

Christine M. Todaro
Laura Basford
Benjamin R. Davidson
(Each appearing pursuant to DUCivR 83-1.1(b)(1))
FEDERAL TRADE COMMISSION
Attorneys for Plaintiff
600 Pennsylvania Avenue, NW
Mail Stop CC-8528
Washington, DC 20580
202-326-3711; ctodaro@ftc.gov
202-326-2343; lbasford@ftc.gov
202-326-3055; bdavidson@ftc.gov
202-326-3395 (Fax)

**IN THE UNITED STATES DISTRICT COURT
DISTRICT OF UTAH, CENTRAL DIVISION**

FEDERAL TRADE COMMISSION,)	Case No. 2:20-cv-00864-HCN
)	
Plaintiff,)	
)	
v.)	
)	COMPLAINT FOR
COMPLETE MERCHANT SOLUTIONS, LLC)	PERMANENT INJUNCTION
a Utah Limited Liability Company, and)	AND OTHER EQUITABLE
)	RELIEF
JACK WILSON, individually and as a former)	
officer of COMPLETE MERCHANT)	
SOLUTIONS, LLC,)	
)	
Defendants.)	

Plaintiff, the Federal Trade Commission (“FTC”), for its Complaint alleges:

1. The FTC brings this action under Section 13(b) of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 53(b), to obtain permanent injunctive relief, rescission or reformation of contracts, restitution, the refund of monies paid, disgorgement of ill-gotten

monies, and other equitable relief for Defendants' acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a) in connection with Defendants' providing payment processing services.

SUMMARY OF CASE

2. This is an action by the FTC for injunctive and equitable monetary relief on behalf of consumers against Complete Merchant Solutions, LLC, and its former principal Jack Wilson (collectively, "CMS"), for their actions in causing more than \$93 million in charges to consumers. CMS caused these charges by arranging for merchants engaged in fraud to obtain and maintain merchant accounts to process unlawful credit and debit card payments through the card networks (e.g., Visa and Mastercard).

3. CMS is an Independent Sales Organization ("ISO") that helps merchants open accounts with acquiring banks (e.g., Commercial Bank of California) so that the merchants can obtain payment processing services through the card networks.

4. The card networks, acquiring banks, and ISOs take various steps to minimize the ability of merchants engaged in illegal conduct, such as deception or fraud, to use the card networks to charge consumers' debit and credit cards. This requires transparency. Without knowing who the merchant is, what the merchant is selling, and how much the merchant is selling, it is difficult for a card network, an acquiring bank, or an ISO to assess the risk of whether a merchant is engaged in illegal activity.

5. In multiple instances, CMS arranged for the opening of and maintained merchant accounts for merchants when CMS knew or should have known that the merchant accounts were being used by third parties that CMS had not underwritten or that they were being used to sell

products that CMS had not underwritten. CMS also concealed its merchant-clients' fraudulent business practices from its acquiring bank and from the card networks in order to keep those clients' merchant accounts open. Ultimately, many of these merchant-clients were shut down by federal law enforcement actions, such as the frauds perpetrated by Apply Knowledge, USFIA, and Tarr, which are described in this Complaint.

6. CMS's unfair acts and practices have provided fraudulent merchants with access to the payment system, which they used to take millions of dollars from consumers, in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

JURISDICTION AND VENUE

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

8. Venue is proper in this District under 28 U.S.C. § 1391(b)(1), (b)(2),(c)(1) and (c)(2), and 15 U.S.C. § 53(b).

PLAINTIFF

9. The FTC is an independent agency of the United States Government created by statute. 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.

10. The FTC is authorized to initiate federal district court proceedings, by its own attorneys, to enjoin violations of the FTC Act, and to secure such equitable relief as may be appropriate in each case, including rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies. 15 U.S.C. § 53(b).

DEFENDANTS

11. Complete Merchant Solutions, LLC is a limited liability company organized under the laws of the State of Utah. CMS’s principal place of business is located at 727 N 1550 E, Third Floor, Orem, UT 84097. CMS arranges for merchants to obtain merchant accounts to process credit card sales transactions with a bank with which CMS has a contractual relationship. CMS transacts or has transacted business in this District.

12. Jack Wilson (“Wilson”) was the Chief Executive Officer of CMS from 2009 through 2016. For at least this period, acting alone or in concert with others, Wilson has formulated, directed, controlled, or participated in the acts and practices of CMS, including the acts and practices set forth in this Complaint. Wilson, in connection with the matters alleged herein, transacts or has transacted business in this District.

COMMERCE

13. At all times material 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.

DEFENDANTS’ PAYMENT PROCESSING BUSINESS

14. CMS was founded in 2008 by David M. Decker, Jr. (“Decker”), Trever Hansen and Kyle Hall. CMS’s co-founder Kyle Hall explained in a 2009 SEC deposition that CMS’s “core industry is sales force coaching programs, things more of a high risk nature . . . there’s a lot larger margin in those deals.” In an October 28, 2014 presentation at Brigham Young University, Decker explained that CMS was created to assist “high risk” merchants such as multi-level marketers obtain payment-processing services.

15. Merchants need access to the card networks in order to accept credit card payments from consumers. Some merchants and merchant categories are considered “high risk” or “higher risk” by acquiring banks and ISOs because consumers tend to dispute transactions with such merchants at a higher than average rate.

16. The card networks impose fees in connection with high dispute rates, and acquiring banks and ISOs might lose money if they cannot pass on the fees or any costs associated with a dispute won by a consumer to the merchant; for example, when the merchant is insolvent or ceased operations because of a law enforcement action.

17. The card networks permit processing for high-risk merchants, but require acquiring banks and ISOs that process for such merchants to screen and monitor the merchants at a level that is commensurate with the risk they carry.

18. As an ISO, CMS acts as an intermediary to link its merchant-clients with an acquiring bank that has the ability to process sales through the card networks. CMS has referred merchant-clients to several acquiring banks, including Commercial Bank of California (formerly National Bank of California) (“CBCal”), Chesapeake Bank, HSBC Bank and Wells Fargo Bank. CMS earns money based on each transaction between its merchant-clients and consumers.

