REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

Andrew Hudson (DC Bar No. 996294)
(202) 326-2213 / ahudson@ftc.gov
Karen S. Hobbs (DC Bar No. 469817)
(202) 326-3587 / khobbs@ftc.gov
600 Pennsylvania Ave., NW, CC-8528
Washington, DC 20580

Local Counsel
Delilah Vinzon (CA Bar No. 222681)
(310) 824-4328 / dvinzon@ftc.gov
10990 Wilshire Boulevard, Suite 400
Los Angeles, California 90024

Attorneys for Plaintiff
Federal Trade Commission

IN THE UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

Federal Trade Commission,

Plaintiff,

vs.

AlliedWallet, Inc., also d/b/a Allied Wallet, a Nevada company,
Allied Wallet, Ltd., a United Kingdom company,
GTBill, LLC, a Nevada company,
GTBill, Ltd., a United Kingdom company,
Ahmad Khawaja, also known as Andy Khawaja, individually and as an officer, member, and/or manager of AlliedWallet, Inc., Allied Wallet, Ltd., GTBill LLC, and GTBill, Ltd.,
Mohammad Diab, also known as Moe Diab, individually and as an officer, member, and/or manager of AlliedWallet, Inc. and Allied Wallet,

No. 2:19-CV-4355

COMPLAINT FOR PERMANENT INJUNCTION AND OTHER EQUITABLE RELIEF

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

Ltd., and
Amy Rountree, also known as Amy Ringler, individually and as an officer, member, and/or manager of AlliedWallet, Inc. and Allied Wallet, Ltd.,
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).

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337(a), and 1345, and 15 U.S.C. §§ 45(a) and 53(b).

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

SUMMARY OF THE CASE

4. Defendants run a payment facilitating and processing business that enables their merchant-clients to accept debit and credit card payments from consumers. Since at least 2012, Defendants have knowingly processed payments for numerous merchant-clients engaged in fraudulent activities, including merchants that have been subject to law enforcement actions by the FTC, the Securities Exchange Commission ("SEC"), and criminal authorities. Defendants have submitted merchant applications containing false information, and actively worked with their reseller agents, Thomas Wells and his company Priority Payout, to circumvent card network rules and transaction monitoring designed to prevent fraud. Defendants were not deterred by a 2009 federal court ruling in the District of Nevada, finding Wells liable for knowingly debiting bank accounts of numerous

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

fraud victims; to the contrary, they continued to accept numerous referrals of unscrupulous merchant-clients from Wells and benefited from the fraud perpetrated by those clients.

5. Because of Defendants' unfair acts and practices, perpetrators of business opportunity and coaching scams, pyramid schemes, and unlawful debt collection operations gained access to the credit and debit card payment system and charged more than $110 million to consumer accounts.

PLAINTIFF

6. 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.

7. 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

The Corporate Defendants

8. **AlliedWallet, Inc., also d/b/a Allied Wallet** ("Allied Inc.") is a Nevada corporation with a registered agent address of 769 Basque Way, Suite 300, Carson City, Nevada, and has maintained a principal place of business at 9000 Sunset Boulevard, Suite 820, West Hollywood, California. Defendant Ahmad Khawaja ("Khawaja") is the founder, CEO, director, and owner of Allied Inc., and its managers and officers include Defendants Moe Diab ("Diab") and Amy Rountree ("Rountree"). Allied Inc. transacts or has transacted business in this district and throughout the United States.

9. **Allied Wallet Ltd.** ("Allied UK") is a United Kingdom company that lists Second Floor, 1-2 Broadgate, London, England, EC2M 2QS, the address of a shared office space provider, as its registered business address. Since its inception, Allied UK has been wholly owned, directly or indirectly, by Khawaja. Between April 23, 2013 and March 13, 2018, Allied Inc. owned more than 50% of Allied UK, and Khawaja owned the remainder. At all other times, Khawaja has owned 100% of the shares of Allied UK. Khawaja has also been a director of Allied UK since its inception. Allied UK transacts or has transacted business in this district and throughout the United States.

10. **GTBill, LLC** ("GTBill LLC") is a Nevada corporation with a registered agent address of 2215-B Renaissance Dr., Las Vegas, Nevada. GTBill LLC was formed on May 21, 2008, and its Nevada business license expired on May 31, 2015. Its official status with the Nevada Secretary of State is "Revoked." Khawaja is the sole director of GTBill LLC.

11. **GTBill Ltd.** ("GTBill UK") is a United Kingdom company that lists 269 Farnborough Road, Farnborough, Hampshire, GU14 7LX, the offices of Treetops Chartered Accountants, as its registered business address. Since its inception, Khawaja has been the sole owner and director of GTBill UK. Since 2009, annual filings with Companies House, the United Kingdom's registrar of companies, have claimed it is a "dormant company."

The Individual Defendants

12. **Ahmad Khawaja,** also known as "Andy Khawaja," is a California resident. He is the founder, CEO, director, and owner of Allied Inc. and a director and the sole shareholder of Allied UK. He is the sole principal of both GTBill LLC and GTBill UK. At all times material 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 set forth in this Complaint.

Khawaja has been involved in Allied's* creation of U.K. shell companies for U.S. fraudsters, had knowledge about Allied's use of tactics to evade card networks' anti-fraud monitoring, and has communicated with reseller Wells, Allied employees, and merchants about opening and maintaining accounts for merchants engaged in or likely to be engaged in fraud. Khawaja resides in California and, in connection with the matters alleged herein, transacts or has transacted business in this district and throughout the United States.

13. **Mohammad Diab**, also known as "Moe Diab," is a California resident. He is the Chief Operations Officer for Allied Inc. and formerly the Director of Risk and Chargebacks. During all or part of the times material 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 set forth in this Complaint. Diab has been involved in Allied's creation of U.K. shell companies for U.S. fraudsters, had knowledge about Allied's use of tactics to evade card networks' anti-fraud monitoring, and has communicated with reseller Wells, Allied employees, and merchants about opening and maintaining accounts for merchants engaged in or likely to be engaged in fraud. In connection with the matters alleged herein, Diab transacts or has transacted business in this district and throughout the United States.

14. **Amy Rountree**, *nee* Ringler, is a Utah resident. She is the VP of Operations for Allied Inc. During all or part of the times material 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. Rountree has been involved in Allied's creation of U.K. shell companies for U.S. fraudsters, had knowledge about Allied's use of tactics to evade card networks' anti-fraud monitoring, and has communicated with reseller

* Defendants Allied Inc., Allied UK, GTBill LLC, and GTBill UK are collectively referred to as "Allied."

