

UNITED STATES OF AMERICA  
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS:     **Lina M. Khan, Chair**  
                              **Noah Joshua Phillips**  
                              **Rebecca Kelly Slaughter**  
                              **Christine S. Wilson**

**In the Matter of:**

**Electronic Payment Systems, LLC**, a  
limited liability company, d/b/a EPS,

**Electronic Payment Transfer, LLC**, a  
limited liability company, d/b/a EPS,

**John Dorsey**, individually and as an  
officer of Electronic Payment Systems,  
LLC and Electronic Payment Transfer,  
LLC, and

**Thomas McCann**, individually and as  
an officer of Electronic Payment  
Systems, LLC and Electronic Payment  
Transfer, LLC.

**Docket No. C-4764**

**COMPLAINT**

The Federal Trade Commission, having reason to believe that Electronic Payment Systems, LLC, a limited liability company, Electronic Payment Transfer LLC, a limited liability company, and John Dorsey and Thomas McCann, individually and as officers of Electronic Payment Systems, LLC and Electronic Payment Transfer, LLC (collectively “Respondents”), have violated the provisions of the Federal Trade Commission Act and the Telemarketing Sales Rule (“TSR”), and it appearing to the Commission that this proceeding is in the public interest, alleges:



7. The acts and practices of Respondents alleged in this complaint have been in or affecting commerce, as “commerce” is defined in Section 4 of the Federal Trade Commission Act.

### **Respondents’ Business Activities**

8. In 2013, the FTC sued a deceptive telemarketing scam called Money Now Funding (“MNF” or “MNF scam”) for telemarketing worthless business opportunities to consumers



against the remaining MNF defendaini7.6 0.001 Tc -0.4y.52426 1f001 -1.32ul.9 (N)7.6 0.00iag in8 (F d)7.6

26. Consumers initiate “chargebacks” when they dispute credit card charges by contacting their “issuing bank,” which is the bank that issued the credit card to the consumer. When a consumer successfully disputes the charge, the consumer’s issuing bank credits the consumer’s credit card for the disputed amount, and then recovers the chargeback amount from the acquirer (the merchant’s bank). The acquirer, in turn, collects the chargeback amount from the merchant, either directly or through its ISO or payment processor.

27. In order to detect and prevent illegal, fraudulent, or unauthorized merchant activity, the card networks operate various chargeback monitoring and fraud monitoring programs. For example, if a merchant generates excessive levels of chargebacks that trigger the thresholds set under VISA’s chargeback monitoring program, the merchant is subject to additional monitoring requirements and, in some cases, penalties and termination.

28. In recent years, credit card laundering has become a common practice of fraudulent merchants who cannot meet a bank’s underwriting criteria or who cannot obtain merchant accounts under their own names (whether because of excessive chargebacks, complaints, or other signs of illegal activity).

29. Even when the fraudulent merchant can qualify for a merchant account, it often engages in laundering to conceal its true identity from consumers, the acquirer, the card networks, and law enforcement agencies.

30. To conceal their identities, fraudulent merchants often create shell companies to act as fronts, and apply for merchant accounts under these shell companies. Once the merchant accounts are approved, the fraudulent merchant then launders its own transactions through the shell company’s merchant accounts.

31. Fraudulent merchants often generate excessive rates of “chargebacks” from consumers who dispute the credit card charges. To avoid triggering the card networks’ chargeback monitoring programs and attracting the scrutiny of the acquirer, fraudulent merchants often spread out their sales transaction volume across multiple merchant accounts—a practice commonly referred to as “load balancing.”

32. Because the VISA and Mastercard chargeback monitoring programs apply only to merchants with at least 100 chargeback transactions per month,

triggering the monitoring programs by simply processing for short time periods, such as for a few weeks, that fall below the monitoring programs' time thresholds.

33. In addition to evading the card networks' merchant monitoring programs, frequent merchants sometimes spread their transactions over short periods of time to avoid triggering the monitoring programs' time thresholds.

37. Ii165 0 T17 52.78d(201)68 Td0 Td()Tj-17.4017 52.F2MC /LBody Td( g)CID (d)1d( o)0.001



44. In 2013, the principals, employees and associates of MNF changed the MNF fraudulent scheme's name and continued operating the same scam through newly created companies and aliases. Wigdore and his associates submitted to EPS phony applications for these fictitious companies. In turn, EPS approved the phony applications, opened merchant accounts for the companies at Merrick, and continued processing transactions for the MNF scam through these fraudulent merchant accounts.