19. The card networks require acquiring banks and ISOs to comply with rules the networks establish to avoid processing for merchants engaged in fraud. Under its contractual arrangement with CBCal, CMS is required to review potential merchant-clients to make sure that they meet certain criteria, a process known as screening or underwriting. For example, when CMS is underwriting merchants for CBCal, the bank requires CMS to identify the business and business owners, obtain a credit report, perform a site visit, review the business’ website, and

obtain its credit card processing history. These criteria are designed, in part, to prevent fraudulent merchants from obtaining access to the card networks.

20. In addition to underwriting merchants, CBCal also requires CMS to monitor its portfolio of existing merchants and notify CBCal of any information that suggests that merchants may be engaged in fraudulent conduct.

21. Historically, one of the primary indicators a merchant is engaged in fraudulent conduct 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.

22. Chargebacks are not the primary method for consumers to get a refund. Ordinarily, consumers can get refunds directly from the merchant, but when a merchant does not offer a refund, or makes the refund difficult to obtain, consumers may resort to the chargeback process to dispute the charge.

23. The card networks prohibit a merchant from submitting, through its merchant accounts, transactions representing sales of goods or services generated by another merchant. The card networks seek to ensure that a merchant's account processes only transactions involving goods or services for which the acquiring bank approved the accounts.

24. The card networks have chargeback monitoring programs designed to flag merchants with excessive chargeback rates (*i.e.*, 100 or more chargebacks in one month, and a monthly chargeback-to-transaction ratio of 1% or greater). Merchants placed in excessive chargeback programs are subject to additional scrutiny by the card networks, as well as possible fines and termination. If a merchant's account is terminated for excessive chargebacks, an acquirer must place the merchant on a list maintained by the card networks. Mastercard, for

example, maintains the Member Alert to Control High-risk Merchants (“MATCH”) list, which identifies terminated merchants and their principals, and the reason for termination.

25. From its inception, CMS has failed to adequately screen and monitor certain of its merchant-clients. Instead, CMS has aggressively lobbied to open accounts for certain merchants despite clear red flags that the merchants are engaged in unlawful activity.

26. For example, the following dialogue between former CMS CEO Jack Wilson and CBCal employee Vince Lombardo (further discussed in Paragraphs 121 and 122) took place over a series of emails from August 6 to August 7, 2014, in response to CBCal’s initial denial of a merchant account application:

Wilson: “Their chargebacks are well below the card associations’ thresholds [by count] even though they may be at 3%.”

Lombardo: “It is too obvious that [the merchant] has several accounts and is load balancing the accounts among as many as processors as he can to avoid the card associations [chargeback] programs. If we get an examiner, auditor or card association reviewing this file, there will be a significant issue if we approved a business where we know the client has engineered his card acceptance to avoid chargeback penalties. My main issue with this is there is no way we could play dumb with this file.”

Wilson: “If it is picked up, which it probably won’t be then we close it down. If they don’t manage their chargebacks we also shut them down.”

Lombardo: “[S]ince they trigger all of the indicators listed in the VISA best practices guidebook, there could be a compelling argument that we buried our head in the sand & assisted this merchant in avoiding detection. I say we steer clear.”

Wilson: “We have a lot of this type of account and picking it out of our portfolio would be difficult... VISA isn’t going to say we are aiding and abetting nor will the regulators. So we just need to move forward.”

27. On October 7, 2009, Global Payments, a processor that served as an intermediary for Wells Fargo Bank and HSBC Bank, notified CMS that CMS’s overall portfolio chargeback

rate was over 4%, that they expected the chargeback rate to be below 1%, and that two thirds of CMS's merchants were "prohibited business types." In response, Decker "sincerely apologize[d]." He explained that CMS was trying to avoid "land mine" accounts and thought that they "were doing a pretty good job," but they "simply didn't understand how [CMS was] measured from a chargeback perspective."

28. More than seven years later, a December 9, 2016 annual review of CMS conducted by an independent auditor found that CMS's underwriting team "was not able to assess predict or quantify the risk associated with merchant processing." CMS failed to show that it had "the expertise to effectively underwrite or monitor high risk accounts." At the time of the December 2016 review, CMS had focused its business on processing for high-risk merchants for more than eight years.

29. A December 19, 2018 annual review of CMS conducted by another independent auditor noted that, of the 10 CMS merchant accounts with the largest processing volume in October 2018, nine appeared to be "higher risk" merchants.

30. As the following three examples illustrate, instead of screening and monitoring its high-risk merchant-clients or terminating merchant-clients CMS knew or should have known were engaged in fraud, CMS devised ways to help its merchant-clients open accounts and keep their accounts open. This conduct by CMS caused substantial harm to consumers.

A. CMS's Support For The Apply Knowledge Enterprise

31. On February 10, 2014, the FTC filed suit in this District against Apply Knowledge, LLC, Supplier Source, LLC, Ken Sonnenberg (collectively the "Apply Knowledge enterprise"), and a group of telemarketing defendants for operating a fraudulent business

coaching scheme (collectively the “Gannuscia telemarketers”). *FTC v. Apply Knowledge, LLC*, No. 2:14-cv-00088 (D. Utah Feb. 14, 2014). The FTC alleged that the Apply Knowledge enterprise violated the FTC Act and the Telemarketing Sales Rule by misrepresenting the income consumers would likely make through a “business coaching program,” and by assisting and facilitating the Gannuscia defendants’ telemarketing floors that sold the business coaching. On February 16, 2016, the court entered a stipulated order with conduct prohibitions and a judgment against the Apply Knowledge defendants.

32. According to Sonnenberg, Apply Knowledge acted as a “vendor of coaching services” for more than 100 different telemarketing sales floors. Consumers would purchase an online kit for less than \$100 with information about how to start a business. Telemarketing sales floors would then call those consumers and try to sell them purported business coaching that often cost thousands of dollars. The Gannuscia telemarketers told consumers they should expect to quickly recoup their investment and start making thousands of dollars a month.

