an ACRO Services representative and a consumer. In the recording, the ACRO Services representative told the consumer that they could "invalidate" the consumer's credit card debt—an utterly bogus claim. The representative also told the consumer they could provide this service after charging over $1,200 to the consumer's card, which is an illegal advance fee. This recording was consistent with information BlueSnap's fraud prevention team had gathered from chargeback documentation as well as consumer complaints online. For each chargeback or refund a consumer requested, BlueSnap received the "reason code" for that request. Many of the chargeback and refund requests for

ACRO Services, especially in 2020 and 2021, had reason codes reported as "fraudulent transaction," "unauthorized transaction," "product not as advertised," "product not received," or other fraud-related reason codes. BlueSnap's fraud prevention team also reviewed consumer complaints from online sources such as the Better Business Bureau. For instance, the Better Business Bureau webpage for ACRO Services (also doing business as American Consumer Rights Organization) displays numerous consumer complaints (including complaints submitted in 2020 and 2021) about the company's deceptive promises to resolve or remove their credit card debt, such as the following:

- "This company ruin my credit, when they were suppose to fix it, and take care of debt. I have been dealing with these people for almost two years, they take your money and make promises they cannot keep, it been a horror show ever since . . . ."

- "This is the most deceptive company ever. After being bombarded with heavy telemarketing on January 28, 2021[,] I very reluctantly signed up for ACRO Services LLC. They promised to remove all my credit card debt with little to no effect on my credit score for $8050.00. . . . They will not answer or call you back as they promise once they have your money. I am now forced to have more stress in trying to get my money back."

- "They charged my credit card $2930 for 'credit coaching' & acting in my behalf to creditors to settle the debt. They advised me not to let the creditors know I was working with them. . . . The only thing I have on credit is now this $2930 for something I never needed or understood what it was really for."

79. BlueSnap's fraud prevention team also gathered more damning, direct evidence of fraud and deception from the ACRO owners themselves. On March 31, 2021, a fraud investigator from Synchrony Bank made an unannounced visit to ACRO Services' headquarters in Nashville to inquire about millions of dollars in disputed charges involving Synchrony cardholders. The ACRO owners then reported the incident to BlueSnap's Director of Fraud Strategy, confessing that they misled the investigator about the owners not being present. The Fraud Director then sent an email to Monteith and Dangelmaier warning them about "multiple indicators and flags" that ACRO Services (also referred to as "TriStar") could "get shut down for illegal activity." In the email, the Fraud Director explained to Monteith and Dangelmaier that Synchrony Bank "wanted documents related to multiple customers that were recently told by TriStar to charge $10K onto their credit cards for the AcrosServices [sic] fee, then were instructed to never pay the credit card back so the bank is forced to close it and write it off as a loss, or have the customer include it in a bankruptcy." He further reported that he had listened to customer call recordings with ACRO Services, where he "heard them purposely speak fast and make it confusing for senior citizens, one of which did not give his authorization to make the purchase."

80. After this email, Dangelmaier and Monteith both told the Director of Fraud Strategy that ACRO Services was an important client for the company and they needed to work closely with them so they could continue processing.

4) BlueSnap Did Not Stop Processing for ACRO Services Until It Was Forced to Do So

81. Despite awareness of the rampant fraud occurring on ACRO Services' merchant accounts, BlueSnap continued to process its unlawful charges and continued to make money off the high fees charged to ACRO Services. BlueSnap only stopped processing for ACRO Services when other payment processors and credit card networks forced it to stop.

82. As described above, starting on February 4, 2021, American Express emailed Monteith and requested that BlueSnap cancel processing on the Thacker account "within 48 hours" due to high levels of fraud and reports of consumers being scammed. Despite the urgent nature of this request, Monteith did not immediately respond, and American Express had to follow up at least three additional times with her. BlueSnap did not stop processing Thacker transactions for American Express until about a month later, on March 1.

83. Several months later, on May 11, Fiserv notified Monteith that Discover was requesting termination of all Discover card processing for ACRO Services. Fiserv reported the reason for termination as follows: "This merchant is prohibited business type 'Deb[t] Consolidation' as well as a 15% Dispute rate.

Due to violation of ops regs, as well as merchant considered outside our risk tolerance. We are requesting to remove Discover Acceptance."

Still, BlueSnap did not completely stop processing for ACRO Services until Fiserv finally ordered it to do so in July 2021.

84. BlueSnap's failure to terminate merchants in these circumstances flies in the face of industry standards for fraud reporting and merchant termination. For example, in August 2019, Huffman and Thompson submitted a merchant application on behalf of Music City Ventures (one of the entities affiliated with ACRO Services) to another processing entity called Merchant Industry. After just two months of processing activity, Merchant Industry terminated the ACRO-affiliated entity's merchant account and placed it on the MATCH list with the reason code "03-Laundering." In other words, it took just a few months for another payments company to determine that ACRO Services was fraudulent and to terminate its processing. By contrast, Defendants facilitated the ACRO Services scam for years by disregarding such evidence of fraud and actively enabling the company to evade industry controls.

B. Defendants Took Deliberate Actions to Provide False Merchant Account Information and Hide the True Nature of ACRO Services' Business

1) Defendants Misrepresented ACRO Services as a Lower Risk Business to Avoid Scrutiny from Fiserv and Card Networks

85. Over the course of doing business with ACRO Services, BlueSnap knew ACRO Services was engaged in outbound telemarketing—a business category that card networks have deemed to be high risk or otherwise prohibited payment facilitators from servicing at all. Yet BlueSnap knowingly misclassified ACRO Services' merchant accounts as generic, lower-risk business categories to evade card network rules, increased scrutiny, and fraud monitoring. Monteith, for example, signed and submitted multiple remediation plans on behalf of ACRO Services to Visa, where she represented that ACRO Services was not a high-risk business, even though the very remediation plans demonstrated that this was false.

86. Major card networks require that merchants are assigned the merchant category code ("MCC") that reflects their primary business and most closely describes the goods or services sold. This is an ongoing requirement that extends beyond the initial signing of a merchant. For example, Visa rules state that acquirers or their agents must provide to Visa a merchant's primary and secondary MCCs, and that this information must be accurate and updated whenever there are changes. American Express rules state that payment facilitators must monitor merchants on an ongoing basis to ensure that they are not engaged in prohibited

merchant industries, and that a payment facilitator must assign a new, correct MCC if it determines that an MCC was incorrectly assigned at the time of signing.

87. Furthermore, Visa rules make clear that merchants are to be assigned the "miscellaneous" MCCs usually ending in "99"—which act as a sort of catch-all category—only if there is no MCC specific to the merchant's business.

88. BlueSnap assigned miscellaneous MCCs to all three merchant accounts for ACRO Services, even though there was at least one MCC specific to its business: "MCC 5966—Direct Marketing—Outbound Telemarketing Merchants." Mastercard rules describe this MCC as "initiat[ing] direct contact with consumers to sell products and services." Visa rules describe this MCC as "sell[ing] a variety of products using outbound telemarketing methods, where the merchant initiates contact with prospective buyers via telephone . . . ." Notably, Visa rules state when MCC 5966 is required to be used:

> Direct marketing and wholesale club MCCs describe how the merchant conducts its business rather than what the merchant sells or provides. For example, a direct marketing merchant sells through catalogs, brochures, telemarketing, direct mailings, etc and conducts card-absent transactions. **A direct marketing merchant can sell any type of product or service physical or digital to consumers but must use a direct marketing MCC**.

(emphasis added). BlueSnap's internal Underwriting & Risk Management Policy—which BlueSnap submitted to its processing partners as evidence of its policies and procedures—also explains that MCC 5966 applies to the "[s]ale of

products or services using outbound telemarketing such as unsolicited tech support desks or credit card protection."

89. Notably, Visa considers any merchant processing card-absent transactions under MCC 5966 to be a "high-brand risk" merchant subject to heightened underwriting and monitoring requirements. Among other things, high-brand risk merchants must be registered as such with Visa, and BlueSnap is required to provide reports on their monthly transaction activity. If a high-brand risk merchant is placed on the Visa Fraud Monitoring Program, Visa rules dictate that the merchant be placed on a "High Risk/Excessive" timeline with accelerated deadlines and more severe fines compared to the "Standard" VFMP timeline that applies to other merchants.

90. As shown above, Defendants knew that ACRO Services was engaged in outbound telemarketing, and therefore all three of its accounts should have been assigned the 5966 MCC or some other MCC that more closely identified the high-risk nature of its business.

91. Instead, contrary to the card rules and its own underwriting policies, BlueSnap assigned the following miscellaneous MCCs to ACRO Services' merchant accounts:

a. Thacker: MCC 7399 ("Business Services Not Elsewhere Classified")

b. Nashville Ventures: MCC 7299 ("Other Services–Not Elsewhere Classified")

c. First Call Processing: MCC 8299 ("Schools And Educational Services–Not Elsewhere Classified")

92. None of these MCC's are considered high-risk MCCs by the card networks. By assigning incorrect miscellaneous MCCs—and failing to correct these misclassifications over the years—BlueSnap enabled these merchant accounts to evade additional scrutiny and potentially greater penalties from the card networks.

93. This fact was well-illustrated when the Thacker account was placed on the VFMP. In March 2020, after the Thacker account had been flagged for excessive fraud charges (with an over 17% fraud-to-sales ratio), Visa placed it on the VFMP. However, instead of placing the account on the High-Risk VFMP timeline (as Visa rules dictate for merchants with high-risk MCCs), Visa placed it on the Standard VFMP timeline. At this time and repeatedly thereafter, Fiserv told BlueSnap that a merchant should be placed in the High-Risk VFMP timeline if it is categorized with a high-risk MCC code as defined by Visa rules, including MCC 5966. Despite these emails and knowing that ACRO Services was engaged in outbound telemarketing, BlueSnap took no action to correct the MCC for the Thacker account. If the Thacker account had been correctly classified as a high-

risk MCC and placed on the High-Risk VFMP timeline, the Thacker account would have faced much higher fines and would have drawn higher scrutiny from the acquirer than under the Standard VFMP timeline.

94. Monteith perpetuated this deception by submitting multiple VFMP remediation plans to Visa, via Fiserv, in which she falsely represented that the Thacker account was not a high-brand risk MCC. From June 2020 to January 2021, Monteith signed at least five remediation plans on behalf of the Thacker account (identified as ACRO Services), and in all of them she marked "No" next to the field "High-Brand Risk MCC," even though she knew ACRO Services was engaged in the high-risk business of outbound telemarketing. She showed as much when, in each of these plans, she checked the boxes for "Outbound Telemarketing" and "Inbound Telemarketing" next to the field "Business Model."

95. Ultimately, the Thacker account remained on the Standard VFMP timeline until Visa imposed its $75,000 fine after the account exceeded 12 months on the VFMP—as opposed to BlueSnap being fined multiple times and as early as Month 1 on the program if the account had been correctly placed in the High-Risk VFMP timeline.

2) Defendants Helped ACRO Services Create a Merchant Account for a Shell Company

96. After the Thacker account had remained on the VFMP for so many months due to excessive fraud charges, Defendants anticipated that they may be

forced to shut down the account and looked for ways to keep ACRO Services processing under the radar.

97. In April and May 2021, Dangelmaier had multiple calls with the ACRO owners in which they discussed the exorbitant chargeback rates on the Thacker account, its placement on the VFMP, and Discover's request to terminate all processing for ACRO Services. During these calls, Dangelmaier instructed the ACRO owners to obtain a new merchant account at BlueSnap under a different business and different owner's name, which they could use to continue processing payments if other accounts such as the Thacker account were required to be terminated in light of the VFMP. Dangelmaier also instructed BlueSnap employees, including Monteith, to use a different business descriptor when processing the merchant application for this "new" business, directing them to classify the business as providing educational services rather than debt-related services. Dangelmaier further directed Monteith to make sure that the new merchant account went through the underwriting process and was approved as quickly as possible.

98. Following Dangelmaier's direction, the ACRO owners applied for a new merchant account with BlueSnap on behalf of a shell company called "First Call Processing." The merchant application listed Huffman as the owner,

described the business as "Consumer Protection Resources," and identified the business category as "Education."

99. First Call Processing was a continuation of the ACRO Services debt relief scam, just under a different name. For example, one of the documents the ACRO owners submitted to BlueSnap as part of the merchant application was an ambiguously worded "engagement agreement" between First Call Processing and an entity called Consumer Protection Resources LLC dated May 17, 2021. The engagement agreement stated that First Call Processing would "use its sales and marketing expertise to enter into agreements" with consumers and that First Call Processing would exclusively engage the services of Consumer Protection Resources to render the services required by each agreement with consumers. A sample "client agreement" provided to BlueSnap showed that Consumer Protection Resources was charging consumers an upfront fee to enroll in a program that included "Forensic Debt and Credit Auditing on enrolled accounts" and "Development of required documents needed to validate/eliminate debt on enrolled accounts." This client agreement—which referred only to Consumer Protection Resources and did not mention First Call Processing anywhere—also told consumers that "our program has saved our clients thousands over the years," which was clearly false because Consumer Protection Resources, like First Call Processing, had been formed less than a month earlier. Thompson has since

admitted that First Call Processing was used only to process payments for ACRO Services' customers, not to provide the promised debt relief services.

100. Both Dangelmaier and Monteith were concerned that card networks would discover the connection between First Call Processing and the other merchant accounts used by ACRO Services. During the onboarding process, Dangelmaier and Monteith instructed BlueSnap employees that there should be no documentation connecting the new First Call Processing merchant account with the other ACRO Services merchant accounts.

101. On May 23, 2021, a BlueSnap employee sent Monteith an email titled "TriStar ownership" describing the ownership of the three ACRO Services merchant accounts and the possibility of using existing reserve funds to cover potential liabilities with the new account:

Each MID is registered under a different entity but it's the same owner for Nashville and new MID – John Huffman. Potentially we could use the funds from TriStar MID to cover Nashville and then from Nashville we can use it on the new MID (?)

TriStar Consumer Group (legal name Music City Ventures Inc) – Owner is **Preston Thompson**

Nashville Ventures – Owners are **John Steve Huffman** and **Preston Thompson**

NEW First Call Processing LLC – Owner is **John Steve Huffman**

In response, Monteith told the employee that she "decided we are ok with reserves just have to watch carefully. If they don't start processing as planned I will be concerned. . . . Our other risk is that if [D]iscover has a program like [M]atch and Preston gets on it then we will have an issue with Nashville [Ventures]."

102. The next day, May 24, 2021, BlueSnap began processing transactions on the new First Call Processing account (MID 1253610). Most of these transactions used the descriptor "CP Resources." Almost immediately, BlueSnap's fraud prevention team began noticing a large volume of transactions and a high rate of chargebacks on the account. Within the first few weeks, the account had processed over $2 million, with more than $130,000 in chargebacks and an additional $160,000 in refunds issued.

103. On June 14, 2021, BlueSnap's Director of Fraud Strategy told Monteith that they were seeing such rapid chargebacks on the First Call Processing account because ACRO Services had charged multiple consumers' credit cards without authorization—a fact he had learned directly from Sean Austin. The Director stated, "These guys are really sketchy. . . . [they] are for sure not operating a legit business." Monteith responded, "Can you call the [ACRO Services] CEO tomorrow and tell him how careful he has to be. No mistakes. If you want we can ask Ralph [Dangelmaier] to call him."

104. On June 18, 2021, Fiserv emailed Monteith and other BlueSnap employees about First Call Processing, stating, "We need to have this account closed today as they are in violation of our policies." Fiserv followed up a few hours later emphasizing the urgency of the matter: "We need to stress the importance of closing this account down today. If you are unable to do so we can

complete by EOD." Fiserv noted that the First Call Processing account had only been registered to process up to $300,000 per month, but it had already processed over $2 million with over 7% refunds and 6% chargebacks. Fiserv further stated, "We've also confirmed through chargeback documentation that customers were supposed to receive debt consolidation and credit repair services which are unqualified [i.e., prohibited business categories]. The overall consumer harm impact that this merchant has on its customers poses great risk to us for processing these sales and we need to stop any further processing immediately."

105. Fiserv reported that Monteith "initially resisted the closure" of the First Call Processing account and "indicated that [First Call Processing] was engaged in outbound marketing." However, she ultimately acquiesced, and BlueSnap stopped processing new transactions on the First Call Processing account (except for refunds and chargebacks).

106. On June 22, 2021, Fiserv placed the First Call Processing account on the MATCH list with the reason code "04 – EXCESSIVE CHARGEBACKS."

107. On June 23, 2021, Fiserv told Monteith in an email: "While the main reason for the account closure was the unqualified business model, the overall concern on the account was the chargebacks at an exceptionally high level with just a month of processing. . . . Given the concern of the business model alongside

the high chargeback volumes, the closure was necessary, but the chargebacks are what drove the [MATCH] placement."

108. By the time BlueSnap was forced to terminate the First Call Processing account—less than 30 days after it was opened—BlueSnap had processed over 1,000 orders totaling over $3.1 million in consumer payments.

3) Defendants Conspired with ACRO Services to Continue Processing After the First Call Processing Account Was Terminated

109. Around June 23, 2021, Dangelmaier and Monteith had another call with the ACRO owners regarding the termination of the First Call Processing account. During the call, the owners admitted that they had charged some consumers' credit cards before obtaining signed contracts from the consumers. One of the owners asked if their business was completely shut down from processing, and Dangelmaier said it was. But later in the call, when an owner asked if they could keep processing payments on their other companies, Dangelmaier said, "Yep, you're 100 percent fine over there." Dangelmaier also told the owners that "we got to keep Steve [Huffman] from getting on this thing called the MATCH list," explaining that would be "a disaster" and "like a criminal record almost." Dangelmaier told the ACRO owners to immediately issue refunds to consumers who complain so that they would not initiate chargebacks, because otherwise their chargeback thresholds would be too high and they would be shut down due to fraud.

110. The next day, Monteith sent an email titled "Re: First Call Processing Required Next Steps" to the ACRO owners (copying Dangelmaier), telling them: "Following up on our discussion yesterday, you can process on Nashville Ventures. We would like to go over a plan to move volume back before starting." Dangelmaier and Monteith had decided that ACRO Services could resume processing payments using the Nashville Ventures account, but they wanted to coordinate a plan to ensure that their processing would not draw additional scrutiny from Fiserv or the card networks.

111. When the ACRO owners reached out to Dangelmaier directly for clarification, Dangelmaier messaged Monteith and others: "Why does Preston think he can not process for other accounts? I am texting with him. I said he could[,] you guys need to clean that point up. The communication here is a mess[.] Terry he liked your email it was clear you need to call him today or email with him, Sean and Steve are also confused." BlueSnap's Fraud Director responded, "Because you told him his debt business was dead at bluesnap. All other businesses they have with us are the exact same business, same MID, same employees." Dangelmaier then responded: "I did not I said only that ONE MID[.] Only that one mid is dead[,] that's it[.] [W]e have to put things in clear communication[.] Terry's going to talk to him[.] I spoke to him this morning again."

112. Well before this point, BlueSnap knew that ACRO Services had been submitting payments for its debt relief scam through the Nashville Ventures account, even though that account had been set up to process payments for the ACRO owners' separate timeshare cancellation business. ACRO Services started doing this around 2020 despite the fact that it did not use the Nashville Ventures name or entity in dealing with consumers who signed up for ACRO Services' debt relief services. BlueSnap was aware of this practice at least as early as March 2021, when the Nashville Ventures account was placed on the VFMP and BlueSnap was involved in chargeback remediation efforts—which required BlueSnap to review consumers' complaints about debt relief services they had been charged for via the Nashville Ventures account. By June 2021, Dangelmaier and Monteith were expressly telling the ACRO owners they could keep processing payments for the debt relief scam on the Nashville Ventures account.