45. Throughout 2012 and 2013, EPS—by underwriting and approving the MNF-related businesses for processing, establishing merchant accounts for these entities with Merrick, and processing for these merchant accounts—enabled MNF to charge consumers' credit or debit card accounts for its non-existent services.

46. Without the ISO and processing services provided by EPS, the MNF scam could not have obtained the fraudulent merchant accounts established at Merrick, through which their credit card transactions were processed.

47. According to statements made by EPS in court filings in July 2016 (see Mot. To Quash (ECF No. 9), *Electronic Payment Transfer, LLC v. Federal Trade Commission and Citywide Banks*, No. CV-01653-RBJ (D. Colo. July 11, 2016)), EPS's relationship with Wigdore dated back to approximate iii

---

50. As an ISO for Merrick, EPS was required to comply with Merrick's underwriting rules for screening merchants, which included guidelines designed to verify the identity of the merchant and the legitimacy of the merchant's business, and to screen out merchants potentially engaged in fraud. Indeed, Merrick's policy required EPS to verify "that each merchant is a bona fide business and that the transactions of such merchant will reflect bona fide business between the merchant and the cardholder, and will not violate any applicable provision of law." EPS was also required to monitor its merchants' transactions, update merchant information in the merchant database, and ensure that its merchants complied with the card networks' rules and various fraud monitoring programs. As a registered ISO with VISA (through Merrick), EPS also was required to comply with VISA's rules and regulations.

51. However, rather than verify its merchants' identities, EPS opened merchant accounts in the names of numerous fictitious companies for the same underlying merchant and submitted them to Merrick. By submitting those applications, EPS also enabled MNF to evade the various card network fraud and chargeback monitoring programs that were designed to detect and prevent fraudulent activity.

52. The chronology of EPS's involvement in the MNF scam's credit card laundering shows that EPS: (a) ignored obvious warning signs of fraud, including the likely presence of credit card laundering, (b) concealed from Merrick (the acquirer) and the card networks the true identity and nature of the MNF-related fictitious companies, and (c) made every effort to continue processing for the fictitious companies, and other merchants related to Wigdore and his associates, even after Merrick noticed signs of fraud and instructed EPS to stop.

53. On May 24, 2012, Merrick informed EPS's then-Risk Manager Michael Peterson that it had declined three merchant a1.9 (aydn a)1 (f)0J-04 (e).5 (re)0.8 (d(d)1.6 ( (c)1.v)-1.7 (e)6

55. Two weeks later, on June 14, 2012, Merrick declined four more merchant applications, this time highlighting the fact that all four applications had been referred to EPS by the same sales agent (“sales channel 2088,” a sales office number that EPS had assigned to KMA, acting as its sales agent), and that the merchants were all “home-based marketing companies,” a business model that Merrick had indicated was often problematic.

56. Despite these rejections and Merrick’s repeatedly-stated desire not to do business with companies linked to KMA, Peterson continued to submit new merchant applications to Merrick that had been referred by EPS’s “sales agent” KMA, without informing Merrick that KMA was the underlying sales agent who had referred those applications to EPS.

57. Each of the 23 MNF-related merchant applications Wigdore submitted to EPS in 2012 indicated that the sales agent was “Jay Wigdore” of sales office “2088.” As noted above, this was the number EPS had assigned to its sales agent KMA, although on their face the applications did not mention KMA directly. In addition to the fact that the applications were referred by the sales agent KMA, an entity whose own business (as an EPS client merchant) Merrick had repeatedly rejected due to concerns about fraud, these applications from 23 supposedly different merchants appeared virtually identical and contained numerous suspicious red flags, as described below. EPS approved them all.

- a) Almost all the merchants were located in the Phoenix, Arizona area. The “business description” provided for most of the merchants was extremely vague, almost always identical (i.e., “marketing and advertising”), and provided no specific description of the product or service being sold.
- b) The 23 supposedly separate merchants attached facially suspect checks that appeared almost identical in form. Each of the attached doctored checks was drawn on Chase bank and had the same bank routing number, indicating the same bank branch. Almost all of them bore the same check number: “1001.” The fact that 23 supposedly different merchants all purported to hold accounts at the same bank branch and submitted virtually identical checks (almost always bearing the same check number) was an indicator that they were likely related to each other or to the same underlying merchant. Despite these red flags, EPS did not verify the legitimacy of the 23 bank accounts at Chase.