33. After consumers purchased business coaching, the telemarketing sales floors signed a contract with the consumer and then referred the consumer to a “fulfillment” company like Apply Knowledge that would provide the purported coaching. Apply Knowledge would also attempt to sell the consumers additional goods and services like web hosting and search engine optimization. Telemarketing sales floors like the Gannuscia telemarketers often worked with multiple fulfillment companies at the same time.

34. Under the contractual arrangement between Apply Knowledge and the Gannuscia telemarketers, the Gannuscia telemarketers kept 90% of the sales price of the business coaching, and Apply Knowledge kept the other 10%. Under the contract, Apply Knowledge exercised no

control over how the business coaching was marketed and sold, though Apply Knowledge did forbid any of the 100 sales floors it worked with from using Apply Knowledge's name or brand in their sales pitches and marketing materials.

35. In June 2017, after three years of litigation with the FTC, the Gannuscia telemarketers were unable to identify a single one of the more than 10,000 customers they referred to Apply Knowledge who had turned a profit on, or even returned his or her investment in, the business coaching services.

36. From January 2011 through March 2013, the Apply Knowledge enterprise took more than \$14 million from consumers through merchant accounts that CMS arranged to open through CBCal. Nearly all of this volume was processed through two merchant accounts: one in the name "Apply Knowledge" and the other in the name "Supplier Source."

37. CMS knew or should have known that the Apply Knowledge enterprise was using its merchant accounts to process sales of business coaching by third-party telemarketing sales floors, even though the accounts had not been approved for this purpose. CMS never screened or monitored the third-party sales floors.

38. Decker, CMS's co-founder and president, advised Apply Knowledge to establish a limited liability company under Ken Sonnenberg's wife's name to use for the Supplier Source account so that the account would appear to be unrelated to Apply Knowledge.

1. CMS Caused The Opening Of And Maintained Merchant Accounts For The Apply Knowledge Enterprise That It Knew Or Should Have Known Were Being Used By Third-Party Telemarketers To Sell Products That Had Not Been Underwritten

39. In May 2010, CMS submitted a merchant application for an Apply Knowledge account to CBCal. The application stated that Apply Knowledge would use the merchant

account to sell a recurring \$39.95 monthly web hosting service, and that sales would be made through e-commerce and not by telephone. The “Merchant Profile Analysis” submitted with the application stated that the products and services being sold were “consulting services, website hosting.” In response to the question, “Please explain, in detail, exactly what you will be charging the customer for,” the application said “39.95 / month for hosting.” In a memorandum accompanying the application, Decker wrote “[t]his particular account is for the web hosting payments students pay to maintain their website.”

40. The application did not indicate that the account would also be used by third-party telemarketing sales floors to sell business coaching. The application did not include any telemarketing scripts, which CBCal required if the prospective merchant was engaged in telemarketing.

41. In a January 2011 memo, Jack Wilson wrote that the Apply Knowledge account “is for web hosting only.”

42. In total, the Apply Knowledge account’s average sales transaction was \$305, more than seven times the \$39.95 indicated on the account application. Under CMS’s policies for monitoring suspicious transactions, a merchant’s average transactions exceeding the transaction amount listed on the application is a cause for further review because it may indicate that the merchant is not using this account to sell the products listed on the merchant application.

43. CMS knew or should have known that the Apply Knowledge enterprise was allowing third-party telemarketing sales floors to use the account to sell business coaching. In fact, Sonnenberg discussed this with CMS on several occasions.

44. For example, in October 2010, Decker asked Sonnenberg if there was a way to reduce the dollar amount of chargebacks on his account. Sonnenberg told Decker that the chargebacks were coming from a particular telemarketing sales floor and he had been “working hard to get them down” by issuing refunds before the consumers filed chargebacks.

45. In December 2010, Decker forwarded Sonnenberg an e-mail from CBCal asking why the Apply Knowledge account’s chargeback ratio continued to get worse. Sonnenberg told Decker that he had been processing transactions for two different telemarketing sales floors, and “other than that I’m only running hosting through” the Apply Knowledge account. Sonnenberg explained that he processed for one of the sales floors because he trusted the owner, and he was processing for the other sales floor because the owner owed Sonnenberg money.

46. In January 2011, Sonnenberg asked CMS for help in setting up “sub-accounts for sales floors to run transactions using my merchant account.”

47. In July 2011, Decker asked Sonnenberg if he could keep the Gannuscia telemarketers’ chargebacks low, and Sonnenberg responded that he could by “limiting how much processing I would do for them.”

48. In December 2011, Sonnenberg told Decker that “back-end sales account for about 50% of what we are processing through you guys.” As Sonnenberg later noted in a deposition, “front-end” sales refers to the sale of business coaching made by third-party telemarketing sales floors, while “back-end sales” refers to Sonnenberg selling additional goods and services to consumers who had already purchased business coaching.

49. CBCal only approved the Apply Knowledge enterprise merchant accounts to process “back-end” sales conducted by Apply Knowledge. Put differently, when Sonnenberg

told Decker that back-end sales account for 50% of what Apply Knowledge processed through CMS, he told CMS that half of the processing volume being run through the account was: (1) for the sale of business coaching, which had not been underwritten; (2) made by third parties who had also not been underwritten; and (3) using telemarketing, a sales method that had not been approved.

50. CMS did not inform CBCal that the Apply Knowledge account was being used by third-party telemarketing sales floors to sell business coaching. Instead, CMS provided a memorandum to the bank dated November 29, 2011, stating that Decker had visited Apply Knowledge's offices "multiple times" over the past twelve months, and that "[i]t was confirmed, during the visits that there has been no change in the product offering since original inception of the merchant account."

51. CMS knew the card networks forbid merchants from using their accounts to sell products that are different from the products that had been underwritten, and they also forbid merchants from allowing third parties to use their accounts.

52. CMS treated companies that sell business coaching as "high-risk" or "harder-to-place" with banks because many acquiring banks were unwilling to accept the reputational risk associated with these merchants. Although CMS claimed that its policies and procedures were to apply "special screening and monitoring" to its high-risk merchants, CMS allowed Apply Knowledge to process sales of business coaching by third-party telemarketing sales floors without screening or underwriting the telemarketing sales floors.