Wells, Allied employees, and merchants about opening and maintaining accounts for merchants engaged in or likely to be engaged in fraud. In connection with the matters alleged herein, Rountree transacts or has transacted business in this district and throughout the United States.

COMMON ENTERPRISE

15. Defendants Allied Inc., Allied UK, GTBill LLC, and GTBill UK (collectively "Allied") have operated as a common enterprise while engaging in the unfair acts and practices alleged in the Complaint. Defendants have conducted the business practices described herein through the interrelated Allied Inc., Allied UK, GTBill LLC, and GTBill UK, which have a common business purpose, business functions, and employees; have commingled funds; and are all controlled by Khawaja, the other individual defendants, and others acting at their behest. Allied Inc. and Allied UK utilize a single website, alliedwallet.com, and GTBill LLC and GTBill UK utilize a single website, gtbill.com, which lists the same address that Allied UK uses as its registered address. Because Allied Inc., Allied UK, GTBill LLC, and GTBill UK have operated as a common enterprise, each of them is jointly and severally liable for the acts and practices alleged below. Khawaja, Diab, and Rountree have formulated, directed, controlled, had the authority to control, or participated in the acts and practices of Allied that constitute the common enterprise.

ALTER EGO

16. As stated above, there is such a unity of interest between Allied Inc., Allied UK, GTBill LLC, and GTBill UK, Khawaja, Diab, and Rountree, that Allied UK is an alter ego of Allied Inc., GTBill LLC, GTBill UK, Khawaja, Diab, and Rountree, individually and/or collectively, and GTBill UK is an alter ego of Allied Inc., GTBill LLC, Allied UK, Khawaja, Diab, and Rountree, individually and/or collectively. Allied UK and GTBill UK are dominated and controlled by Khawaja, directly or through the other Defendants and others involved with the

scheme, and were created to facilitate Defendants' unfair payment processing activities. Defendants operate through the interrelated Allied Inc. and Allied UK, which they use interchangeably and project the image of being a singular entity. Defendants also operate through the interrelated GTBill LLC and GTBill UK, which they use interchangeably and project the image of being a singular entity.

17. Allied Inc., Allied UK, GTBill LLC, and GTBill UK share a single set of mainly U.S.-based employees. Merchants corresponding with Allied have corresponded with the same set of mainly U.S.-based personnel, regardless of which company's name is on the contract with the merchant.

18. Defendants have used bank accounts in the names of Allied Inc., Allied UK, GTBill LLC, and GTBill UK interchangeably, in some cases paying a given merchant from an Allied UK bank account one month, a GTBill bank account another, and an Allied Inc. bank account on another month.

19. On April 23, 2013, Khawaja transferred to Allied Inc. ownership of 319,000 shares of Allied UK, representing more than half of Allied UK's 550,000 shares. As recently as February 2017, Allied UK reported, in an official filing with Companies House, the United Kingdom's registrar of companies, that Allied Inc. was "a 58% shareholder of Allied Wallet UK and includes Allied Wallet UK in its consolidated financial statements. Allied Wallet UK and Allied Wallet Inc. are under common control."

20. In March of 2018, after Allied received a Civil Investigative Demand from the FTC, Khawaja transferred Allied Inc.'s shares in Allied UK back to himself.

21. When registering as a payment facilitator with Mastercard and Visa, both Allied UK and Allied Inc. have used the d/b/a "Allied Wallet" or "AlliedWallet" and the same website of alliedwallet.com. The office locations listed on the alliedwallet.com website include offices in West Hollywood, CA and Gilbert, AZ.

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

22. GTBill's website states "GTBill was formed in 2006," although only Allied Inc. and Allied UK were formed in 2006; neither GTBill LLC nor GTBill UK was formed until 2008.

23. Allied has used Allied Inc. and Allied UK's names interchangeably on contracts with merchants and third-party agents. Allied processes virtually all of the merchant transactions it sponsors through European banks that only have contracted with Allied UK. The only transactions processed through Allied Inc. are in a *de minimis* amount, and pertain to a single legacy merchant. Yet Allied has contracted with numerous new merchant-clients under Allied Inc.'s name, and proceeded to process their transactions through European banks.

24. Allied has contracted with numerous merchant-clients under the name of GTBill, and processed their transactions, and collects fees for doing so, even though GTBill LLC is defunct and GTBill UK is a dormant company that has claimed, for years, to have only £ 1.00 in assets.

25. Allied's internal documents include account-opening checklists that include items for both "AW" (Allied Wallet) merchants and "GTBill" merchants, reflecting that, regardless of which Allied entity a merchant contracts with, the same set of employees work to board the merchant.

26. Third-party agents, commonly known as "resellers," earn commissions from the transactions of merchants that they refer to Allied. Allied has directed some resellers to sign contracts with Allied Inc., rather than Allied UK. The contracts claim that Allied Inc. "offers merchant accounts," and that Allied Inc. will control the merchant accounts opened as a result of Allied's partnership with the third-party agent. Resellers that have signed contracts with Allied Inc. have referred merchants to Allied, which has processed the merchants' transactions through European banks.

27. Failure to disregard the corporate form of Allied UK and GTBill UK would sanction a fraud and injustice by shielding and safeguarding Allied UK and

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

GTBill UK from liability for their role in causing more than $110 million in consumer injury, thereby unjustly enriching Allied UK and GTBill UK by permitting them to keep funds obtained from consumers through fraud and facilitated by their unlawful conduct.

28. This Court has personal jurisdiction over Allied UK because it is the alter ego of Allied Inc., GTBill LLC, GTBill UK, Khawaja, Diab, and Rountree, individually or collectively, and has conducted business in this district and throughout the United States.

29. This Court has personal jurisdiction over GTBill UK because it is the alter ego of Allied Inc., Allied UK, GTBill LLC, Khawaja, Diab, and Rountree, individually or collectively, and has conducted business in this district and throughout the United States.

COMMERCE

30. 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.

THE CREDIT CARD PAYMENT SYSTEM AND MERCHANT ACCOUNTS

31. A merchant account allows merchants to process consumer payments by a credit or debit card. Merchant accounts are available through financial institutions referred to as acquiring banks or "acquirers" that are members of the card networks (*e.g.*, Mastercard, Visa).

32. Without access to a merchant account through an acquirer, merchants cannot accept consumer credit or debit card payments.

33. Various entities act as intermediaries between merchants and acquirers. These entities include payment processors, independent sales organizations, sales agents, and payment facilitators (sometimes referred to as internet payment service providers or IPSPs).

