

FILED UNDER SEAL PURSUANT TO ORDER OF THE COURT DATED MAY 23, 2019

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

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

13 41. These rules also prohibit an entity from acting as a payment facilitator
14 for a merchant that has annual sales volume exceeding certain thresholds. For
15 example, before Visa raised its threshold to \$1,000,000 in September 2017,
16 payment facilitators could not facilitate payments for merchants with \$100,000 or
17 more in Visa transactions. In 2014, Mastercard raised its annual threshold from
18 \$100,000 to \$1,000,000 in Mastercard transactions. Merchants that exceed these
19 thresholds must enter into a direct contract with an acquirer.

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

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

28

FILED UNDER SEAL PURSUANT TO ORDER OF THE COURT DATED MAY 23, 2019

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

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

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

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

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

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

FILED UNDER SEAL PURSUANT TO ORDER OF THE COURT DATED MAY 23, 2019

1 55. One of the fraudulent merchants that Wells referred to Allied was
2 Stark Law, a phantom debt collector for which Allied processed roughly
3 \$1,153,107, net of chargebacks and refunds. A federal court in Illinois shut down
4 Stark Law's scheme following an enforcement action by the FTC, and the
5 defendants subsequently agreed to a stipulated permanent injunction and entry of a
6 partially-suspended judgment of more than \$47 million. *FTC v. Stark Law*, 1:16-
7 cv-3463 (N.D. Ill. Mar. 27, 2017).

8 56. Allied and Wells worked together to obtain merchant accounts for a
9 second fraudulent merchant, TelexFree, which operated a massive internet-based
10 Ponzi scheme for which Allied processed \$86,980,081 net of chargebacks and
11 refunds. A federal court in Massachusetts shut down that scheme following an
12 SEC enforcement action, resulting in multiple defendants entering into consent
13 judgments. *SEC v. TelexFree, Inc. et al.*, No. 1:14-cv-11858 (D. Mass. filed Apr.
14 15, 2014). In addition, both of TelexFree's principals were charged with criminal
15 offenses in connection with operating TelexFree. *United States v. Carlos Nataniel*
16 *Wanzeler and James Matthew Merrill*, Case No. 14-cr-4002814 (D. Mass. May 9,
17 2014). James Merrill admitted that TelexFree was an illegal pyramid scheme,
18 pleaded guilty, and is serving a six-year sentence for wire fraud. Carlos Wanzeler
19 fled, and remains a fugitive to this day.

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

28

FILED UNDER SEAL PURSUANT TO ORDER OF THE COURT DATED MAY 23, 2019

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

FILED UNDER SEAL PURSUANT TO ORDER OF THE COURT DATED MAY 23, 2019

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

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

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

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

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

18 ***Allied Misrepresented the True Nature of Merchant-Clients' Businesses***

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

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

FILED UNDER SEAL PURSUANT TO ORDER OF THE COURT DATED MAY 23, 2019

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

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

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

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

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

18 72. The card networks have chargeback monitoring programs designed to
19 flag merchants with excessive chargeback rates (*i.e.*, 100 or more chargebacks in
20 one month, and a monthly chargeback-to-transaction ratio of 1 percent or greater).
21 Merchants placed in excessive chargeback programs are subject to additional
22 scrutiny by the card networks, as well as possible fines and termination.

23 73. If a merchant's account is terminated for excessive chargebacks, an
24 acquirer must place the merchant on a list maintained by the credit card networks.
25 Mastercard, for example, maintains the Member Alert to Control High-risk
26 Merchants ("MATCH") list, which identifies terminated merchants and their
27 principals, and the reason for termination.

28

FILED UNDER SEAL PURSUANT TO ORDER OF THE COURT DATED MAY 23, 2019

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.

FILED UNDER SEAL PURSUANT TO ORDER OF THE COURT DATED MAY 23, 2019

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, Payvision, 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
20 value cards, and work with Thayne [an Allied employee]
21 to balance the MIDS). (Emphasis in original.)

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

25 85. As Khawaja promised, Allied eventually boarded the merchant in or
26 around December 2016, but not before Wells emailed Khawaja, Rountree, and
27 Diab again on November 3, 2016. In his email, Wells emphasized the need for six
28 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. . . .”

FILED UNDER SEAL PURSUANT TO ORDER OF THE COURT DATED MAY 23, 2019

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.

FILED UNDER SEAL PURSUANT TO ORDER OF THE COURT DATED MAY 23, 2019

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].”

FILED UNDER SEAL PURSUANT TO ORDER OF THE COURT DATED MAY 23, 2019

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, Payvision 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, Payvision risk analyst Snelling warned Diab and Rountree

FILED UNDER SEAL PURSUANT TO ORDER OF THE COURT DATED MAY 23, 2019

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.

FILED UNDER SEAL PURSUANT TO ORDER OF THE COURT DATED MAY 23, 2019

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,

FILED UNDER SEAL PURSUANT TO ORDER OF THE COURT DATED MAY 23, 2019

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

FILED UNDER SEAL PURSUANT TO ORDER OF THE COURT DATED MAY 23, 2019

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

FILED UNDER SEAL PURSUANT TO ORDER OF THE COURT DATED MAY 23, 2019

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 Wirecard, 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

FILED UNDER SEAL PURSUANT TO ORDER OF THE COURT DATED MAY 23, 2019

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, Payvision, 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 Wirecard, 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

FILED UNDER SEAL PURSUANT TO ORDER OF THE COURT DATED MAY 23, 2019

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.

FILED UNDER SEAL PURSUANT TO ORDER OF THE COURT DATED MAY 23, 2019

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

FILED UNDER SEAL PURSUANT TO ORDER OF THE COURT DATED MAY 23, 2019

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

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

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

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

28

FILED UNDER SEAL PURSUANT TO ORDER OF THE COURT DATED MAY 23, 2019

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

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

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

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

FILED UNDER SEAL PURSUANT TO ORDER OF THE COURT DATED MAY 23, 2019

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

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

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

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

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

24 **VIOLATIONS OF THE FTC ACT**

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

27 153. Acts or practices are unfair under Section 5 of the FTC Act if they
28 cause or are likely to cause substantial injury to consumers that consumers cannot

FILED UNDER SEAL PURSUANT TO ORDER OF THE COURT DATED MAY 23, 2019

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

3 **COUNT I**

4 154. Defendants' acts or practices in processing fraudulent and
5 unauthorized transactions to consumers' accounts, as described in paragraphs 45-
6 150 above, have caused or are likely to cause substantial injury to consumers that
7 is not reasonably avoidable by consumers themselves and that is not outweighed
8 by countervailing benefits to consumers or competition. Such injury is the
9 predictable result of the acts or practices described in paragraphs 45-150 above.

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

13 **CONSUMER INJURY**

14 156. Consumers in the United States have suffered and will continue to
15 suffer substantial injury as a result of Defendants' violations of the FTC Act. In
16 addition, Defendants have been unjustly enriched as a result of their unlawful acts
17 or practices. Absent injunctive relief by this Court, Defendants are likely to
18 continue to injure consumers, reap unjust enrichment, and harm the public interest.

19 **THE COURT'S POWER TO GRANT RELIEF**

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

27
28

FILED UNDER SEAL PURSUANT TO ORDER OF THE COURT DATED MAY 23, 2019

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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.

FILED UNDER SEAL PURSUANT TO ORDER OF THE COURT DATED MAY 23, 2019

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Dated: May 20, 2019

Respectfully submitted,

ALDEN F. ABBOTT
General Counsel



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