53. As discussed in Paragraphs 44, 45 and 47, CMS knew that the third-party telemarketing sales floors were generating the chargebacks associated with the Apply

Knowledge accounts.

54. CMS also knew that the Gannuscia telemarketers had a merchant account placed on MATCH in 2011 due to excessive chargebacks.

55. Aside from knowing about Gannuscia, CMS never asked Apply Knowledge to identify the third-party telemarketing floors it worked with, or to describe how the third-party telemarketing sales floors sold the business coaching.

56. Although CMS's policies required the review of scripts of merchants that sold products through telemarketing, CMS's Apply Knowledge merchant file did not include any sales scripts.

2. CMS Advised Apply Knowledge's President To Open A New Account In His Wife's Name To Conceal The Apply Knowledge Enterprise's Second Merchant Account

57. In July 2011, Sonnenberg asked Decker to set up another merchant account with CMS so that Apply Knowledge would "not [be] running too much volume under one account." Decker told Sonnenberg that CBCal associated Apply Knowledge with a "bad stigma" due to chargebacks. To conceal Sonnenberg's and Apply Knowledge's association with the new merchant account, Decker told Sonnenberg that "it may not be a bad idea to use another LLC, (if you have one) and have your partner/wife sign on [it]."

58. In November 2011, American Express placed Ken Sonnenberg on the MATCH list because Sonnenberg's account experienced excessive chargebacks.

59. On December 14, 2011, Sonnenberg asked an employee at Apply Knowledge to set up a corporation called "Supplier Source" in Sonnenberg's wife's name. Sonnenberg told the employee that, according to Decker, if the corporation were in Sonnenberg's wife's name, CMS

would be able to open a merchant account for that corporation that could accept American Express cards.

60. On December 22, 2011, Sonnenberg told Decker that he had “set up a new entity” under his wife’s name, and he would like to open a merchant account for that entity.

61. Within weeks, CMS submitted to CBCal a merchant application for “Supplier Source, LLC” signed by Sonnenberg’s wife, Babata Sonnenberg. The application stated that Supplier Source sold “research services for drop shipping solutions, marketing website tools, logo creation, and video tools.” It also indicated that sales would be made through e-commerce and not by telemarketing, and that the average transaction would cost \$3,000. The merchant applications listed Wilson as the sales agent for the account.

62. CMS approved the Supplier Source account with an \$80,000 monthly limit.

63. In a February 22, 2012 memo, submitted to CBCal, Wilson claimed that Supplier Source was a “new company” and that since January 2012, the company has “quickly grown to monthly volumes well above” the monthly processing limit and that “they are yet to have a chargeback or return.”

64. CMS concealed from CBCal and the card networks that the Supplier Source account was related to the Apply Knowledge enterprise, that the account was for an existing client, Ken Sonnenberg, and that the account would be used to process third-party telemarketing transactions for the sale of business coaching.

65. From January through March 2012, the Supplier Source account processed nearly \$500,000 in sales per month, more than six times the amount for which it had been approved. On March 30, 2012, CBCal told CMS that the processing volume “raised the flags.” CBCal

asked how the account was connected to Apply Knowledge, and CBCal also asked for more detailed information about how the products were being sold since there was no information about this in the underwriting file. After CBCal's March 30, 2012 inquiry, for the next six months, Sonnenberg stopped using the Supplier Source account and instead used only the original Apply Knowledge account.

3. CMS Fought To Keep The Apply Knowledge Enterprise Accounts Open Even As The Apply Knowledge Enterprise Attracted Scrutiny From CBCal

66. Over the next several months, CMS took steps to keep the Apply Knowledge enterprise's accounts open as CBCal's scrutiny of the business increased.

67. On March 1, 2012, the FTC's Business Opportunity Rule went into effect. The rule requires covered sellers of business opportunities to make detailed disclosures to potential buyers. The day before the rule went into effect, in an e-mail entitled "BizOp rate adjustments," CMS nearly doubled the rates it was charging the Apply Knowledge enterprise for its service.

68. When Sonnenberg objected to these higher rates, in an April 25, 2012 e-mail, CMS's co-founder Kyle Hall told Decker that CMS had "protected" the Apply Knowledge enterprise's accounts from the bank on numerous occasions, and that without Decker's protection the accounts "would have been cutoff, mid-month, without warning, as per the Bank's recommendations."

69. On June 20, 2012, the Salt Lake City Weekly ran a story called "Phone Predators Utah's telemarketing wolf packs." The article recounted law enforcement actions against Utah telemarketing businesses that sold business coaching. It also included critical accounts of the Apply Knowledge enterprise from a former telemarketer and a former customer.

70. On June 27, 2012, Kori Marolf, CMS's Vice President of Risk Management, emailed Sonnenberg and explained that CBCal had read the article and was demanding that CMS terminate the Apply Knowledge enterprise's accounts. Marolf explained that CBCal had "requested that we close it in previous months due to chargebacks, new FTC regulations, etc." and CMS had done their best to keep the account open, but this time the bank was insisting.

71. On September 19, 2012, Decker told Sonnenberg that Decker is "really struggling internally with losing your accounts," and that he may make another plea to the bank to continue processing for the Apply Knowledge enterprise. Sonnenberg responded that he had been "moving forward with setting up [merchant accounts] with different signers and that process has been fine" but he offered to meet to discuss reopening his business with CMS depending on the fees.

72. On October 11, 2012, Wilson wrote in a memo, which was submitted to CBCal, that CMS had "restructured" the Supplier Source account and "obtained current financial data and other documents so that it could be re-opened" and that "the account has been handled in satisfactory manner since re-opening date."

73. From October 2012 through May 2013, the Apply Knowledge enterprise processed more than \$4 million in sales through the Supplier Source account. Then, in May 2013, Decker told Sonnenberg that CBCal was again requiring them to terminate the Supplier Source account.

74. On May 13, 2013, Sonnenberg wrote to Decker that "[i]t's really disruptive on the business to have it shut off so quickly. I really liked having accounts with you because I could

keep them in mine and Babata's name. With other processors I have to use employees and I don't like exposing them to the risks."