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

34. Unlike other payment intermediaries (*e.g.*, payment processors, independent sales organizations, and sales agents), a payment facilitator 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. It receives settlement of transaction proceeds from the acquirer on behalf of each merchant, and disburses the funds to each merchant.

35. A payment facilitator enters into contracts with acquirers to provide payment services to merchants, and it enters into a separate contract with each merchant to enable payment acceptance. When a cardholder makes a purchase, the merchant routes the transaction data for processing through the payment facilitator's master merchant account.

36. Like other payment intermediaries, a payment facilitator identifies and solicits merchants in need of credit and debit card processing services and earns commissions (or "residuals") and other fees based on the volume of sales transactions processed through each merchant's account. Payment facilitators typically charge merchants different rates depending on, among other factors, the risk associated with the merchant's business.

37. Allied describes itself as a payment facilitator and is registered through multiple acquirers as a payment facilitator with Mastercard and Visa. In addition, Allied UK is a licensed "principal" of Mastercard and Visa in Europe. As a non-bank acquirer in Europe, Allied UK acquires merchants directly and opens merchant accounts through Allied UK's bank identification number ("BIN").

UNDERWRITING AND MONITORING MERCHANT ACCOUNTS

38. In an effort to deter fraud, increase transparency, comply with anti-money laundering statutes, 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.

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

39. The card networks' rules require registered members, such as payment facilitators, to conduct thorough due diligence prior to "onboarding" a merchant into the network. Transparency is a key requirement of the rules. Knowing the identity of the merchant and its principals, where it is located, the products or services it sells, how it sells (*e.g.*, telemarketing, online, retail store), its marketing practices, and the transaction volume, allows the networks, acquirers, and intermediaries (such as payment processors and facilitators) to assess whether the merchant is engaged in legitimate business.

40. Card network rules prohibit an acquirer or payment facilitator from misrepresenting the location of a merchant (*i.e*. the permanent location at which the merchant's employees, officers, or agents conduct business), which is required to be in the same geographic jurisdiction (or "area of use") as the acquirer.

41. These rules also prohibit an entity from acting as a payment facilitator for a merchant that has annual sales volume exceeding certain thresholds. For example, before Visa raised its threshold to $1,000,000 in September 2017, payment facilitators could not facilitate payments for merchants with $100,000 or more in Visa transactions. In 2014, Mastercard raised its annual threshold from $100,000 to $1,000,000 in Mastercard transactions. Merchants that exceed these thresholds must enter into a direct contract with an acquirer.

42. The card network rules also require payment facilitators to transfer merchants' revenues directly to the merchant of record, as opposed to channeling them through an intermediary such as a reseller.

43. After a payment facilitator and its acquirer "board" a merchant and start processing payments on its behalf, the rules require them to monitor the merchant's sales transaction activity to detect unusual processing volumes and excessive chargebacks, which can indicate illegitimate activity, such as fraud or deceptive marketing.

44. One of the primary indicators of fraudulent or deceptive 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.

DEFENDANTS' BUSINESS PRACTICES

45. At all times relevant to this Complaint, Allied has acted as a non-bank acquirer or payment facilitator providing e-commerce merchants with the ability to accept card payments from consumers.

46. Allied's official due diligence policies and procedures mandate the review and collection of information and documents regarding each merchant applicant, including a completed merchant application, all websites, incorporation documents, bank statements, valid identification of the owner, and six months of past processing history. "[D]epending on business type, length of time in business and risk associated," Allied's policies require it to obtain additional information and conduct a thorough review of the merchant's website, advertising, credit check, and marketing to "[e]nsure that a complete understanding of the merchant business type and all practices are known."

47. In addition, Allied's policies enumerate certain types of "prohibited merchants" that Allied will not sponsor or onboard, including "Get Rich Schemes," "Credit Repair Companies," "Credit Card Protection," "ID Theft Services," "Free Trial-Auto Ship merchants," and "Merchants on MATCH [a Mastercard-maintained list of merchants terminated by acquirers]."

Allied and Reseller Thomas Wells Have Helped Fraudsters Bilk Consumers

48. Allied works with resellers to identify and acquire merchants in need of payment processing.

49. In or around 2006, Allied was working with reseller Thomas Wells and his company Interbill, Ltd. ("Interbill") when the FTC sued Wells and Interbill. *FTC v. Interbill, Ltd.*, No. 2:06-cv-1644 (D. Nev. filed Dec. 26, 2006). The FTC charged them with initiating unauthorized debits against thousands of consumers'

accounts, while ignoring strong indications that their merchant-client, Pharmacycards, elicited the payments through fraud.

50. In 2008, while the FTC case against him was still pending, Wells created Priority Payout, Corp. ("Priority Payout") as a successor to Interbill, and continued soliciting merchants for Allied.

51. In 2009, the court granted summary judgment in favor of the FTC, finding that Wells' and Interbill's actions violated the FTC Act. The court awarded the FTC $1.7 million for consumer redress and entered a permanent injunction enjoining Wells and Interbill from: (a) taking any action to process payments on behalf of merchant-clients while knowing or consciously avoiding knowing that such merchant-clients are or are likely to be engaged in deceptive or unfair acts; (b) failing to conduct a reasonable investigation of prospective merchant-clients and the offers for which they request payment processing services; and (c) failing to monitor each merchant-client's transactions to ensure that the merchant-client is not engaged in practices that are deceptive or unfair.

52. In 2010, the Ninth Circuit affirmed the summary judgment decision. *FTC v. Interbill, Ltd*., 385 Fed. Appx. 712, 713 (9th Cir. 2010).

53. Undaunted by Wells' public and well-documented history of engaging in unauthorized debiting on behalf of fraudsters, Allied continued to accept merchant referrals from Wells and Priority Payout (collectively hereinafter referred to as "Wells") until at least late 2017.

54. As detailed below, during this time, Allied knew or should have known, that many of its merchant-clients, a number of which were referred by Wells, were using fake, Allied-created U.K. shell companies designed to circumvent scrutiny by the card networks, submitting account applications containing false information, providing dummy websites to mask the true nature of the merchants' businesses, and laundering transactions through accounts registered to other merchants.

55. One of the fraudulent merchants that Wells referred to Allied was Stark Law, a phantom debt collector for which Allied processed roughly $1,153,107, net of chargebacks and refunds. A federal court in Illinois shut down Stark Law's scheme following an enforcement action by the FTC, and the defendants subsequently agreed to a stipulated permanent injunction and entry of a partially-suspended judgment of more than $47 million. *FTC v. Stark Law*, 1:16-cv-3463 (N.D. Ill. Mar. 27, 2017).

56. Allied and Wells worked together to obtain merchant accounts for a second fraudulent merchant, TelexFree, which operated a massive internet-based Ponzi scheme for which Allied processed $86,980,081 net of chargebacks and refunds. A federal court in Massachusetts shut down that scheme following an SEC enforcement action, resulting in multiple defendants entering into consent judgments. *SEC v. TelexFree, Inc. et al.*, No. 1:14-cv-11858 (D. Mass. filed Apr. 15, 2014). In addition, both of TelexFree's principals were charged with criminal offenses in connection with operating TelexFree. *United States v. Carlos Nataniel Wanzeler and James Matthew Merrill*, Case No. 14-cr-4002814 (D. Mass. May 9, 2014). James Merrill admitted that TelexFree was an illegal pyramid scheme, pleaded guilty, and is serving a six-year sentence for wire fraud. Carlos Wanzeler fled, and remains a fugitive to this day.

57. Allied has also provided payment processing for many fraudulent merchants not referred to it by Wells. Those include massive business opportunities and coaching scams shut down following FTC enforcement actions, such as MOBE and Digital Altitude. *See FTC v. MOBE Ltd.*, No. 6:18-cv-862 (M.D. Fla. filed June 4, 2018) (Allied processed $18,165,443 in payments net of chargebacks and refunds); *FTC v. Digital Altitude, LLC*, No. 2:18-cv-729 (C.D. Cal. filed Jan. 29, 2018) (Allied processed $3,752,310 in payments, net of chargebacks and refunds).

Allied Knowingly Processed for Merchants Engaged in Unlawful Conduct

58. Allied has provided access to the payment system for numerous merchants engaged in fraud. In numerous instances, including with regard to the frauds perpetrated by Stark Law, TelexFree, MOBE and Digital Altitude—Allied:

1) failed to comply with card network rules for due diligence and monitoring procedures;
2) ignored evidence that its merchant-clients—including those referred by Wells—were engaged or likely to engage in unlawful activity;
3) concealed its merchant-clients' fraudulent business practices from acquirers and from the credit card networks;
4) submitted to acquirers merchant applications containing false information; and/or
5) engaged in tactics designed to circumvent card network rules and anti-fraud monitoring.

59. While engaging in this deceptive and unlawful activity, Allied opened and kept open numerous merchant accounts for merchant-clients engaged in fraud, charging more than $110 million to consumer victims' accounts in the four above-named schemes alone.

Allied Created Sham Foreign Shell Corporations for U.S. Merchants

60. The card network rules define a merchant's location. For example, Visa states that a merchant's location must be the country of its principal place of business, which Visa defines as a fixed location where a merchant's executive officers direct, control, and coordinate its activities—generally, a merchant's headquarters.

61. Allied has procured the registration of U.K. shell companies on behalf of U.S. and other non-U.K. and non-E.U. merchants to circumvent card network

rules requiring that merchants be located in the same geographic jurisdiction as Allied's acquirers.

62. By procuring U.K. shell companies for non-U.K. or non-E.U. merchants, Allied has misrepresented to its acquirers and payment processors that such merchants were located in the U.K. or the E.U. and thus eligible for domestic payment processing. Had Allied been truthful about such merchants' locations, card network rules would have barred E.U. acquirers and payment processors from opening accounts for those merchants.

63. By creating shell foreign corporations to process payments for U.S. merchants offshore instead of in the U.S., Allied has enabled U.S. merchants to evade the generally stricter regulatory framework of the U.S. financial system.

64. Using U.K. shell companies to open accounts for non-U.K. or non-E.U. merchants is standard operating procedure at Allied, to the point that the need to procure an "EU Corporation," in addition to the merchant's actual corporate form, is written into Allied's internal account-opening checklist.

65. These foreign shell companies typically have no employees, officers, or operations located in the U.K. or the E.U.

Allied Misrepresented the True Nature of Merchant-Clients' Businesses

66. Further enhancing the charade that certain U.S. merchants were legitimate U.K. corporations located within an acquirer's geographic jurisdiction, Allied has also submitted to its foreign acquirers and processing partners URLs for "dummy" websites that displayed the U.K. address of the merchants' foreign shell companies.

67. In multiple instances, including the Stark Law scheme discussed further below, the dummy websites Allied submitted to its foreign acquirers on behalf of its merchant-clients were non-functional, with no active payment page, contained static images, and appeared to be created from a template website designed by website developer Risoy Designs.

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

68. These dummy websites have typically misrepresented the nature of the merchants' true business.

69. In many instances, as part of seeking an account for a new merchant referred by Wells, Wells asked Rountree, Allied's VP of Operations, to procure a U.K. shell corporation and provided a name under which such a corporation should be created. In one such instance involving Stark Law, on July 20, 2015, Rountree rejected the URL of the dummy website Wells provided in connection with seeking a new merchant account, explaining that it was "too similar" to another URL; Wells responded to Rountree by proposing a slight variation on the URL, and noting "I'll need a day to set [the website] up."

Allied Ignored Glaring Signs of Merchants' and Wells' Unlawful Conduct

70. During the underwriting process and after opening merchant accounts, Allied actively ignored readily-available evidence that its merchant-clients and resellers, such as Wells, were engaged in or likely to be engaged in fraud or deception.

71. Allied also ignored excessive chargeback and decline ratios generated by merchants, which can be strong indicators of fraudulent activity.

72. 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 percent or greater). Merchants placed in excessive chargeback programs are subject to additional scrutiny by the card networks, as well as possible fines and termination.

73. If a merchant's account is terminated for excessive chargebacks, an acquirer must place the merchant on a list maintained by the credit 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.

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

74. While placement on MATCH does not prohibit an acquirer from boarding a merchant, it is an important factor in underwriting and assessing the risk posed by the merchant.

Allied Took Steps to Evade Risk Controls and Anti-Fraud Monitoring

75. Unscrupulous merchants, payment facilitators, and resellers attempt to avoid placement in the chargeback monitoring programs and MATCH through strategies designed to artificially manipulate and reduce the merchants' chargeback ratios (*i.e.*, the number of chargeback transactions divided by the number of sales transactions in a given month, expressed as a percentage).

76. One common strategy is to artificially inflate the number of sales transactions and thus the denominator of the chargeback ratio, resulting in a reduction of the chargeback ratio. To do this, for example, merchants may load money onto prepaid or stored value cards and e-wallets (*i.e.*, a digital wallet) and make "purchases" of their own products or services.

77. Another strategy is opening enough merchant accounts for the merchant to make sure that no single account has more than 100 or more chargebacks in one month—the threshold required for placement in a chargeback monitoring program. The tactic of spreading transaction volume over multiple merchant accounts to avoid hitting the card associations' monitoring threshold is commonly known in the payment processing industry as "load balancing."