- c) During the initial underwriting stage, EPS obtained credit reports for each of the 23 fictitious companies. For most of the



65. Not only did EPS begin processing for MNF's fictitious companies before these companies were approved by Merrick, but EPS also began processing for certain MNF-related fictitious companies even after Merrick already had declined the applications for these same fictitious companies.

66. Between May 2012 and June 2012, Merrick declined 11 fraudulent merchant applications approved and submitted by EPS on behalf of MNF-related fictitious companies. EPS nonetheless continued processing for these fictitious companies, in some cases for more than two months after they had been declined by Merrick.

67. By the end of June 2012, EPS had processed more than \$573,000 in transactions for the 11 declined fictitious companies, for time periods ranging from just two weeks to eight weeks per merchant—short time periods (between two and eight weeks) that fall below VISA's chargeback monitoring program thresholds.

68. Although Merrick had declined 11 applications that Wigdore had referred to EPS by late June 2012, EPS nonetheless approved and forwarded to Merrick seven additional fraudulent merchant applications, also submitted by Wigdore to EPS, between July 24, 2012 and September 5, 2012.

69. These seven new applications appeared suspiciously similar to the 11 applications that Merrick had previously declined. They attached the same facially suspect checks indicating that the merchants all banked at the same bank ("Chase") and had the same routing number. Four applications indicated that the merchant's bank was Comerica, even though they attached a Chase bank check. The credit report for one merchant indicated an extremely poor credit score and a "past due amount" of \$144,904 owed by the merchant, while the credit report for another merchant showed a "past due amount" of \$24,344. The address listed on the credit report for a third merchant did not match the merchant address listed on the application. For four of the merchants, the initial risk review conducted by an EPS employee specifically noted that no marketing materials or web listings for the merchant had been submitted or found. Despite these obvious red flags, EPS approved all seven applications.

70. As it had before, EPS allowed payments to be processed through these seven new accounts for short time periods, typically ranging from three to seven weeks.

71. Merrick's underwriting policy required EPS to monitor its client merchants' transactions "in order to detect unusual or unacceptable trends in such

Merchant's processing activity," and to monitor its merchants' chargeback transactions and consumer inquiries relating to these chargeback transactions.

72. EPS regularly monitored its merchants' chargeback transactions. Through the processing platforms provided by two payment processors, EPS had access to its merchants' chargeback transaction data, together with the consumer complaints that accompanied chargeback requests.

73. Once EPS began processing for the 23 accounts set up for the MNF-related fictitious merchants, these accounts began generating substantial chargebacks, many of which included "chargeback reason codes" indicating that the merchant's charges either were not authorized by the consumer, were fraudulent, or that the merchant failed to provide the goods or services as promised.

74. In some cases, the chargeback requests included consumer complaints and documentation clearly indicating that the merchant involved was "Money Now Funding," and not the fictitious company whose name was on the merchant account—obvious evidence of credit card laundering.

75. As EPS's Risk Manager, Peterson oversaw EPS's Risk Department, and closely interacted with EPS' principals, Respondents Dorsey and McCann, and EPS's Chief Operating Officer ("COO").

76. Peterson regularly communicated with KMA and Abdelmesseh. On September 4, 2012, Peterson received an email from an EPS employee he supervised. The email forwarded to Peterson a consumer's chargeback dispute documentation for a "KMA Merchant Services" merchant account and stated: "all supporting documentation sent in to rebuttal dispute has 'Rose Marketing, LLC' plastered all over the paperwork." The chargeback documents clearly indicated that the transactions for a company called "Rose Marketing" had been laundered through the KMA merchant account.

77. Peterson immediately forwarded the email to "Mike Stewart" of KMA (Abdelmesseh used "Mike Stewart" as an alias), adding:

Stewart, We cannot win pre-arb [prearbitration] with this documentation. We are going to have to let the cardholder win on this one as the argument against factoring is too great. Please review and advise.

As noted above, credit card laundering is often referred to as "factoring."

78. Peterson also directly instructed Abdelmesseh, acting in his capacity as EPS's sales agent, to spread out the transactions of KMA's client merchant across multiple merchant accounts opened in the names of the fictitious companies.