113. Fiserv, however, was catching on to the scheme. On Friday, July 9, 2021, Fiserv emailed Monteith and Dangelmaier a list of BlueSnap merchant accounts that were of "immediate concern," including the Thacker and Nashville Ventures accounts. Fiserv told BlueSnap, "we would like to see [these accounts] terminated by end of day Monday." Fiserv also asked BlueSnap to identify any other accounts linked to these accounts or the First Call Processing account.

114. BlueSnap finally stopped processing on the Thacker and Nashville Ventures accounts on July 13, 2021, after Fiserv had required it to do so. In the 25 days between the termination of First Call Processing and those two accounts, BlueSnap processed at least another 180 transactions totaling over $200,000.

II. DEFENDANTS' PROCESSING FOR OTHER MERCHANTS WITH HIGH CHARGEBACKS

115. Defendants' support for the ACRO Services scam, even in the face of warnings and direct evidence of fraud, was not an anomaly. Rather, Defendants processed payments for other merchants that they knew or consciously avoided knowing were likely engaged in fraudulent or illegal business practices and that they received multiple warnings about from upstream processors, card networks, and BlueSnap's own Fraud Prevention Team.

116. One example involves Powerline Group, a company that sold software applications advertised as tools for spying on individuals by secretly monitoring their location, text messages, call history, and browsing history, among other things. The New York Attorney General recently found that Powerline Group and its numerous companies had "misrepresented their refund and data security policies, failed to disclose the potential harm to a device caused by the installation of their products, and created sham review sites to lure customers into purchasing and using the stalkerware products." *See* https://ag.ny.gov/press-release/2023/attorney-general-james-secures-410000-tech-companies-illegally-

promoting-spyware. Powerline Group agreed to pay $410,000 to settle charges that it engaged in fraudulent or illegal acts.

117. During the period that BlueSnap processed consumers' payments to Powerline Group, BlueSnap received numerous alerts and warnings about excessive chargebacks. As noted in Paragraph 66, in late 2019 the chargeback rates for Powerline Group were so high—more than six times the threshold required to trigger chargeback monitoring programs—that Fiserv recommended that its merchant account be closed. Despite this warning from Fiserv, BlueSnap continued processing for Powerline Group.

118. In 2021, two of Powerline Group's merchant accounts were placed on the Visa Dispute Monitoring Program for excessive chargebacks, and Monteith submitted a remediation plan for at least one of those accounts. Over the roughly six-year period that BlueSnap processed payments for Powerline Group, one of its merchant accounts had an overall chargeback ratio of 8.55%, with over 25% of the sales on that account being either refunded or charged back by consumers. If BlueSnap followed the fraud monitoring requirements under the VDMP or even its own policies—which require BlueSnap to undertake a meaningful investigation of high-risk merchants, including those with excessive chargeback levels—BlueSnap would have clearly seen that Powerline Group was involved in deceptive or unlawful business practices. Yet BlueSnap chose to turn a blind eye and continue

processing payments for Powerline Group until around July 2021, when Fiserv forced BlueSnap to terminate processing for these accounts after the investigation triggered by the First Call Processing incident.

119. BlueSnap also has repeatedly received warnings, including within the last two years, about high chargeback rates involving merchants who process payments using its "merchant of record" service, in which BlueSnap's subsidiary, BlueSnap Payment Services Ltd, acts as the "reseller" of the products sold by its sub-merchants. As the holder of the "merchant of record" account, BlueSnap Payment Services Ltd enters into agreements with sub-merchants where it resells the sub-merchants' products directly to consumers and accepts consumers' credit card payments in return.