78. Yet another strategy is to repeatedly open new merchant accounts using new corporate shells, nominees, and website URLs, making it difficult for acquirers to identify them as related to an unscrupulous merchant and prevent their access to the payment system.

79. On multiple occasions, Allied has continued to process transactions for merchants even after the merchants' accounts were terminated by an acquiring bank for obvious violations, such as misrepresenting the nature of the merchant's business and using a dummy website.

80. Allied has continued to accept merchant referrals from reseller Wells even after Allied knew Wells was engaged in or was likely engaging in unlawful tactics designed to shield his merchants from anti-fraud monitoring.

81. For example, on February 10, 2016, after a risk analyst at Allied's payment processing partner, REDACTED, caused Allied to close multiple merchant accounts for suspicious activity, Wells emailed Diab stating, "Some of these I will open new MIDS [(merchant accounts)] for, under new names."

82. In another instance, Wells openly discussed with Allied's CEO Khawaja and other Allied executives his intention to use load balancing, multiple merchant accounts, and stored value card "purchases" to manipulate a merchant's potential chargeback ratios.

83. Specifically, on July 13, 2016, Wells sent an email to Khawaja with the subject line: "INTERESTING NEW MERCHANT OPPORTUNITY (HUGE)." (Emphasis in original.) In the email, Wells described an opportunity to board a merchant with over $70 million per month in transaction volume. To "make this work," he told Khawaja, Wells would need:

> [t]he ability to issue multiple MIDS as needed . . . and then balancing of the MIDS with added DEBIT CARD TRANSACTIONS (would use the Allied Wallet Stored value cards, and work with Thayne [an Allied employee] to balance the MIDS). (Emphasis in original.)

84. Khawaja copied Diab and Allied employee Thayne Whipple on his response to Wells, stating "lets get this deal and Im going to make it work for you. call me."

85. As Khawaja promised, Allied eventually boarded the merchant in or around December 2016, but not before Wells emailed Khawaja, Rountree, and Diab again on November 3, 2016. In his email, Wells emphasized the need for six E.U. corporations using nominee directors and repeated his intent to manage chargeback activity through illegitimate tactics, including "add[ing] transactions as required utilizing Allied Debit Stored value cards. . . ."

86. Within weeks, Allied procured the creation of six U.K. shell corporations, with nominee directors, using the company names and websites Wells requested, and opened the accounts.

87. Allied's illegitimate practices described above are exemplified in its involvement and communications with reseller Wells, who referred Stark Law and TelexFree, and in its involvement with Digital Altitude and MOBE.

Allied's Processing for the Stark Law Debt Collection Scheme

88. Starting in the spring of 2015, Wells referred to Allied a series of new merchants purportedly selling retail goods, such as blankets, housewares, paint supplies, and hiking equipment. As Allied would quickly be made aware, that was not the case. Instead, the accounts would be used by Stark, a fraudulent phantom debt collector that extracted payments from consumers with threats to litigate over debts consumers did not owe.

89. To open the accounts, Wells asked Allied to procure U.K. shell companies for each of these "merchants," and submitted for underwriting various websites created by Risoy Designs, a website developer used by Wells to create URLs for many merchants he referred to Allied. Allied listed Wells as the "beneficial owner" of each account for purposes of paying sales revenues to the merchants.

90. The group included the following three accounts used by Stark:

1) Stark Law Ltd., using a website (jvalances.com) that purported to sell window valances;
2) Rolling Plains Ltd., using a website (tlcblankets.com) that purported to sell blankets; and
3) Atlantic Hldg Ltd., using a website (tjtapestry.com) that purported to sell carpets.

91. In July 2015, Allied procured a U.K. shell corporation for Stark, despite its business location in the U.S., and approved the account for processing.

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

Shortly thereafter, the Stark account started generating a chargeback ratio of 2.5% and high fraud-to-sales ratios—a measure of how many fraud transactions have been reported by cardholders to their card-issuing banks.

92. Because it costs issuers to process chargebacks, many will not chargeback transactions under a certain dollar value, even though the issuer has reimbursed its cardholder. The card networks establish monthly monitoring thresholds for such fraud transactions. Issuers can report these transactions to card networks, which use the data to identify problematic merchants. For example, Visa will identify merchants that meet or exceed either $75,000 per month in fraud transactions or 1% monthly fraud-to-sales ratio (based on dollar value).

93. On October 23, 2015, Eliza Snelling, a risk analyst at an independent sales organization ("ISO") working with Allied, emailed Diab and Rountree about Stark's "high fraud and possible misrepresentation of business." In the email, Snelling notified Diab and Rountree that the account had fraud ratios of 3.40% in July, 1.01% in August, 3.57% in September, and 4.59% in October.

94. In the same email, Snelling warned Diab and Rountree that Stark appeared to be misrepresenting its business and described her concerns about the merchant's website:

> In looking at the website [jvalances.com], I found that there was no way to reach a payment page. . . This behavior and the exact layout of the pages is identical to that of [the website associated with the Allied merchant account] AW*100Naturals, which you terminated in July after you discovered that it was engaged in transaction laundering.

95. On October 28, 2015, Allied notified Wells that the Stark account was disabled, and forwarded him the analyst's findings. In response, Wells emailed Khawaja, Diab, and Rountree, stating, "This requirement that the web sites be live for [transactions] is new as of this week, this is killing me, don't we have another bank that we can use for these type accounts [*sic*]."

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

96. Allied did not cut ties with Stark or Wells. To the contrary, Allied and Wells continued processing Stark transactions through the merchant account assigned to Rolling Plains Ltd., a company purportedly selling blankets. In a November 12, 2015 email, Wells reassured Diab that Stark "never stopped processing" with Allied, and that Stark's transactions were simply "put into this [separate Allied] account AWTW Rolling Plains Ltd."

97. Similarly, after Stark's Atlantic Hldgs Ltd. merchant account was terminated "due to consistent excessive fraud levels" on November 30, 2015, Wells quickly confirmed for Diab that "this merchant continues to process in [Allied's] AWTW Rolling Plains Ltd. account."

98. By the end of November 2015, REDACTED risk analyst Snelling had informed Allied of hard evidence that Stark was a phantom debt collector, not a home décor vendor. In a November 30, 2015 email to Diab and Rountree, Snelling copied information from a review of a chargeback request, stating that the "MERCHANT POSED AS PAYDAY LOAN LAWSUIT" and took money from a consumer who "HAS NO PAYDAY LOAN." (Emphasis in original.)