79. In a September 17, 2012 email to "Mike Stewart" of KMA, Peterson wrote:

Stewart, Please see my notes below for the accounts that are on hold. We need to spread this out more, I am trying to cap each individual account in the \$30-\$40K



Arizona), an obvious sign that these entities were related to the same underlying merchant.

85. An EPS Risk Department employee forwarded the list of address changes to Peterson and wrote a note asking: “Why are all the addresses the same?”

86. Despite knowing that numerous allegedly different merchants referred by KMA/Wigdore shared the same business address, in addition to all the other red flags regarding fraudulent activity by Wigdore and Abdelmesseh, EPS decided to renew its sales agent relationship with them.

87. By the end of 2012, Merrick had declined most of the MNF-related merchants. Despite this fact, throughout 2013, EPS continued accepting and approving merchant applications referred by Wigdore, using “sales channel 2088.” These included phony merchant applications for the MNF-related fictitious merchants.

88. Like the merchant applications from 2012, the applications for MNF-related fictitious companies in 2013 contained obvious signs that the merchants likely were not legitimate businesses and were related to the same underlying merchant. For example, at least 14 supposedly different merchants purported to have bank accounts at the same bank branch, this time at a Wells Fargo Bank branch located in Mesa, Arizona.

89. The MNF-related merchant applications submitted in 2013 included four fictitious entities controlled by Luke Rose, the principal of the MNF scam. EPS





102. Similarly, EPS's principals, Respondents McCann and Dorsey, approved and oversaw the MNF-related merchant accounts, and personally met with the sales agents who referred the accounts to EPS.

103. EPS did not have a separate department responsible for underwriting and approving merchant applications. Instead, EPS's principals, McCann and Dorsey, together with EPS's COO, were directly responsible for approving almost all merchant applications submitted to EPS for underwriting approval.

104. Despite being EPS's Risk Manager, Peterson rarely had unilateral authority to approve any merchant applications. In fact, Peterson was generally required to obtain the approval of merchant applications from Respondents Dorsey or McCann, or EPS's COO.

105.

Wigdore was a co-owner or co-officer of the merchant, and five of which stated that  
th

114. Credit card laundering is illegal and prohibited by the rules and policies of the credit card networks. No countervailing benefits flow to consumers or

present to or deposit into the credit card system for payment, a credit card sales draft generated by a telemarketing transaction that is not the result of a telemarketing credit card transaction between the cardholder and the merchant. 16 C.F.R. §§ 310.3(c)(1)–(2).

121. The TSR prohibits any person from providing substantial assistance or support to any seller or telemarketer when that person knows or consciously avoids knowing that the seller or telemarketer is engaged in acts or practices that violate Sections 310.3(a), (c) or (d), or Section 310.4 of the TSR. 16 C.F.R. § 310.3(b).

**Count I**  
**Unfair Credit Card Laundering**

122. As described in Paragraphs 35 through 114 of this Complaint, in numerous instances, Respondents Electronic Payment Systems, LLC; Electronic Payment Transfer, LLC; John Dorsey; and Thomas McCann have engaged in credit card laundering on behalf of the Money Now Funding scam by:

- a) Falsely representing that the fictitious companies listed as the applicants on the merchant applications were the true merchants who were applying for merchant accounts;
- b) Approving and opening merchant accounts in the names of

## Violations of Section 5

124. The acts and practices of Respondents as alleged in Count I of this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act.

### Count II Assisting and Facilitating Credit Card Laundering

125. In numerous instances, Respondents provided substantial assistance or support to sellers and telemarketers (the MNF-related merchants) that the Respondents knew, or consciously avoided knowing, were engaged in credit card laundering acts or practices that violate Sections 310.3(c)(1) and (2) of the TSR, as described in Paragraphs 35 through 114 above.

### Violations of the Telemarketing Sales Rule

126. The acts and practices of Respondents as alleged in Count II of this complaint constitute a violation of the TSR, 16 C.F.R. § 310.3(b), and are therefore a violation of a rule promulgated under Section 18 of the FTC Act, 15 U.S.C. § 57a, and therefore constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act. *See* 15 U.S.C. § 6102(c).

**THEREFORE**, the Federal Trade Commission this ~~day~~ *W K day* 0 D \, 20 , has issued this Complaint against Respondents.

By the Commission.

April J. Tabor  
Secretary

SEAL: