

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

1 Andrew Hudson (DC Bar No. 996294)
2 (202) 326-2213 / ahudson@ftc.gov
3 Karen S. Hobbs (DC Bar No. 469817)
4 (202) 326-3587 / khobbs@ftc.gov
5 600 Pennsylvania Ave., NW, CC-8528
6 Washington, DC 20580

7 Local Counsel
8 Delilah Vinzon (CA Bar No. 222681)
9 (310) 824-4328 / dvinzon@ftc.gov
10 10990 Wilshire Boulevard, Suite 400
11 Los Angeles, California 90024

12 Attorneys for Plaintiff
13 Federal Trade Commission

14 **IN THE UNITED STATES DISTRICT COURT**
15 **FOR THE CENTRAL DISTRICT OF CALIFORNIA**

16 **Federal Trade Commission,**

17 Plaintiff,

18 vs.

19 **AlliedWallet, Inc.**, also d/b/a Allied
20 Wallet, a Nevada company,
21 **Allied Wallet, Ltd.**, a United Kingdom
22 company,
23 **GTBill, LLC**, a Nevada company,
24 **GTBill, Ltd.**, a United Kingdom
25 company,
26 **Ahmad Khawaja**, also known as Andy
27 Khawaja, individually and as an officer,
28 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

1 | Ltd., and
2 | **Amy Rountree**, also known as Amy
3 | Ringler, individually and as an officer,
4 | member, and/or manager of
5 | AlliedWallet, Inc. and Allied Wallet,
6 | Ltd.,
7 | Defendants.

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

7 | 1. The FTC brings this action under Section 13(b) of the Federal Trade
8 | Commission Act (“FTC Act”), 15 U.S.C. § 53(b), to obtain permanent injunctive
9 | relief, rescission or reformation of contracts, restitution, the refund of monies paid,
10 | disgorgement of ill-gotten monies, and other equitable relief for Defendants’ acts
11 | or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

12 | **JURISDICTION AND VENUE**

13 | 2. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§
14 | 1331, 1337(a), and 1345, and 15 U.S.C. §§ 45(a) and 53(b).

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

17 | **SUMMARY OF THE CASE**

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

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

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

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

8 **PLAINTIFF**

9 6. The FTC is an independent agency of the United States Government
10 created by statute. 15 U.S.C. §§ 41-58. The FTC enforces Section 5(a) of the FTC
11 Act, 15 U.S.C. § 45(a), which prohibits unfair or deceptive acts or practices in or
12 affecting commerce.

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

18 **DEFENDANTS**

19 ***The Corporate Defendants***

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

28

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

1 9. **Allied Wallet Ltd.** (“Allied UK”) is a United Kingdom company that
2 lists Second Floor, 1-2 Broadgate, London, England, EC2M 2QS, the address of a
3 shared office space provider, as its registered business address. Since its inception,
4 Allied UK has been wholly owned, directly or indirectly, by Khawaja. Between
5 April 23, 2013 and March 13, 2018, Allied Inc. owned more than 50% of Allied
6 UK, and Khawaja owned the remainder. At all other times, Khawaja has owned
7 100% of the shares of Allied UK. Khawaja has also been a director of Allied UK
8 since its inception. Allied UK transacts or has transacted business in this district
9 and throughout the United States.

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

15 11. **GTBill Ltd.** (“GTBill UK”) is a United Kingdom company that lists
16 269 Farnborough Road, Farnborough, Hampshire, GU14 7LX, the offices of
17 Treetops Chartered Accountants, as its registered business address. Since its
18 inception, Khawaja has been the sole owner and director of GTBill UK. Since
19 2009, annual filings with Companies House, the United Kingdom’s registrar of
20 companies, have claimed it is a “dormant company.”

21 ***The Individual Defendants***

22 12. **Ahmad Khawaja**, also known as “Andy Khawaja,” is a California
23 resident. He is the founder, CEO, director, and owner of Allied Inc. and a director
24 and the sole shareholder of Allied UK. He is the sole principal of both GTBill
25 LLC and GTBill UK. At all times material to this Complaint, acting alone or in
26 concert with others, he has formulated, directed, controlled, had the authority to
27 control, or participated in the acts and practices set forth in this Complaint.