99. Despite this additional evidence that Stark was a fraudulent debt collector, Allied continued to process for Stark by laundering its transactions through the Rolling Plains account until February 2, 2016. On that date, Allied was forced to terminate the Rolling Plains account after risk analyst Snelling emailed Diab and Rountree with evidence that Rolling Plains was affiliated with "a U.S. loan service provider," and was not selling blankets. Shortly thereafter, on February 10, 2016, Wells reassured Diab that he "will open new [Allied] MIDS for [Rolling Plains and other accounts], under new names."

100. At numerous times from July 2015 through February 2016, Allied knew that other merchant accounts referred by Wells were using Risoy Designs' dummy websites and engaging in transaction laundering. For example, on November 3, 2015, REDACTED risk analyst Snelling warned Diab and Rountree

about "Probable Transaction Laundering" by a Wells merchant, and included her observations that the merchant's website was just like Stark's—designed by Risoy Designs. Snelling reported that the phone number on the merchant's website (rkitchenstore.com) was linked to "Cash Fairy," a loan application site. "Based on this," Snelling wrote, "we believe that [the merchant] is in fact processing loan services, and not selling kitchen accessories."

101. On January 14, 2016, Snelling emailed Diab and Rountree about Wells' merchant NRALLC, noting the use of Risoy Designs website template, questioning whether the merchant was selling containers, and raising concern that the account was related to a merchant UPGLLC that was "terminated in December [2015] due [to] apparent misrepresentation of business type."

102. To reduce the odds that acquirers and payment processors would similarly scrutinize other accounts associated with Wells, Allied instructed Wells on ways to set up future merchant-clients' purported websites. For example, in November 2015, Rountree copied Diab on an email in which she told Wells, "I recommend to stop [using] Risoy Design[s] and possibly another system to create the URLs." She later advised him that "[p]rice points have to make sense for the [website's purported] business, phone numbers need to work properly," and "everything must be seamless." In addition, on November 17, 2015, Diab emailed Wells and Rountree to let them know that Allied was receiving pressure from the acquirer to review "any other merchants that have come through the same referral channels, etc., as these ones, particularly those with websites designed by Risoy Design[s]," and Diab later told Wells "This is not good news because the bank has caught too many accounts now."

103. Using the tactics described above, Allied processed transactions for the Stark phantom debt collection scheme from July 2015 through at least February 2016. The three merchant accounts processed a combined total of $1,153,107 in sales, less chargebacks and refunds.

104. One month later, in March 2016, the FTC sued Stark Law LLC and related entities for threatening and intimidating consumers to collect more than $47 million in phantom payday loan "debts" the consumer-victims did not owe, or did not owe to Stark or related entities. *FTC v. Stark Law, LLC*, No. 16-CV-3463 (N.D. Ill. filed Mar. 23, 2016).

Allied's Processing for the TelexFree Pyramid Scheme

105. Months before representatives of TelexFree Inc. sought a merchant account from Allied in 2013, news reports had made public that TelexFree was the subject of an investigation by the Brazilian government on suspicion that its operation was an illegal pyramid scheme. This was one of many warning signs available to Allied indicating that TelexFree was a fraud.

106. Further, in documents it gave to Allied, TelexFree's agent admitted that there was significant bad press about the company, and that it had been "accused . . . of being a Ponzi scheme." TelexFree stated that the ownership and name of the company had recently changed, and that the bad press and Ponzi scheme allegations related to the old enterprise, not the new one. But, the documents obtained by Allied during underwriting showed otherwise.

107. The merchant application that TelexFree submitted to Allied identified the two current owners, James Merrill and Carlos Wanzeler, as the same men who had been controlling the company for eleven years, a fact further substantiated by Allied's own background checks, which showed that they had been owners and officers of the company under its prior name, as well.

108. Not only did Allied ignore public information indicating the risk that TelexFree was operating a Ponzi scheme or unlawful pyramid, it disregarded numerous red flags that surfaced during its underwriting of the merchant. For example, TelexFree claimed it was selling voice and video calling on the internet—services already offered for free by well-known companies such as Skype and Google. Yet, TelexFree claimed it would generate $2 million in sales each month,

and processing statements provided to Allied showed it had sometimes made as much as $11 million in sales in a single month—amounts that seemed questionable if TelexFree was, as it claimed, selling a service consumers could get for free from more well-known companies.

109. The lie at the heart of TelexFree's business model was further exposed to Allied in a Profit & Loss statement that showed that TelexFree took millions from consumers, but paid out only commissions and overhead expenses such as office space and payment processing fees—the statement showed no payments to secure the goods or services TelexFree claimed to be selling to consumers.

110. Among other obvious red flags, Allied's underwriting process revealed that TelexFree was placed on the MATCH list for excessive chargebacks, had generated significant chargebacks in recent months, had an "F" rating from the Better Business Bureau, and identified Google search results with headlines like "TelexFree Scam."

111. Allied's underwriting file also included a printout of a detailed review of TelexFree posted on a website dedicated to multi-level marketing companies. TelexFree held itself out as a multi-level marketer. The website printout explained that "all TelexFree members will be doing is publishing ads advertising the income opportunity itself," and that TelexFree's membership fees and structure "*strongly* indicates" that the company's only source of revenue would be membership fees (emphasis in original); *i.e.*, that it sold no products or goods, and instead was merely a Ponzi scheme or unlawful pyramid.

112. In the months before Allied agreed to open a merchant account for TelexFree, further news reports disclosed that the Brazilian government had shut down TelexFree and opened a criminal investigation into its conduct.

113. On August 16, 2013, Khawaja and Diab received a link to the TelexFree underwriting package for review. On August 21, 2013, Diab approved

the opening of the account, saying "Lets [*sic*] do it," in response to an email from Allied's underwriting department that summarized the details described above.

114. TelexFree's account with Allied generated alarmingly high chargeback rates, including one month in which refunds and chargebacks combined reached 10%. For example, on October 10, 2013, Rountree emailed TelexFree (and copied Diab), to implement a hold back of 20% of TelexFree's sales to cover the risk of chargebacks (known as a "reserve account"), based on a review of TelexFree's "recent volume and recent chargeback ratios."

115. On December 20, 2013, Khawaja, Diab, and James Merrill (one of the owners of TelexFree) were included in an email setting up a time to "discuss the TelexFree account with Allied," due to "fraud notifications coming in from the bank," and ways to "move forward with no volume restrictions on the account."

116. Shortly thereafter, TelexFree reached out to Wells, who intervened with Allied on TelexFree's behalf in January 2014, and Allied opened an additional merchant account for TelexFree's use. Khawaja communicated directly with Wells about opening the new TelexFree account.

117. Allied only stopped processing payments for TelexFree when, in April 2014, the SEC charged TelexFree with operating an illegal pyramid scheme, and obtained a court order halting its operations. Shortly thereafter, both of TelexFree's principals were charged with criminal offenses in connection with operating TelexFree. James Merrill pled guilty and was sentenced to six years in prison. Carlos Wanzeler fled, and remains a fugitive to this day. In all, Allied processed $86,980,081 in consumers' payments for TelexFree, net of chargebacks and refunds.

Allied's Processing for the MOBE Business Opportunity Scheme

118. MOBE ("My Online Business Education") was a fraudulent "business education" program owned by Matthew Lloyd McPhee.

119. From the time Allied first accepted a merchant referral for MOBE, in July of 2015, until the FTC obtained a court order halting the scheme in June of 2018, Allied knew or should have known that it was processing payments for a fraudulent scheme.

120. MOBE submitted a merchant application to Allied in the name of MOBE Processing.com Inc., a U.S. corporation using the websites mobe.com and mobemarketplace.com. As noted by Allied's underwriting manager, MOBE had a history of "significant chargeback problems" and was "over the radar."

121. Despite these concerns, on or about September 5, 2015, Allied approved MOBE for a merchant account and boarded it with REDACTED, a German acquirer. In an email to Rountree, Michael Carrasco, Allied's Chief Compliance Officer, described MOBE as an "MLM" ("multi-level-marketing") company. Allied's underwriting file for MOBE contained a pre-application summary, bank statements, bank authorization letter, a copy of Matthew McPhee's passport, past processing statements, and a "profit and loss balance sheet." The file, however, did not contain any website print out, internet search results, credit check, Office of Foreign Assets Control screening, or results of online searches for consumer complaints about MOBE.

122. In December 2015, Allied executive Steve Wilson sought permission from Diab to board another merchant account for MOBE because the merchant was "looking to increase volume and diversify." Diab responded, "Absolutely, lets [*sic*] do it."

123. Around the same time, Allied received a copy of MOBE's membership compensation plan, which revealed that MOBE was offering numerous supposed online coaching products with suspicious names, such as "make millions selling other people's work in 7 days or less" and "60K in 60 days."

124. On December 9, 2015, Wilson asked Allied's risk manager, Jason Luker, to "look again at the docs for Mobe," noting that MOBE was already "on [Allied's] books." Luker reviewed "the few docs included with the pre-app[lication]" and reported to Wilson, "Looking at the service from the website, I'm amazed that it was signed [(boarded)] in the first place, so it's hard to comment on what more is needed." Wilson then instructed Luker to "leave the yes/no decision to Moe [Diab]."

125. By March 2016, Allied had ample evidence that MOBE was likely engaged in fraud. For example, Allied received multiple notices from its payment processor, REDACTED, regarding high fraud and chargeback rates. By March 28, 2016, Diab was concerned about potential fines from the card networks. He emailed MOBE about its "alarming elevated fraud ratios for 2 months now" and "very high" chargeback ratios, and demanded immediate reductions.

126. In early March 2016, Allied sent to payment processor Vantiv a list of potential merchant referrals, including MOBE. In response, Vantiv provided Allied with a spreadsheet in which MOBE was identified as a "prohibited merchant" type because it was "[s]elling 'get rich quick' schemes." Like Vantiv, Allied's Underwriting Guidelines and Procedures define "Get Rich Schemes" as a prohibited business type.

127. Internal Allied emails show that MOBE continued to generate high fraud and chargeback ratios, eventually drawing scrutiny from the acquirer, REDACTED, and fines from the card networks on multiple occasions throughout 2017 and 2018. For example, on November 20, 2017, Diab emailed MOBE to advise that the account had "been breaching the [chargeback] thresholds for several months, however last month was a severe breach and the account has already breached again in November with another 10 days left" and warned that "a fine will be issued by [Allied] for October and November, aside from the fines by the [card network] schemes." In January 2018, Diab warned MOBE that it would be

"now liable for penalties by [Mastercard]" because the account generated chargeback ratios "above 10% – which placed the merchant within [Mastercard's] 'Excessive Chargeback Merchant' (ECM) program's tier."

128. Also in January 2018, a MOBE employee called Allied's compliance department and accused Allied of failing to pay $2 million owed. Through a series of emails with Diab, MOBE eventually discovered and reported the reason for its misunderstanding. MOBE explained, "[W]e did receive the funds. But they were not settled under Allied Wallet as before, but from a different originator. . . a[n Allied] company called 'GTBill.'"

129. To keep MOBE's accounts open, Allied apparently moved or spread out MOBE's merchant accounts among acquirers, as evidenced by an email exchange in which Diab complained to MOBE that Allied had "lost 3 banks to these chargebacks."

130. To keep processing payments for MOBE, Allied accepted an application for two new merchant accounts in the name of MOBE's "secondary company," Transaction Management USA.

131. Despite these clear warning signs early on and throughout its relationship with MOBE, Allied processed payments for MOBE for nearly three years.

132. On February 1, 2018, the FTC obtained a temporary restraining order against the MOBE spinoff, Digital Altitude, discussed in the next section of the Complaint.

133. On February 8, 2018, Diab emailed MOBE:

> the probability of being placed on [MATCH] is very likely and fines are going to be issued, this is now the second bank to request immediate termination. We are trying to find another bank to accept the account, but for now you cannot process with us.

134. The next day, Diab informed MOBE that its account "is live again, you can process. . . . you can start processing now."

135. Nearly three months later, Allied finally terminated MOBE. In an email to MOBE dated April 30, 2018, Diab cited "high levels of fraud and chargebacks" and its decision "to no longer support this business model moving forward."

136. On June 4, 2018, the FTC charged MOBE (including three individuals and nine businesses) with bilking more than $125 million from thousands of consumers. *FTC v. MOBE Ltd*., 18-CV-862 (M.D. Fla. filed June 4, 2018). The district court entered a temporary restraining order and froze the defendants' assets, putting an end to a scheme for which Allied had processed $18,165,443 (net of chargebacks and refunds) in payments since September 2015.

Allied's Processing for the Digital Altitude Business Coaching Scheme

137. Digital Altitude, established by former MOBE employee Michael Force, also purported to be an online business coaching company. In August 2016, MOBE sued Digital Altitude for intellectual property violations for using MOBE's "system." Like MOBE, Digital Altitude induced consumers to buy into a purported educational program by claiming consumers would quickly earn substantial income, such as six figures in ninety days or less. These claims were false—like MOBE, Digital Altitude was a massive fraud.