75. On June 19, 2013, CMS received an email notice from the card network Discover asking that CMS terminate Discover's acceptance of payments to Apply Knowledge LLC. The email noted that "this merchant address and last name was related to other accounts we have deemed as deceptive. The merchants were promising one thing and either doing nothing or were trying to get more money from consumers in order to fulfill obligations. These business [sic] are all intermingled (supplier source, vi education, coaching department, apply knowledge)."

76. On January 22, 2014, Sonnenberg asked Decker if CBCal would allow the Apply Knowledge enterprise to open a new account with CMS. He asked if CMS should turn on one of the previously used accounts, and Decker responded that they should "re-paper it," and it is "probably best to have [Sonnenberg's wife] Babata sign for both accounts."

77. That same day, CMS emailed CBCal and, referring to the Apply Knowledge and Supplier Source accounts, stated, "we are allowing the accounts to process again." CMS also noted that they "want to begin processing large volumes quickly."

78. On January 27, 2014, the Apply Knowledge enterprise submitted a merchant application on behalf of Supplier Source. Decker signed the application on January 29, 2014 and is listed on the application as the sales agent. On January 30, 2014, Wilson wrote a memo stating that CMS re-opened the Supplier Source account.

79. On February 10, 2014, the FTC filed its lawsuit against the Apply Knowledge enterprise. Shortly after the suit, CMS was served a copy of the temporary restraining order entered in the case.

80. On June 20, 2014, Decker emailed another payment processor, Tom Lineen at Parallel Payments, to see if he would be able to open offshore accounts for Sonnenberg.

B. CMS's Support For The USFIA Scheme

81. On September 28, 2015, the SEC filed a complaint against Steve Chen ("Chen"), USFIA, Inc. Amauction Inc., Amkey, Inc. and other affiliated businesses (collectively, the "USFIA enterprise") for engaging in fraud in connection with the sale of securities. *See SEC v. Chen*, No. 2:15-cv-07425 (C.D. Cal. Sept. 28, 2015). On December 8, 2016, the court granted the SEC's motion for summary judgment as to liability, finding that Chen operated an unlawful pyramid scheme that purported to sell different investment packages. One of the packages was a pyramid scheme that sold a virtual currency called "gem coins." On March 13, 2017, the court entered a stipulated judgment ordering Chen to pay \$71.7 million.

82. From January 2011 through July 2015, the USFIA enterprise took in more than \$66 million in sales through two merchant accounts associated with Amauction and Amkey. These accounts, which CMS arranged to open through CBCal, purported to process sales for antiques, nutraceuticals, and related products, but the accounts instead were largely fronts that the USFIA enterprise used to process investments in its unlawful pyramid scheme.

83. The court-appointed receiver in *SEC v. Chen* determined that more than 90% of the sales made by Amauction and Amkey were sales of the illegal pyramid investments, and not the products that the companies purported to sell.

84. CMS knew or should have known that the accounts it caused to have opened and maintained for the USFIA enterprise were used by the enterprise largely as fronts to conceal the enterprise's sale of bogus investments for its illegal pyramid scheme. Moreover, when the

processing activity of these accounts triggered further review from CBCal, CMS misled CBCal in order to keep the accounts open, allowing the USFIA enterprise to further its illegal scheme.

1. CMS Disregarded Multiple Red Flags When Arranging For The Opening Of Accounts For The USFIA Enterprise

85. On June 22, 2010, CMS arranged for the opening of a merchant account for Amkey, Inc., a company owned by Chen. According to the application, Amkey would be selling personal care products including nutritional supplements, skincare products and household cleaning products. The application claimed that Amkey stored the products at its business address.

86. In signing the Amkey application, CMS's CEO, Wilson, verified that he had physically visited Amkey's business premises.

87. At the time CMS reviewed the application, Amkey did not have a working website, though Amkey's merchant applications claimed that the company would sell products through its website.

88. On August 30, 2012, CMS arranged for the opening of a second account for Chen in the name Amauction, Inc. According to the application, Amauction would be selling contemporary arts, rare antiques and other items, 80% of which would be sold face-to-face. The application stated that Amauction stored its products in a warehouse and showroom.

89. As with the Amkey application, Wilson signed the Amauction application, which verified that he had physically visited Amauction's business premises. CMS approved Amauction for a \$100,000 monthly processing limit.

90. In November 2013, Chen applied for a third merchant account in the name of a company called USFIA, Inc. According to the SEC's complaint, USFIA was the primary entity

Chen used to market his investment scheme. CMS denied the USFIA merchant application in July 2014. According to CMS's records the account was denied due to "non receipt of requested information."

91. While CMS was evaluating the USFIA application, the processing volume on Chen's existing merchant accounts increased dramatically. The accounts processed a combined total of \$120,000 in total sales in October 2013, \$600,000 in November 2013, and more than \$1 million in the months of December 2012, and January 2013.

92. A merchant seeking to open a new account while simultaneously increasing its processing volume in existing accounts is a strong indication that the merchant may be using the accounts interchangeably.

93. Under its agreements with CBCal, CMS should have disclosed the USFIA application to CBCal and investigated the corresponding increase in processing activity in Chen's Amkey and Amauction accounts, but CMS did not do so. Nearly \$64 million of the \$66 million CMS processed for the USFIA enterprise occurred after Chen applied for the USFIA account.

94. In December 2014, Mo Chen, Steve Chen's son, applied for a merchant account for a company called Amkey Global, Inc. CMS submitted the Amkey Global, Inc. application to CBCal on February 27, 2015, as the processing volume in the Amkey account sharply increased and the processing volume for the Amauction account decreased. According to a February 21, 2015 memorandum from Jack Wilson that was provided to CBCal, the new account was to be used to process sales of certain Amkey Inc. products. On March 4, 2015, CBCal informed CMS that it had flagged a number of concerns it had with the application, including that no documents

confirmed that Mo Chen was indeed an officer of the company. CBCal ultimately declined to open this account in June 2015.

2. CMS Misled CBCal About the USFIA Enterprise's Accounts

95. In the fall of 2014, the USFIA enterprise's processing volume through the Amkey and Amauction accounts continued to increase. It processed \$4.8 million in September 2014, \$5.7 million in October 2014, and \$5.7 million in November 2014.

96. The increased volume in these account triggered a review by CBCal's Bank Secrecy Act Department ("BSA"). On December 10, 2014, Vince Lombardo, who worked in CBCal's Bank Card Division emailed Wilson to let him know that BSA had flagged the Amauction account. Lombardo noted that the account had been approved to process \$100,000 a month, but in November 2013, it processed \$636,000. He asked for an "updated write up, including complete financials and financial analysis" as soon as possible so that CBCal could "know what is going through the account."

97. On January 14, 2015, Lombardo e-mailed Decker and Wilson with additional questions about the Amauction account, and he also asked about the Amkey account. Lombardo told Decker and Wilson that "BSA is all over these two accounts."

98. Lombardo relayed a number of concerns including that: (1) the Amauction website is no longer active and a BSA employee could not reach an employee by calling the phone number associated with the account; (2) the corporate tax returns indicated gross receipts that were equivalent to a single month's processing volume; and (3) on a YouTube video Chen "outlines an almost pyramid scheme." Lombardo cautioned that, for the accounts to remain open, CMS needed to address these concerns.

99. The next day, Lombardo suggested in an e-mail to Decker and Wilson that a first step “to CYA” would be to show that the spikes in processing volume align with the timing of auctions held by Amauction. In response, Wilson asked Cindy Zhao, a USFIA employee, for more information about Amauction and then proceeded to misrepresent Zhao’s answers and provide false information to CBCal.

100. First, Wilson asked Zhao if there were scheduled auction dates in the future. On January 21, 2015, Zhao told Wilson that she did not think there would be any auctions anymore and that the last auction was in 2012 or 2013. Notwithstanding Zhao’s answer, Wilson told CBCal in a March 3, 2015 memo that “in early 2014 [Amauction] had regularly scheduled auctions which caused their volume to spike and dip on a regular basis.” Wilson also wrote that Amauction was no longer holding auctions and would instead be selling their items on a wholesale basis.

101. Second, Wilson told Zhao that when he goes to the Amauction website on the internet “there doesn’t appear to be one” and instead he was redirected to “Live Auction.” Wilson asked Zhao to explain how this worked and what the relationship was between Amauction and Live Auction. The merchant application Amauction submitted said that their web address was www.amauction.com and it did not mention any other websites used by the company or a business relationship with Live Auction.

102. In response, on January 19, 2015, Zhao told Wilson that she will have the IT department “fix it” because it had been hacked before. Zhao did not claim that there was a business relationship between Amauction and Live Auction.

103. CMS was obligated to notify CBCal of any hacking incidents its merchant-clients experience because these incidents could compromise consumer data. Rather than tell CBCal that Zhao blamed a hacking incident when she tried to explain why visitors to Amauction's website were redirected to Live Auction's website, Wilson stated that Amauction and Live Auction had a business relationship. In a February 11, 2015 memo, Wilson wrote that Amauction "utilize[s] liveauctioneers.com in NY for the infrastructure of the bidding process" so that the items Amauction is selling are listed on the liveauctioneers.com website, but when consumers make purchases, the transactions go through the Amauction merchant account.

104. The liveauctioneers.com website could not account for Amauction's sales volume. The liveauctioneers.com website indicated that only three auctions took place in 2014. The auctions were held on February 15, February 22, and March 1, 2014. CMS processed 8,311 sales for Amauction in 2014 and those sales were spread throughout the year.

105. As CBCal raised questions about the Amauction account from December 2014 through early 2015, the processing volume in the account decreased dramatically, and the processing volume in the Amkey account increased. This was a further sign suggesting that the USFIA enterprise may have used the two accounts interchangeably even though they had been underwritten to sell different products. The following chart shows the processing volume for Amauction and Amkey accounts during this period:

Month	Amauction	Amkey	Total
2014 Dec	\$1,068,770	\$1,323,390	\$2,392,160
2015 Jan	\$180,470	\$2,170,470	\$2,350,940
2015 Feb	\$186,261	\$2,177,535	\$2,363,796
2015 Mar	\$65,015	\$5,693,266	\$5,758,281
2015 Apr	-	\$7,435,420	\$7,435,420
2015 May	-	\$6,145,543	\$6,145,543
2015 Jun	-	\$7,754,674	\$7,754,674

106. On March 17, 2015, executives from CBCal and CMS had a lunch meeting where the Amkey and Amauction accounts were discussed. Among others, the meeting was attended by Wilson, Decker and CBCal's CEO. During the meeting, CBCal's BSA analyst shared his concerns about the accounts.

107. On April 16, 2015, CMS told CBCal that they would be shutting down the Amauction account.

3. CMS Continued Processing Sales For the USFIA Enterprise After Closing the Amauction Account

108. After CMS shut down the Amauction account, it kept the Amkey account open and CBCal continued to investigate that account. On April 20, 2015, CBCal's BSA analyst asked for invoices showing the sale of nutraceutical products by Amkey. CMS provided the invoices in April and May of 2015. CBCal's BSA analyst determined that the invoices appeared to be fraudulent. For example, the sales prices were all in even amounts (e.g., \$8,000, \$10,000), and the credit card numbers listed on the invoices did not match the credit card numbers that were actually used to process the sales.

109. On June 18, 2015, CBCal's BSA analyst and Wilson conducted a site visit of the Amkey location. CBCal's BSA analyst noted that the location appeared to be staged. For example, the amount of inventory present was not consistent with a company that made millions of dollars in sales every month, much of the inventory was expired and appeared to have been only recently delivered, and no employees were present.

110. On July 1, 2015, CMS closed the Amkey account. Three months later, the SEC filed its action against the USFIA enterprise.

C. CMS's Support For The Tarr Scheme

111. On October 3, 2017, the FTC sued Tarr, Inc., 18 corporate defendants and three individuals (collectively, "Tarr") for engaging in unauthorized billing and deceiving consumers with respect to weight loss, muscle building, and skin cream products. *FTC v. Tarr Inc.*, No. 3:17-cv-02024 (S.D. Cal. October 3, 2017).

112. The FTC alleged that Tarr marketed a variety of products: (1) using a free trial offer that failed to disclose to consumers that they would be automatically enrolled into a

monthly subscription for the product; (2) using websites that gave the misleading impression that they were objective independent news reports; and (3) by making false and unsubstantiated claims about the effectiveness of Tarr's products. The FTC alleged that Tarr's scheme deceived consumers out of hundreds of millions of dollars. On November 14, 2017, the court entered a stipulated order against Tarr with a monetary judgment and conduct prohibitions.

113. From August 2014 through January 2016, the Tarr scheme took in more than \$15 million from consumers through 15 merchant accounts that were opened in the name of 10 different corporations. CMS helped Tarr open those accounts and keep those accounts open through "load balancing."

114. Load balancing refers to the practice of a merchant allocating its sales among multiple merchant accounts in an attempt to prevent the chargebacks on any single account from reaching the level that would trigger further scrutiny based on Visa and Mastercard rules (100 chargebacks and a 1% chargeback rate).

115. In addition to the chargeback levels that would trigger scrutiny based on the card networks' rules, CBCal requested further information about merchants when merchant accounts had either 70 or 75 chargebacks. Similarly, CMS's 2015 Chargeback and Retrieval Policy states that it would request a chargeback reduction plan from a merchant whenever the merchant has more than 70 chargebacks in any given month.

116. CMS arranged for the opening of multiple accounts for Tarr that concealed the connection among these accounts and allowed Tarr's chargebacks to be calculated on a per-account basis instead of on an aggregate basis (*i.e.*, counting chargebacks based on the

cumulative total for each of a merchant's accounts). CMS's conduct shielded Tarr's illegal business practices from further review by CBCal and the card networks.

1. CMS Convinced CBCal To Open Accounts For Tarr

117. On July 23, 2014, Jack Cooper ("Cooper"), a Tarr employee, sent Wilson three merchant applications: Elite Test 360; Ripped Muscle X; and Garcinia Cambogia Slim Fast. At the time CMS received the applications, CMS's underwriting policy indicated that "free' trials with subsequent billing" was a "disqualifying item." All three application materials indicated that the merchants used free trial offers, but CMS submitted them to CBCal for approval.

118. The Elite Test 360 application materials included a website print out whose terms and conditions said "Try EliteTest360 absolutely free, just pay a small shipping and handling fee" and after 14 days customers will be billed automatically.

119. The application materials also included a website print out from the Better Business Bureau which noted that the BBB contacted Garcinia Cambogia Slim Fast in January 2014 with concerns about unsubstantiated health claims, and the company's 14-day trial.

120. The Ripped Muscle X application materials said that the product was for a "14-day trial on muscle building dietary supplement." The Garcinia Cambogia Slim Fast application materials also said the product was for a 14-day trial of a dietary supplement.

121. On August 6, 2014, CBCal denied the EliteTest360 application that CMS submitted. Wilson then persuaded Vince Lombardo at CBCal's Bank Card Division to approve the account, over a series of emails from August 6 to 7, 2014:

Wilson: "Their chargebacks are well below the card associations' thresholds [by count] even though they may be at 3%."

Lombardo: “It is too obvious that [Jack Cooper] has several accounts and is load balancing the accounts among as many as processors as he can to avoid the card associations [chargeback] programs. If we get an examiner, auditor or card association reviewing this file, there will be a significant issue if we approved a business where we know the client has engineered his card acceptance to avoid chargeback penalties. My main issue with this is there is no way we could play dumb with this file.”

Wilson: “If it is picked up, which it probably won’t be then we close it down. If they don’t manage their chargebacks we also shut them down.”

Lombardo: “[S]ince they trigger all of the indicators listed in the VISA best practices guidebook, there could be a compelling argument that we buried our head in the sand & assisted this merchant in avoiding detection. I say we steer clear.”

Wilson: “We have a lot of this type of account and picking it out of our portfolio would be difficult... VISA isn’t going to say we are aiding and abetting nor will the regulators. So we just need to move forward.”

122. Lombardo ultimately agreed, though he warned Wilson that they would need to have “tools to document/protect our decision for allowing these type of merchants into the processing network.”

123. After CMS convinced CBCal to open the first batch of accounts for Tarr, on September 22, 2014, Wilson encouraged Cooper to request another three merchant accounts for approval from CBCal.

2. CMS Helped Tarr Conceal Its Actual Volume Of Chargebacks

124. Over the next several months, Tarr’s accounts, when viewed in the aggregate, had monthly chargebacks well above the levels at which they would be flagged for scrutiny. CMS worked with Tarr in an attempt to make sure that no single account had 75 chargebacks, which would trigger scrutiny from CBCal.

125. First, CMS set low monthly volume limits in order to keep each Tarr account’s chargebacks in check. On August 28, 2014, Wilson asked Cooper whether he would be able to

keep his chargebacks in the 40 to 50 chargeback range if the accounts had a \$100,000 a month processing limit. Wilson told Cooper that “most of my other like merchants get approved at 50k so they can manage their chargebacks at those levels.” Cooper responded that he did not think Tarr would have a problem, and if it did, “we’ll turn the set volume down in our load balance in order to stop chargebacks on that account.” Wilson replied, “That is fine, thanks for the information.”

126. On August 1, 2015, after several months when Tarr’s chargebacks exceeded the CBCal threshold, Cooper asked CMS to “set a hard cap at \$75,000 for all of our MIDs” in order to “help mitigate the number of chargebacks” Tarr received. CMS agreed to the request.

127. Second, CMS alerted Tarr when an account was experiencing high chargebacks in the middle of a month so that Tarr could better load balance. On July 1, 2015, Wilson warned Cooper that four of Tarr’s many accounts were showing increased chargebacks and Tarr needed to “keep watch on them” to make sure they stayed under the “75 bank threshold.” On October 12, 2015, Wilson told Cooper that one of Tarr’s accounts already had 11 chargebacks that month, and Tarr responded that they would “make adjustments on our balancers to make sure it doesn’t hit the threshold.”