28

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

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

8 13. **Mohammad Diab**, also known as "Moe Diab," is a California
9 resident. He is the Chief Operations Officer for Allied Inc. and formerly the
10 Director of Risk and Chargebacks. During all or part of the times material to this
11 Complaint, acting alone or in concert with others, he has formulated, directed,
12 controlled, had the authority to control, or participated in the acts and practices set
13 forth in this Complaint. Diab has been involved in Allied's creation of U.K. shell
14 companies for U.S. fraudsters, had knowledge about Allied's use of tactics to evade
15 card networks' anti-fraud monitoring, and has communicated with reseller Wells,
16 Allied employees, and merchants about opening and maintaining accounts for
17 merchants engaged in or likely to be engaged in fraud. In connection with the
18 matters alleged herein, Diab transacts or has transacted business in this district and
19 throughout the United States.

20 14. **Amy Rountree**, *nee* Ringler, is a Utah resident. She is the VP of
21 Operations for Allied Inc. During all or part of the times material to this
22 Complaint, acting alone or in concert with others, she has formulated, directed,
23 controlled, had the authority to control, or participated in the acts and practices set
24 forth in this Complaint. Rountree has been involved in Allied's creation of U.K.
25 shell companies for U.S. fraudsters, had knowledge about Allied's use of tactics to
26 evade card networks' anti-fraud monitoring, and has communicated with reseller

27
28 _____
* Defendants Allied Inc., Allied UK, GTBill LLC, and GTBill UK are collectively referred to as "Allied."

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

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

5 **COMMON ENTERPRISE**

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

21 **ALTER EGO**

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

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

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

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

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

14 | 19. On April 23, 2013, Khawaja transferred to Allied Inc. ownership of
15 | 319,000 shares of Allied UK, representing more than half of Allied UK's 550,000
16 | shares. As recently as February 2017, Allied UK reported, in an official filing with
17 | Companies House, the United Kingdom's registrar of companies, that Allied Inc.
18 | was "a 58% shareholder of Allied Wallet UK and includes Allied Wallet UK in its
19 | consolidated financial statements. Allied Wallet UK and Allied Wallet Inc. are
20 | under common control."

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

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

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

1 22. GTBill’s website states “GTBill was formed in 2006,” although only
2 Allied Inc. and Allied UK were formed in 2006; neither GTBill LLC nor GTBill
3 UK was formed until 2008.

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

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

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

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

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

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

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

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

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

13 **COMMERCE**

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

17 **THE CREDIT CARD PAYMENT SYSTEM**

18 **AND MERCHANT ACCOUNTS**

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

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

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

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

1 34. Unlike other payment intermediaries (*e.g.*, payment processors,
2 independent sales organizations, and sales agents), a payment facilitator does not
3 procure a separate merchant account for each of its merchant-clients. Instead, the
4 payment facilitator, itself, is a merchant registered by an acquirer to facilitate
5 transactions on behalf of other merchants. It receives settlement of transaction
6 proceeds from the acquirer on behalf of each merchant, and disburses the funds to
7 each merchant.

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

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

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

UNDERWRITING AND MONITORING MERCHANT ACCOUNTS

24 38. In an effort to deter fraud, increase transparency, comply with anti-
25 money laundering statutes, and reduce risk to the payment system, card networks
26 impose operating rules and restrictions on registered members and third parties,
27 including acquirers and payment facilitators.
28

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

1 ***Allied Knowingly Processed for Merchants Engaged in Unlawful Conduct***

2 58. Allied has provided access to the payment system for numerous
3 merchants engaged in fraud. In numerous instances, including with regard to the
4 frauds perpetrated by Stark Law, TelexFree, MOBE and Digital Altitude—Allied:
5 1) failed to comply with card network rules for due diligence and
6 monitoring procedures;
7 2) ignored evidence that its merchant-clients—including those
8 referred by Wells—were engaged or likely to engage in
9 unlawful activity;
10 3) concealed its merchant-clients’ fraudulent business practices
11 from acquirers and from the credit card networks;
12 4) submitted to acquirers merchant applications containing false
13 information; and/or
14 5) engaged in tactics designed to circumvent card network rules
15 and anti-fraud monitoring.

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

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

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

26 61. Allied has procured the registration of U.K. shell companies on behalf
27 of U.S. and other non-U.K. and non-E.U. merchants to circumvent card network
28

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

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

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

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

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

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

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

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

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

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

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

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

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

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

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

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

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

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

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

7 ***Allied’s Processing for the Stark Law Debt Collection Scheme***

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

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

20 90. The group included the following three accounts used by Stark:
21 1) Stark Law Ltd., using a website (jvalances.com) that purported
22 to sell window valances;
23 2) Rolling Plains Ltd., using a website (tlcblankets.com) that
24 purported to sell blankets; and
25 3) Atlantic Hldg Ltd., using a website (tjtapestry.com) that
26 purported to sell carpets.