138. As set out below, the Digital Altitude underwriting materials submitted to Allied raised serious red flags, but did not stop Allied from opening and maintaining merchant account for the scheme.

139. Allied's underwriters reviewed Digital Altitude's "Earnings Disclaimer," which indicated that Digital Altitude was marketing its products or services using outlandish earnings claims.

140. As part of the underwriting process, Allied commissioned a third-party report, dated September 1, 2016, which strongly advised Allied to

"DECLINE" Digital Altitude's application for a merchant account, rating it "High Risk" and awarding it a score of 3% out of 100%. The report explicitly warned Allied that Digital Altitude was using "Deceptive Marketing," and was a "[p]ossible MLM/Ponzi scheme," advising, "[w]e strongly recommend to review the sales and marketing procedure in detail." The report also warned of "indication[s] that the only opportunity for the customers to earn money is by reselling the membership they have signed up for"—in other words, it appeared to be a pyramid scheme. It also noted "very recent customer complaints," and identified a number of them, including some calling Digital Altitude a "Pyramid Scheme" and a "Bare Naked Scam."

141. Allied received from Digital Altitude a Profit and Loss statement showing that in the first half of 2016, consumers paid Digital Altitude nearly $5 million for goods or services that purportedly cost a mere $1,390. Of the $5 million, half was paid out in "commissions" and $1.4 million was profit; the rest was spent on sundry operating expenses, such as payroll, business meals, and travel.

142. In addition, Allied's underwriters ran searches on Google about "Digital Altitude LLC," and reviewed a results page including hits such as "Is Digital Altitude a Scam? - How To Stay Safe On The Net," and "What Is Digital Altitude? Beware Of This High Ticket Scam."

143. After Allied began processing for Digital Altitude, it ignored warning signs raised by Digital Altitude's processing statistics. For example, in April 2017, refunds issued to Digital Altitude's customers through Allied exceeded 10% of Digital Altitude's sales, prompting alarms from Allied's internal monitoring system. Instead of terminating the fraudulent merchant or investigating the reason for excessive refunds, Diab directed employees to raise the refund monitoring threshold from 10% to 25% of sales.

144. At times, Allied continued to process for Digital Altitude as a payment facilitator even though the processing volume far exceeded the permissible limits for a payment facilitator sub-merchant, and thus violated the card network rules and Allied's agreements with its acquirers. Indeed, from the beginning, Digital Altitude had informed Allied, in its merchant application, that its estimated monthly volume would be between $500,000 and $1 million. Once it began processing, Allied learned those estimates were accurate; in the first full month of processing (February 2017), Allied processed over $600,000 in payments for Digital Altitude. Allied did not cease processing for Digital Altitude or tell the merchant to enter into a direct contract with the acquirer, as required by the card networks' rules.

145. On March 31, 2017, the FTC issued a Civil Investigative Demand to Allied, seeking information and documents pertaining to Digital Altitude. While responding to the CID, Allied temporarily closed Digital Altitude's account (on May 10, 2017), and so informed the FTC. However, in September 2017, a few months after Allied completed its response to the CID, Allied's VP of Sales, John Thorpe, requested that Allied re-activate Digital Altitude's merchant account, and Diab approved the re-activation. As Thorpe said to Digital Altitude's agent in response to a request for lower fees on the re-activated account, "we can do that, not a problem. Get them to push more volume and we all make more money."

146. Allied's processing for Digital Altitude ceased only after the FTC sued Digital Altitude and obtained an order freezing all its assets. *FTC v. Digital Altitude LLC, et al.*, No. 2:18-cv-0729 (C.D. Cal. filed January 29, 2018). Allied processed at least $3,752,310 in consumers' payments for Digital Altitude, net of chargebacks and refunds.

147. As demonstrated above, Allied has engaged in unfair acts or practices, including concealing the true nature of its merchants' businesses, setting up sham shell U.K. corporations, engaging in tactics designed to evade anti-fraud

monitoring, and actively ignoring numerous signs that its merchant-clients and Wells were engaged in or likely engaged in unlawful activity.

148. The evidence described above demonstrates that the Allied executives named as individual defendants have directly participated in the unfair acts or practices of Allied. Khawaja, Diab, and Rountree have been directly involved in all aspects of Allied's business operations, including Allied's policies and procedures for opening and monitoring merchant accounts, conducting due diligence on merchants, and its relationship with Wells.

149. The individual defendants knew or should have known about the unlawful conduct used by Allied to obtain and maintain processing for merchant-clients engaged in or likely to be engaged in fraud, the use of U.K shell corporations, and Wells' and merchant-clients' intention to engage in load balancing and other tactics to evade card networks' chargeback and anti-fraud monitoring programs.

150. As a result of Defendants' unlawful actions, consumer victims lost at least $110 million in the four fraudulent schemes described herein.

151. Based on Defendants' long history of continuous conduct of the type described above; Defendants' continued use of the practices challenged above after learning of the Commission's investigation; Defendants' continuance in the business of payment processing; and the ease with which Defendants can engage in similar conduct for existing or future merchants, the Federal Trade Commission has reason to believe that Defendants are violating or are about to violate laws enforced by the Commission.

VIOLATIONS OF THE FTC ACT

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

153. 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

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n).

COUNT I

154. Defendants' acts or practices in processing fraudulent and unauthorized transactions to consumers' accounts, as described in paragraphs 45-150 above, have caused or are likely to cause substantial injury to consumers that is not reasonably avoidable by consumers themselves and that is not outweighed by countervailing benefits to consumers or competition. Such injury is the predictable result of the acts or practices described in paragraphs 45-150 above.

155. Therefore, Defendants' acts or practices, as described above, constitute unfair acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C.§§ 45(a) and 45(n).

CONSUMER INJURY

156. Consumers in the United States 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 or 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

157. 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 Plaintiff such relief as the Court finds necessary to redress injury to consumers resulting from Defendants' violations of the FTC Act, including but not limited to, 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: May 20, 2019

Andrew Hudson
Karen S. Hobbs
Federal Trade Commission
600 Pennsylvania Ave., NW
Mailstop CC-8528
Washington, DC 20580
(202) 326-2213 / ahudson@ftc.gov
(202) 326-3587 / khobbs@ftc.gov

Local Counsel
Delilah Vinzon (CA Bar No. 222681)
(310) 824-4328 / dvinzon@ftc.gov
10990 Wilshire Boulevard, Suite 400
Los Angeles, California 90024

Attorneys for Plaintiff
FEDERAL TRADE COMMISSION