120. For example, in multiple instances, BlueSnap has moved payment traffic for merchants generating excessive chargebacks onto its "merchant of record" account, presumably to dilute that merchant's high chargeback rates with the dozens of other merchants whose payments were also processed through that account—which would evade the card networks' fraud and chargeback monitoring programs. Despite this load-balancing strategy, the chargeback rates for these merchants were so high that BlueSnap's "merchant of record" account itself exceeded chargeback monitoring thresholds.

121. In particular, from about October 2020 through August 2021, and as recently as late 2022, BlueSnap's processing partner, as well as its own fraud prevention team, repeatedly raised concerns about certain merchants that were the main drivers of the fraud-related chargebacks on BlueSnap's "merchant of record" account and that might be engaged in fraudulent and deceptive business practices. Instead of taking the warnings seriously by investigating those merchants and following its own risk management policy, Defendants engaged in load-balancing and continued processing for these merchants. Indeed, in 2021, Visa assessed a fine of over $100,000 on the acquiring bank for BlueSnap's "merchant of record" account (which the bank passed down to BlueSnap) due to the excessive chargebacks on the account.

122. Based on the facts and violations of law alleged in this Complaint, the FTC has reason to believe that Defendants are violating or are about to violate laws enforced by the Commission because, among other things:

a. Defendants engaged in their unlawful acts and practices repeatedly over a number of years;

b. Defendants engaged in their unlawful acts and practices knowingly;

c. Defendants continued their unlawful acts and practices despite knowledge of numerous complaints from consumers as well as warnings and terminations from banks, payment processors, and

card networks, only terminating processing for merchants when compelled to do so; and

d. Defendants remain in the payment processing business, which is their core business, and maintain the means, ability, and incentive to continue their unlawful conduct.

VIOLATIONS OF THE FTC ACT

123. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits "unfair or deceptive acts or practices in or affecting commerce."

124. Acts or practices are unfair under Section 5 of the FTC Act if they cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n).

Count I
Unfair Payment Processing Practices
(Against All Defendants)

125. In numerous instances, Defendants have:

a. Provided payment processors or financial institutions false or deceptive information to obtain and maintain merchant accounts;

b. Opened or maintained merchant accounts for merchants that were shell companies or other companies engaged in fraud;

c. Processed transactions to consumers' accounts for merchants that were shell companies or engaged in fraud;

d. Ignored evidence of fraudulent or illegal activity on merchant accounts; and

e. Failed to timely terminate merchants that were engaged in fraud or other illegal activity.

126. Defendants' acts or practices cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition.

127. Therefore, Defendants' acts or practices as set forth in Paragraph 125 constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a), (n).

VIOLATIONS OF THE TELEMARKETING SALES RULE

128. In 1994, Congress directed the FTC to prescribe rules prohibiting abusive and deceptive telemarketing acts or practices pursuant to the Telemarketing Act, 15 U.S.C. §§ 6101–6108. The FTC adopted the original TSR in 1995, extensively amended it in 2003, and amended certain sections thereafter.

129. Under the TSR, a "merchant" means a person who is authorized under a written contract with an acquirer to honor or accept credit cards, or to transmit or

process for payment credit card payments, for the purchase of goods or services or a charitable contribution. 16 C.F.R. § 310.2(u).

130. It is a violation of the TSR for a person to provide substantial assistance or support to any seller or telemarketer when that person "knows or consciously avoids knowing" that the seller or telemarketer is engaged in any act or practice that violates Sections 310.3(a), (c) or (d) or Section 310.4 of the TSR. 16 C.F.R. § 310.3(b).

131. It is also a violation of the TSR for any person to employ, solicit, or otherwise cause a merchant, or an employee, representative, or agent of the merchant, to present to or deposit into the credit card system for payment, a credit card sales draft generated by a telemarketing transaction that is not the result of a telemarketing credit card transaction between the cardholder and the merchant. 16 C.F.R. § 310.3(c)(2).

132. Pursuant to Section 3(c) of the Telemarketing Act, 15 U.S.C. § 6102(c), a violation of the TSR is treated as a violation of a rule promulgated under the FTC Act regarding unfair or deceptive acts or practices.