128. When Tarr’s accounts did exceed the chargeback threshold, CMS papered its files with *pro forma* chargeback reduction plans. These plans illustrate CMS’s failure or unwillingness to adequately monitor Tarr’s processing.

129. Under CMS’ “Chargeback and Retrieval” policy, when a merchant accrues more than 70 chargebacks in a month, CMS requests a chargeback reduction plan. CMS claims that the chargeback reduction plan “allows us at CMS to communicate with the merchant our

concerns,” it “establish[es] the major causes of their chargebacks,” and allows CMS to “utilize several tools to manage chargebacks.”

130. CMS required Tarr to submit no less than seven chargeback reduction plans in 2015— two on January 6, two on February 3 one on February 4, one on April 29, and one on September 1. With the exception of the name of the company and the product being sold, all seven of the chargeback reduction plans Tarr submitted in 2015 were virtually identical. The plans stated that “[d]uring the last few weeks we experienced . . . some fraudulent traffic on one of our networks.” The plans stated that this was “unusual or unforeseen,” the merchant had “addressed the issue and placed additional security to prevent it from happening in the future,” and the merchant “do[es] not foresee any similar issues like this moving forward.” All plans also stated, “This has been an excellent learning time for our growing organization and the lessons we have learned will insure our stability in the future.”

131. All seven of the chargeback reduction plans Tarr submitted to CMS stated the merchant charged \$4.95 for a 14 day negative-option trial, then billed consumers on a monthly basis, which was a business model that, according to CMS’s own underwriting policies, disqualified the merchant from processing with CMS.

132. On December 9, 2015, Pilar Herrera a Merchant Services Representative for CBCal, noted to CMS that four different Tarr merchant accounts had the same address. A week later, CMS informed CBCal that it would be placing the merchants on 100% reserve until they could update the addresses.

133. A “reserve” is a financial account that an ISO or acquiring bank maintains to protect itself against financial risks if a merchant becomes insolvent. While a merchant is on

100% reserve, CMS withholds from the merchant 100% of the money processed through the merchant account.

134. On January 18, 2016, CMS told Cooper in an e-mail that, due to “chargeback volumes over the last six months across the series of accounts listed below,” CMS would be terminating the Tarr accounts.

135. On January 22, 2016, CBCal contacted Decker to discuss the e-mail exchange between Wilson and Vince Lombardo that is summarized in Paragraphs 121 and 122. CBCal told Decker that they believed the e-mail exchange demonstrated strong misconduct on Wilson’s part.

136. According to Decker, when he asked Wilson about the exchange, Wilson “didn’t really have a response” and “didn’t really remember” the emails. As a result, “upon much consideration and discussion,” Decker and the other CMS co-founders, Kyle Hall, and Trever Hansen, decided to “part ways” with Wilson.

137. Wilson received a severance package from CMS executives including a \$250,000 a year payment for ten years as well as health insurance benefits. Wilson also continues to act as a sales agent for CMS where he receives commissions for referring potential new merchant-clients to CMS as well as commissions for prior independent contractors he oversaw during his employment at CMS.

VIOLATIONS OF THE FTC ACT

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

139. 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

Unfairness

140. As alleged in Paragraphs 14 through 137, in numerous instances, Defendants have:

- a. Caused to have opened or maintained payment processing accounts for merchants when the merchants in whose names the accounts were opened were not the merchants processing payments through the accounts;
- b. Caused to have opened or maintained payment processing accounts for merchants when the accounts were not being used to process sales of the products indicated in the account applications;
- c. Caused to have opened or maintained payment processing accounts for merchants when the merchants were using the accounts for load balancing, which, among other things, enabled the accounts to avoid triggering chargeback monitoring systems; or
- d. Ignored evidence of fraudulent activity on merchant accounts.

141. Defendants' actions 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.

142. Therefore, Defendants' acts or practices as set forth in Paragraph 140 constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a), (n).

CONSUMER INJURY

143. Consumers are suffering, have suffered, and will continue to suffer substantial injury as a result of Defendants' violations of the FTC Act. In addition, Defendants have been unjustly enriched as a result of their unlawful acts and practices. Absent injunctive relief by this Court, Defendants are likely to continue to injure consumers, reap unjust enrichment, and harm the public interest.

THE COURT'S POWER TO GRANT RELIEF

144. Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), empowers this Court to grant injunctive and such other relief as the Court may deem appropriate to halt and redress violations of any provision of law enforced by the FTC. The Court, in the exercise of its equitable jurisdiction, may award ancillary relief, including rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies, to prevent and remedy any violation of any provision of law enforced by the FTC.

PRAYER FOR RELIEF

Wherefore, Plaintiff FTC, pursuant to Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), and the Court's own equitable powers, requests that the Court:

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

B. Award such relief against Defendants as the Court finds necessary to redress injury to consumers resulting from Defendants' violations of the FTC Act, including rescission

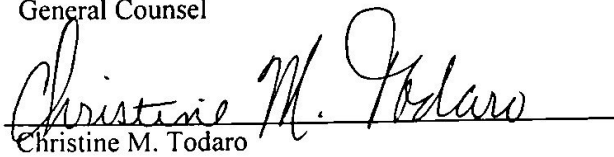
or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies; and

C. Award Plaintiff the costs of bringing this action, as well as such other and additional relief as the Court may determine to be just and proper.

Respectfully submitted,

ALDEN F. ABBOTT
General Counsel

Dated: 12/7/2020

A handwritten signature in cursive script, reading "Christine M. Todaro", is written over a horizontal line.

Christine M. Todaro
Laura Basford
Benjamin R. Davidson
Federal Trade Commission
600 Pennsylvania Avenue, NW
Mail Stop CC-8528
Washington, DC 20580
202-326-3711; ctodaro@ftc.gov
202-326-2343; lbasford@ftc.gov
202-326-3055; b davidson@ftc.gov

Attorneys for Plaintiff
FEDERAL TRADE COMMISSION