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

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

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

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

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

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

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

26 | 95. On October 28, 2015, Allied notified Wells that the Stark account was
27 | disabled, and forwarded him the analyst’s findings. In response, Wells emailed
28 | 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

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

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

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

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

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

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

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

7 101. On January 14, 2016, Snelling emailed Diab and Rountree about
8 Wells’ merchant NRALLC, noting the use of Risoy Designs website template,
9 questioning whether the merchant was selling containers, and raising concern that
10 the account was related to a merchant UPGLLC that was “terminated in December
11 [2015] due [to] apparent misrepresentation of business type.”

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

25 103. Using the tactics described above, Allied processed transactions for
26 the Stark phantom debt collection scheme from July 2015 through at least February
27 2016. The three merchant accounts processed a combined total of \$1,153,107 in
28 sales, less chargebacks and refunds.

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

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

6 ***Allied’s Processing for the TelexFree Pyramid Scheme***

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

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

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

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

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

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

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

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

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

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

26 113. On August 16, 2013, Khawaja and Diab received a link to the
27 TelexFree underwriting package for review. On August 21, 2013, Diab approved
28

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

1 the opening of the account, saying “Lets [sic] do it,” in response to an email from
2 Allied’s underwriting department that summarized the details described above.

3 114. TelexFree’s account with Allied generated alarmingly high chargeback
4 rates, including one month in which refunds and chargebacks combined reached
5 10%. For example, on October 10, 2013, Rountree emailed TelexFree (and copied
6 Diab), to implement a hold back of 20% of TelexFree’s sales to cover the risk of
7 chargebacks (known as a “reserve account”), based on a review of TelexFree’s
8 “recent volume and recent chargeback ratios.”

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

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

17 117. Allied only stopped processing payments for TelexFree when, in April
18 2014, the SEC charged TelexFree with operating an illegal pyramid scheme, and
19 obtained a court order halting its operations. Shortly thereafter, both of TelexFree’s
20 principals were charged with criminal offenses in connection with operating
21 TelexFree. James Merrill pled guilty and was sentenced to six years in prison.
22 Carlos Wanzeler fled, and remains a fugitive to this day. In all, Allied processed
23 \$86,980,081 in consumers’ payments for TelexFree, net of chargebacks and
24 refunds.

25 ***Allied’s Processing for the MOBE Business Opportunity Scheme***

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

28

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

1 119. From the time Allied first accepted a merchant referral for MOBE, in
2 July of 2015, until the FTC obtained a court order halting the scheme in June of
3 2018, Allied knew or should have known that it was processing payments for a
4 fraudulent scheme.

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

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

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

23 123. Around the same time, Allied received a copy of MOBE's
24 membership compensation plan, which revealed that MOBE was offering
25 numerous supposed online coaching products with suspicious names, such as
26 "make millions selling other people's work in 7 days or less" and "60K in 60
27 days."
28

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

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

8 125. By March 2016, Allied had ample evidence that MOBE was likely
9 engaged in fraud. For example, Allied received multiple notices from its payment
10 processor, REDACTED, regarding high fraud and chargeback rates. By March 28,
11 2016, Diab was concerned about potential fines from the card networks. He
12 emailed MOBE about its “alarming elevated fraud ratios for 2 months now” and
13 “very high” chargeback ratios, and demanded immediate reductions.

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

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

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

1 “now liable for penalties by [Mastercard]” because the account generated
2 chargeback ratios “above 10% – which placed the merchant within [Mastercard’s]
3 ‘Excessive Chargeback Merchant’ (ECM) program’s tier.”

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

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

14 130. To keep processing payments for MOBE, Allied accepted an
15 application for two new merchant accounts in the name of MOBE’s “secondary
16 company,” Transaction Management USA.

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

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

23 133. On February 8, 2018, Diab emailed MOBE:
24 the probability of being placed on [MATCH] is very
25 likely and fines are going to be issued, this is now the
26 second bank to request immediate termination. We are
27 trying to find another bank to accept the account, but for
28 now you cannot process with us.

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

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

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

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

13 ***Allied’s Processing for the Digital Altitude Business Coaching Scheme***

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

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

24 139. Allied’s underwriters reviewed Digital Altitude’s “Earnings
25 Disclaimer,” which indicated that Digital Altitude was marketing its products or
26 services using outlandish earnings claims.

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