133. Pursuant to Section 18(d)(3) of the FTC Act, 15 U.S.C. § 57a(d)(3), a violation of the TSR constitutes an unfair or deceptive act or practice in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

Count II
Assisting and Facilitating Violations of the TSR
(Against All Defendants)

134. In numerous instances, Defendants have provided substantial assistance or support to sellers or telemarketers whom the Defendants knew, or consciously avoided knowing:

a. Induced consumers to pay for goods and services through the use of false or misleading statements, including but not limited to false or misleading statements regarding any material aspect of the performance, efficacy, nature, or central characteristics of goods or services that are the subject of a sales offer; or any material aspect of the nature or terms of the seller's refund, cancellation, exchange, or repurchase policies; in violation of Sections 310.3(a)(2)(iii) and (iv) of the TSR (16 C.F.R. § 310.3(a)(2)(iii)-(iv));

b. Induced consumers to pay for goods and services through the use of false or misleading statements, including but not limited to false or misleading statements in connection with the telemarketing of debt relief services, in violation of Section 310.3(a)(2)(x) of the TSR (16 C.F.R. § 310.3(a)(2)(x));

c. Charged an advance fee for debt relief services, in violation of Section 310.3(a)(5)(i) of the TSR (16 C.F.R. § 310.4(a)(5)(i));

d. Presented to or deposited into, or caused another to present to or deposit into, the credit card system for payment a credit card sales draft generated by a telemarketing transaction that is not the result of a telemarketing credit card transaction between the cardholder and the merchants, without the express permission of the applicable credit card system, in violation of Section 310.3(c)(1) of the TSR (16 C.F.R. § 310.3(c)(1)); and

e. Obtained access to the credit card system through the use of a business relationship or an affiliation with a merchant, when such access is not authorized by the merchant agreement or the applicable credit card system, in violation of Section 310.3(c)(3) of the TSR (16 C.F.R. § 310.3(c)(3)).

135. Therefore, Defendants' acts or practices as set forth in Paragraph 134 are deceptive telemarketing acts or practices that violate the TSR, 16 C.F.R. § 310.3(b).

Count III
Credit Card Laundering
(Against BlueSnap, Dangelmaier, and Monteith)

136. In numerous instances, and without the express permission of the applicable credit card system, Defendants BlueSnap, Dangelmaier, and Monteith have employed, solicited, or otherwise caused merchants, or representatives or agents of merchants, to present to or deposit into, the credit card system for payment, a credit card sales draft generated by a telemarketing transaction that is not the result of a telemarketing credit card transaction between the cardholder and the merchants.

137. Therefore, Defendants BlueSnap's, Dangelmaier's, and Monteith's acts or practices as set forth in Paragraph 136 are deceptive telemarketing acts or practices that violate the TSR, 16 C.F.R. § 310.3(c)(2).

CONSUMER INJURY

138. Consumers are suffering, have suffered, and will continue to suffer substantial injury as a result of Defendants' violations of the FTC Act and the TSR. Absent injunctive relief by this Court, Defendants are likely to continue to injure consumers and harm the public interest.

PRAYER FOR RELIEF

Wherefore, the FTC requests that the Court:

A. Enter a permanent injunction to prevent future violations of the FTC Act and the TSR by Defendants;

B. Award monetary and other relief within the Court's power to grant; and

C. Award any additional relief as the Court determines to be just and proper.

Dated: May 1, 2024

Respectfully submitted,

/s/ Alan Bakowski
MARGARET BURGESS
Georgia Bar No. 167433
ALAN BAKOWSKI
Georgia Bar No. 373002
NATALYA RICE
Georgia Bar No. 975012
Federal Trade Commission
233 Peachtree Street, NE, Ste. 1000
Atlanta, GA 30303
(202) 250-4693; mburgess1@ftc.gov
(404) 656-1363; abakowski@ftc.gov
(202) 455-8587; nrice@ftc.gov

Attorneys for Plaintiff
FEDERAL TRADE COMMISSION